Учреждение образования
«Белорусский государственный университет
культуры и искусств»

Факультет культурологии и социокультурной деятельности
Кафедра информационных технологий в культуре

СОГЛАСОВАНО
Заведующий кафедрой

_____ П. В. Гляков
«___»_____ 2017 г.

СОГЛАСОВАНО
Декан факультета

_____ И. Н. Воронович
«___»_____ 2017 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

для специальности 1-21 04 01 Культурология (по направлениям),
направления специальности 1-21 04 01-02 Культурология (прикладная)
специализации 1-21 04 01-02 04 Информационные системы в культуре

Составители:
П. В. Гляков, заведующий кафедрой информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат физико-математических наук, доцент
Т. С. Жилинская, старший преподаватель кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат педагогических наук
Т. И. Песецкая, доцент кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат физико-математических наук

Рассмотрено и утверждено
на заседании Совета университета
(протокол № 10 от 28 июня 2016 г.)

Минск
БГУКИ
2017

УДК 004:[519.1+519.7]+008:001](075.8)
ББК 22.17+22.18+78.07]я73
Т 338

Р е ц е н з е н т ы :
кафедра Web-технологий и компьютерного моделирования Белорусского государственного университета;
А. К. Демидович, доцент кафедры современных методик и технологий образования государственного учреждения образования «Академия последипломного образования», кандидат физико-математических наук, доцент

Т338 **Теоретические основы** информационных технологий : учеб.-метод. комплекс / сост.: П. В. Гляков, Т. С. Жилинская, Т. И. Песецкая ; Белорус. гос. ун-т культуры и искусств. – Минск : БГУКИ, 2017. – 319 с.
ISBN 978-985-522-182-2.

Излагаются основы линейной алгебры, теории графов, теории вероятностей и математической статистики, теории информации и криптологии, а также информационно-коммуникационные технологии социально-культурной сферы, медиасреды и медиаобразования.

Предназначен для студентов, магистрантов и аспирантов творческих специальностей учреждений высшего образования.

УДК 004:[519.1+519.7]+008:001](075.8)
ББК 22.17+22.18+78.07]я73

ISBN 978-985-522-182-2

СОДЕРЖАНИЕ

III. МЕДИАКУЛЬТУРА СПЕЦИАЛИСТА

ПРАКТИЧЕСКИЙ РАЗДЕЛ

РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

ВВЕДЕНИЕ

В системе учебных дисциплин, предусмотренных для студентов специальности 1-21 04 01 Культурология (по направлениям), направления специальности 1-21 04 01-02 Культурология (прикладная), значимое место занимает учебная дисциплина «Теоретические основы информационных технологий». Она призвана стать основой для понимания практически всех изучаемых направлений информационных технологий. Эта дисциплина является интегральной и состоит из трех разделов – «Прикладная математика», «Основы теории информации и криптологии», «Медиакультура специалиста».

Учебная дисциплина «Теоретические основы информационных технологий» ориентирована на формирование у студентов способностей к межличностным коммуникациям, работе в команде, критическому мышлению, эффективному использованию информационных технологий, рекламе в социокультурной сфере, анализу и оценке собранных сведений, разработке социально-культурных программ, организации межкультурной, познавательной и творческой деятельности.

Изучение этой дисциплины поможет студентам не только глубже разобраться в тех процессах, которые происходят в культуре при построении информационного общества, но и стать активными участниками этих процессов.

Учебная дисциплина «Теоретические основы информационных технологий» имеет связь с такими учебными дисциплинами, как «Основы информационных технологий», «Информационные технологии в культуре», «Информационные процессы и системы», «Проектирование информационных ресурсов и систем».

Концептуальная новизна учебно-методического комплекса «Теоретические основы информационных технологий» заключается в изучении и применении элементов медиаобразования как эффективного средства развития творческой, самостоятельно и критически мыслящей личности в условиях интенсивного увеличения информационного потока.

Целями учебно-методического комплекса «Теоретические основы информационных технологий» являются формирование знаний и умений по использованию математических методов при моделировании информационных процессов в культуре и искусствах; формирование знаний и умений для представления, измерения, сжатия и передачи информации и ее защиты с помощью криптографических методов; формирование знаний, умений и навыков доступа к информационным ресурсам посредством медиасреды, критического восприятия медиавоздействий, позиционирования в медиасреде, а также использование элементов медиаобразования в профессиональной деятельности культуролога.

Основными *задачами* являются:

– изучение основных понятий линейной алгебры, теории графов, теории вероятностей, математической статистики и теории фракталов;

– знакомство с центральными теоремами и методами указанных разделов математики;

– приобретение умений постановки и решения практических задач математическими методами;

– знакомство с процессами передачи и восприятия информации;

– изучение основных способов представления, измерения, сжатия и передачи информации;

– приобретение умений защищать информацию с помощью криптографических методов;

– изучение основных платформ для работы с медиаприложениями, знание их достоинств и недостатков, возможностей

использования в зависимости от поставленных профессиональных задач;

– изучение особенностей поиска различных видов медиаресурсов (текстовых, графических, видео, звуковых и др.) профессиональной тематики;

– знакомство с авторскими правами в Интернете;

– освоение технологий создания, редактирования, размещения и управления медиатекстами, поиска, участия, организации и регулирования деятельности сетевых сообществ;

– знакомство с основными этапами исторического развития медиакультуры;

– развитие способности к критическому восприятию и анализу медиатекстов.

В предлагаемом учебно-методическом комплексе представлены материалы четырех разделов: теоретический (материалы для теоретического изучения учебной дисциплины), практический (материалы для проведения лабораторных, практических, семинарских и индивидуальных учебных занятий), раздел контроля знаний (материалы, позволяющие определить соответствие результатов учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации образовательных программ высшего образования), вспомогательный (учебные программы, методические рекомендации, иные материалы, содержащие сравнительную и аналитическую информацию). Занятия проходят в виде погружения студентов в коммуникационный процесс: поиск, создание, редактирование, анализ, размещение и тиражирование электронных медиатекстов. Методика проведения занятий предполагает использование проблемных и эвристических форм обучения, которые развивают индивидуальность студентов, самостоятельность их мышления. Сотрудничество в группах, коллективные дискуссии, экспериментирование, проектирование, привлечение дополнительного информационного материала с использованием электронной

медиасреды – основные методы обучения. Материал излагается на основе современных методических требований с учетом педагогических целей на уровнях представления, понимания, знания, применения и творчества. При чтении лекций, проведении семинарских, практических и лабораторных занятий особое внимание уделяется рассмотрению примеров, иллюстрирующих то или иное понятие, приводятся различные способы интерпретации понятий.

Практические и лабораторные занятия направлены на формирование умений использования полученных знаний при решении конкретных задач. Методика их проведения должна содействовать развитию творческих способностей каждого студента и приобретению навыков самостоятельной работы. Используются такие новые формы активизации образовательного процесса, как игры, викторины и т. п.

В соответствии с учебным планом на изучение учебной дисциплины «Теоретические основы информационных технологий» всего предусмотрено 412 часов, из которых 198 часов – аудиторные занятия (64 часа – лекции, 72 часа – лабораторные занятия, 34 часа – практические занятия, 28 часов – семинары).

Примерный тематический план
(дневная форма обучения)

Разделы и темы	Количество аудиторных часов				
	всего	лекции	лабораторные	семинары	практические занятия
Раздел 1. Прикладная математика					
Тема 1. Введение в прикладную математику	2	2			
Тема 2. Матрицы	4	2			2
Тема 3. Линейные уравнения	4		2		2
Тема 4. Основные понятия теории графов	2	2			
Тема 5. Матричные представления графов	2				2
Тема 6. Задачи оптимизации на графах	6	2	2		2
Тема 7. Пространство событий	4	2			2
Тема 8. Способы задания вероятностей	4	2			2
Тема 9. Операции над вероятностями	4	2			2
Тема 10. Дискретная случайная величина	4	2			2
Тема 11. Основные распределения случайных величин	4	2	2		
Тема 12. Основные понятия математической статистики	4	2	2		
Тема 13. Основы фрактальной геометрии	4	2	2		
Тема 14. Алгебраические и стохастические фракталы	2	2			2
Всего по 1 разделу…	**52**	**24**	**10**		**18**
Раздел 2. Основы теории информации и криптологии					
Тема 15. Введение в теорию информации	2	2			
Тема 16. Система передачи информации	4	2		2	
Тема 17. Представление информации	6	2	4		
Тема 18. Форматы данных в Интернете	6	2		4	
Тема 19. Сжатие информации	8	2	4	2	
Тема 20. Энтропия дискретного источника	8	2	4	2	
Тема 21. Введение в криптологию	2	2			
Тема 22. Методы шифрования информации	8	2	6		
Тема 23. Электронная цифровая подпись	2	2			

Тема 24. Стандарты и правовые акты электронной цифровой подписи	2			2	
Тема 25. Генерация простых чисел	4		4		
Тема 26. Алгоритмы хеширования	6	2	4		
Всего по 2 разделу…	**58**	**20**	**26**	**12**	
Раздел 3. Медиакультура специалиста					
Тема 27. Введение. Медиасреда и медиакультура в условиях информационного общества	4	2		2	
Тема 28. Место и роль медиасреды и медиаобразования в профессиональной деятельности культуролога	8	4		4	
Тема 29. Медиатекст как средство художественно-творческой, воспитательной и организационно-методической деятельности учреждений культуры и искусств	8	2			6
Тема 30. Информационные ресурсы социокультурной сферы: технологии их поиска и использования	2	2			
Тема 31. Коммуникативное пространство. Сетевые сообщества	20	2	10	4	
Тема 32. Авторское право и информационная безопасность в Интернете	4	2		2	
Тема 33. Компьютерные среды для работы с медиаприложениями	10	2	8		
Тема 34. Программные средства создания, редактирования и управления медиатекстами	30	2	18	4	6
Тема 35. Медиапроект социально-культурной тематики: технологии создания и размещения	2	2			
Всего по 3 разделу…	**88**	**20**	**36**	**16**	**16**
Итого…	**198**	**64**	**72**	**28**	**34**

Примерный тематический план
(заочная форма обучения)

Разделы и темы	Количество аудиторных часов				
	всего	лекции	лабораторные	семинары	практические занятия
Раздел 1. Прикладная математика					
Тема 1. Введение в прикладную математику					
Тема 2. Матрицы	2	2			
Тема 3. Линейные уравнения	2		2		
Тема 4. Основные понятия теории графов	2	2			
Тема 5. Матричные представления графов	2				2
Тема 6. Задачи оптимизации на графах	2		2		
Тема 7. Пространство событий	2	2			
Тема 8. Способы задания вероятностей	2	2			
Тема 9. Операции над вероятностями	2				2
Тема 10. Дискретная случайная величина	2				2
Тема 11. Основные распределения случайных величин	2	2			
Тема 12. Основные понятия математической статистики	2		2		
Тема 13. Основы фрактальной геометрии	2	2			
Тема 14. Алгебраические и стохастические фракталы					
Всего по 1 разделу…	**24**	**12**	**6**		**6**
Раздел 2. Основы теории информации и криптологии					
Тема 15. Введение в теорию информации	2	2			
Тема 16. Система передачи информации	2	2			
Тема 17. Представление информации	4	2	2		
Тема 18. Форматы данных в Интернете	2			2	
Тема 19. Сжатие информации	2	2			
Тема 20. Энтропия дискретного источника	2	2			
Тема 21. Введение в криптологию	2	2			
Тема 22. Методы шифрования информации	4	2	2		
Тема 23. Электронная цифровая подпись	2			2	

Тема 24. Стандарты и правовые акты электронной цифровой подписи	2			2	
Тема 25. Генерация простых чисел	2		2		
Тема 26. Алгоритмы хеширования	2		2		
Всего по 2 разделу…	**28**	**14**	**8**	**6**	
Раздел 3. Медиакультура специалиста					
Тема 27. Введение. Медиасреда и медиакультура в условиях информационного общества	2	2			
Тема 28. Место и роль медиасреды и медиаобразования в профессиональной деятельности культуролога	4	2		2	
Тема 29. Медиатекст как средство художественно-творческой, воспитательной и организационно-методической деятельности учреждений культуры и искусств	6	2			4
Тема 30. Информационные ресурсы социокультурной сферы: технологии их поиска и использования	2	2			
Тема 31. Коммуникативное пространство. Сетевые сообщества	12	2	6	2	2
Тема 32. Авторское право и информационная безопасность в Интернете	2			2	
Тема 33. Компьютерные среды для работы с медиаприложениями	6	2	4		
Тема 34. Программные средства создания, редактирования и управления медиатекстами	20	2	12	2	4
Тема 35. Медиапроект социально-культурной тематики: технологии создания и размещения	2		2		
Всего по 3 разделу…	**56**	**14**	**24**	**8**	**10**
Итого…	**108**	**40**	**38**	**18**	**12**

ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

КОНСПЕКТЫ ЛЕКЦИЙ

I. ПРИКЛАДНАЯ МАТЕМАТИКА

Тема 1. Введение в прикладную математику

Современные информационные технологии позволяют любому пользователю вне зависимости от образования, профессиональной деятельности, навыков и умений легко осваивать методики, необходимые для того либо иного рода деятельности. Не секрет, что любой информационный ресурс базируется на тех либо иных математических алгоритмах. Однако, знание математических основ требуется не только для создания информационных ресурсов, но и для решения многих прикладных задач с их помощью.

Так, например, в моделировании 2D и 3D изображений широко применяется такой математический объект, как матрица. Знакомство с этим объектом не обязательно для пользователя графического редактора, но необходимо для его создания. Например, с помощью матриц задаются координаты объекта и осуществляются операции по его перемещениям. Рассмотрим случай однородной двумерной системы координат. Здесь координаты объекта задаются в виде матрицы размером n×3:

$$\begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ \cdot & \cdot & \cdot \\ x_n & y_n & 1 \end{pmatrix}$$

где x_i и y_i – координаты вершин объекта по осям X и Y, n – количество строк матрицы соответствует количеству вершин

объекта, каждая из которых занимает в матрице свою строку. Значения третьего столбца соответствуют масштабирующему множителю.

Базовым преобразованием двумерных объектов является преобразование, которое можно выполнить за один шаг с помощью матрицы преобразования:

$$\begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ \cdot & \cdot & \cdot \\ x_n & y_n & 1 \end{pmatrix} \times \underbrace{\begin{pmatrix} a & b & p \\ d & e & q \\ l & m & s \end{pmatrix}}_{\text{матрица преобразования}} = \begin{pmatrix} x'_1 & y'_1 & 1 \\ x'_2 & y'_2 & 1 \\ \cdot & \cdot & \cdot \\ x'_n & y'_n & 1 \end{pmatrix}$$

Каждый параметр матрицы преобразования отвечает за определенный вид преобразования:

– перенос (параметры ***l, m***);

– масштабирование (параметры ***a, e, s***);

– зеркальное отображение относительно осей или начала координат (параметры ***a, e, s***);

– сдвиг (параметры ***b, d***);

– проецирование (параметры ***p, q***);

– вращение вокруг осей координат (параметры ***a, b, d, e***).

Теория **графов** широко используется, например, в логистике – области планирования, управления и контроля движения материальных, информационных и финансовых ресурсов в различных системах. Одной из первых логистических задач, решенных с помощью использования теории графов, можно считать задачу о Кенигсбергских мостах. В центральной части города Кенигсберг (ныне Калининград), включающей два берега реки Перголя, имеется два острова и семь соединяющих мостов (рис. 1.1). Задача состоит в том, чтобы обойти все четыре части суши, пройдя по каждому мосту один раз, и вернуться в исходную точку. Задача была решена Эйлером в 1736 г. Он показал, что решения не существует.

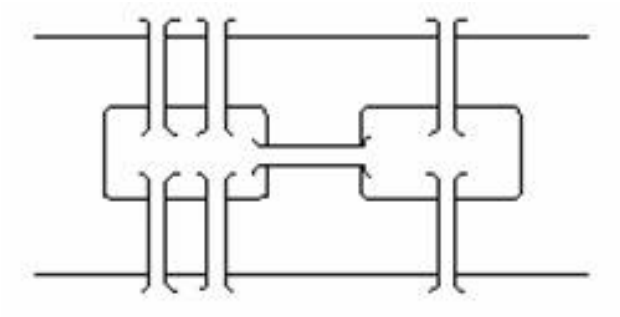


Рис. 1.1. Задача о Кенигсбергских мостах

Такие разделы математики, как теория **вероятности и статистический анализ,** широко применяются в исследованиях любой области человеческой деятельности от финансово-экономических исследований до исследований в области генетики, от менеджмента качества до медицины. Развитие информационных технологий и сети интернет вывело возможности анализа с помощью статических методов на абсолютно новый уровень, стимулируя, в том числе и развитие самой статистики, как математической дисциплины. Современные статистические пакеты позволяют легко и быстро обрабатывать огромные массивы статистических данных, и с каждой следующей версией пополняются новым статистическим арсеналом, разработанным математиками. В последнее время статистический анализ активно используется в сфере продвижения и рекламы в интернете, помогая оптимизировать информационные потоки и направлять их целевым группам пользователей посредством определенных интернет-ресурсов, выбранных в результате статистического анализа.

Фракталы, относительно молодой математический объект, обязанный своим рождением и развитием изобретению компьютера. Диапазон применения фракталов невероятно широк – от создания спецэффектов и виртуальных декораций в кино до генерации музыкальных произведений. В современном изобразительном искусстве отдельным разделом выделена фрактальная графика. Ее уникальность заключается в том, что в создании произведения участвуют как компьютер, генерирующий фрактальное изображение с помощью запрограммированного

математического алгоритма, так и художник, управляющий генерацией изображения с помощью выбора параметров и настроек генерации и обрабатывающий полученное изображение с целью создания художественного произведения.

Тема 2. Матрицы

Матрицей размера $m \times n$ называется прямоугольная таблица элементов a_{ij}, расположенных в m строках и n столбцах:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

где первый индекс i элемента a_{ij} означает номер столбца, второй индекс j – номер строки. Элементами матрицы чаще всего являются числа, однако могут быть и другие математические объекты. Для сокращенного обозначения матрицы используют также запись (a_{ij}).

Матрица размера $n \times n$ называется **квадратной матрицей порядка *n***

$$A_{n\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

Элементы a_{11}, a_{22} … a_{nn}, стоящие на диагонали квадрата, проходящей из левого верхнего угла в правый нижний, образуют **главную диагональ квадрата** и называются **главными диагональными элементами**. Элементы a_{1n}, $a_{2n\text{-}1}$ … a_{n1}, стоящие на диагонали квадрата, проходящей из правого верхнего угла в левый нижний, образуют побочную диагональ квадрата и называются **побочными диагональными элементами.** Матрица, у которой все элементы равны нулю, кроме главных диагональных элементов называется **диагональной матрицей**.

Матрица, состоящая из одного столбца (строки), называется **матрицей-столбцом (матрицей-строкой)**.

Транспонированной матрицей A^T называется матрица, полученная из исходной матрицы A заменой строк на столбцы.

Симметричной (симметрической) называют квадратную матрицу, элементы которой симметричны относительно главной диагонали, то есть $a_{ij} = a_{ji}$ для всех i, j.

Для симметрической матрицы верно $A = A^T$.

Произведение матрицы $A=(a_{ij})$ на число λ есть матрица $\lambda A=(\lambda\ a_{ij})$, где каждый ее элемент равен соответствующему элементу матрицы A, умноженному на число λ.

Суммой $A+B$ двух матриц $A_{m\times n}=(a_{ij})$ и $B_{m\times n}=(b_{ij})$, имеющих одинаковый размер, является матрица $C_{m\times n}= (c_{ij})$, имеющая тот же размер с элементами $c_{ij} = a_{ij} + b_{ij}$. Сложение матриц одинакового размера происходит поэлементно.

Пример. Даны матрицы A и B

$$A = \begin{pmatrix} -1 & 2 & 0 \\ 1 & 3 & -3 \\ 4 & 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 3 \\ 4 & -2 & 0 \\ 3 & -1 & 1 \end{pmatrix}$$

Найти матрицу $C = (A + 2B)^T$.

Решение.

$$2 \cdot B = 2 \cdot \begin{pmatrix} 0 & 1 & 3 \\ 4 & -2 & 0 \\ 3 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 6 \\ 8 & -4 & 0 \\ 6 & -2 & 2 \end{pmatrix}$$

$$A + 2B = \begin{pmatrix} -1 & 2 & 0 \\ 1 & 3 & -3 \\ 4 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 6 \\ 8 & -4 & 0 \\ 6 & -2 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 4 & 6 \\ 5 & -1 & -3 \\ 10 & -2 & 1 \end{pmatrix}.$$

$$C = (A + 2B)^T = \begin{pmatrix} -1 & 4 & 6 \\ 5 & -1 & -3 \\ 10 & -2 & 1 \end{pmatrix}^T = \begin{pmatrix} -1 & 5 & 10 \\ 4 & -1 & -2 \\ 6 & -3 & 1 \end{pmatrix}$$

Нулевой матрицей, обозначаемой O, называется матрица все элементы которой равны нулю.

Матрицей **противоположной** для матрицы $A = (a_{ij})$ является матрица $-A = (-a_{ij})$:

$A + (-A) = O$.

Таким образом, $B + (-A) = B - A$ и $-(-A) = A$.

Свойства сложения и умножения на числа.

1. Сложение матриц одинакового размера:

– ассоциативно $(A + B) + C = A + (B + C)$

– коммутативно $A + B = B + A$

2. Умножение матрицы А на числа λ, μ подчиняется правилам:

$$(\lambda\mu)\cdot A = \lambda\cdot(\mu A);\ 0\cdot A = 0;\ \lambda\cdot O = O;\ (-1)\cdot A = -A.$$

3. Сложение матриц и умножение на числа подчиняются законам дистрибутивности:

$$(\lambda\mu)\cdot A = \lambda A + \mu A,\ \lambda\cdot(A+B) = \lambda A + \lambda B.$$

Произведением двух матриц $A_{m\times n}$ и $B_{n\times k}$ является матрица

$$C_{m\times k} = A_{m\times n} \times B_{n\times k} = (c_{ij} = \sum_j^n a_{ir} \times b_{rj}).$$

Важно отметить, что перемножение двух матриц $A_{m\times p}$ и $B_{s\times k}$ возможно при условии того, что число столбцов матрицы $A_{m\times p}$ равно числу строк матрицы $B_{s\times k}$, то есть $p = s$. Из этого следует, что для двух квадратных матриц одинакового размера перемножение всегда допустимо.

Пример. Даны матрицы A и B. Найти матрицу $C = A\times B$.

$$A = \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix}, B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & -3 \end{pmatrix}$$

Решение. Число столбцов матрицы A размерности 2×2 равно числу строк матрицы B размерности 2×3, следовательно матрицы можно перемножить. Согласно правилу перемножения матриц, итоговая матрица C будет иметь размерность 2×3:

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix}$$

$c_{11}=1\cdot(-1)+(-2)\cdot0=-1$; $c_{12}=1\cdot2+(-2)\cdot1=0$; $c_{13}=1\cdot0+(-2)\cdot(-3)=6$;

$c_{21}=0\cdot(-1)+3\cdot0=0$; $c_{22}=0\cdot2+3\cdot1=3$; $c_{23}=0\cdot0+3\cdot(-3)=-9$.

$$C = \begin{pmatrix} -1 & 0 & 6 \\ 0 & 3 & -9 \end{pmatrix}$$

Единичной матрицей E_n n-го порядка называется диагональная матрица размерности $n \times n$, главные диагональные элементы которой равны 1:

$$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

Для единичной матрицы верно: $A \times E = E \times A = 0$.

Обратной матрицей для квадратной матрицы A называется матрица A^{-1}, такая, что $A \cdot A^{-1} = A^{-1} \cdot A = E$.

Один из способов нахождения обратной матрицы связан с такими понятиями, как определитель матрицы, миноры и алгебраические дополнения.

Определителем квадратной матрицы второго порядка является число Δ, равное разности произведения главных диагональных элементов и побочных диагональных элементов:

$$A_{2\times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$det\, A_{2\times 2} = \Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Определитель квадратной матрицы третьего порядка можно найти **разложением по строке или столбцу.** Пусть имеется матрица третьего порядка A:

$$A_{3\times 3} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Ее определитель равен числу Δ, вычисленному разложением по первой строке:

$$\Delta = \begin{vmatrix} a_{11}^{+} & a_{12}^{-} & a_{13}^{+} \\ a_{21}^{-} & a_{22}^{+} & a_{23}^{-} \\ a_{31}^{+} & a_{32}^{-} & a_{33}^{+} \end{vmatrix} =$$

$$= a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$$

Строка определителя состоит из трех элементов a_{11}, a_{12}, a_{13}, каждому из которых в соответствие поставлен знак «+» если сумма индексов элемента четна (для a_{11} это 1+1=2) или знак

«-», если сумма индексов элемента нечетна (для a_{12} это 1+2=3). Далее каждый из элементов, взятый с соответствующим знаком умножается на определитель второго порядка, полученный из определителя третьего порядка вычеркиванием строки и столбца, в которой находится этот элемент. Например, для элемента a_{12}

$$-a_{12}\times\begin{vmatrix} \cancel{a_{11}^{+}} & \cancel{a_{12}^{-}} & \cancel{a_{13}^{+}} \\ a_{21}^{-} & \cancel{a_{22}^{+}} & a_{23}^{-} \\ a_{31}^{+} & \cancel{a_{32}^{-}} & a_{33}^{+} \end{vmatrix} = -a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$$

В этом случае определитель $M_{12}=\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$ называется **минором** элемента a_{12}, а число $A_{12}=(-1)^{1+2}\times M_{12}$ называется его **алгебраическим дополнением**.

Пример. Найти определитель матрицы

$$A=\begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & 2 \\ 4 & 1 & 3 \end{pmatrix}$$

Решение.

$$\det A=\begin{vmatrix} 3^{+} & 2^{-} & 1^{+} \\ 1 & 0 & 2 \\ 4 & 1 & 3 \end{vmatrix}=3\begin{vmatrix} 0 & 2 \\ 1 & 3 \end{vmatrix}-2\begin{vmatrix} 1 & 2 \\ 4 & 3 \end{vmatrix}+1\begin{vmatrix} 1 & 0 \\ 4 & 1 \end{vmatrix}=$$

$$=3\cdot(0\cdot 3-2\cdot 1)-2\cdot(1\cdot 3-2\cdot 4)+(1\cdot 1-0\cdot 4)=$$

$$=3\cdot(-2)-2\cdot(-5)+1\cdot(1)=-6+10+1=5.$$

Вычисление определителя четвертого порядка и далее порядка n осуществляется аналогично вычислению определителя третьего порядка разложением по строке или столбцу.

В общем случае **минором** M_{ij} определителя n-го порядка называют определитель $(n-1)$-го порядка, полученный из исходного определителя вычеркиванием i-й строки и j-го столбца. Существуют также миноры $(n-2)$-го порядка, которые получа-

ются аналогично минорам (n-1)-го порядка, при рассмотрении каждого из миноров M_{ij} в качестве определителя порядка (n-1).

Алгебраическим дополнением A_{ij} к элементу a_{ij} определителя n-го порядка называют число $A_{ij} = (-1)^{i+j} \times M_{ij}$.

Рангом матрицы *A*, обозначаемым rang(A) называют наивысший из порядков миноров этой **матрицы**, определитель которых отличен от нуля.

Пример на нахождение ранга матрицы.

Обратную матрицу A^{-1} для матрицы n-го порядка A, можно вычислить согласно следующему правилу:

$$A^{-1} = \frac{1}{\det A} \times \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix}^{T}$$

где A_{ij} – алгебраические дополнения к элементу a_{ij}. Таким образом, обратная матрица A^{-1} для матрицы A существует при условии, что ее определитель не равен нулю, в этом случае говорят, что матрица A **обратима**.

Пример. Найти обратную матрицу для матрицы А:

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & 2 \\ 4 & 1 & 3 \end{pmatrix}$$

Решение. Определитель матрицы найден в предыдущем примере $\det A = 5$.

Найдем алгебраические дополнения:

$$A_{11} = (-1)^{1+1} \begin{vmatrix} \cancel{3} & \cancel{2} & \cancel{1} \\ \cancel{1} & 0 & 2 \\ \cancel{4} & 1 & 3 \end{vmatrix} = (-1)^2 \begin{vmatrix} 0 & 2 \\ 1 & 3 \end{vmatrix} = 0 \cdot 3 - 2 \cdot 1 = -2$$

$$A_{12} = (-1)^{1+2} \begin{vmatrix} \cancel{3} & \cancel{2} & \cancel{1} \\ 1 & \cancel{0} & 2 \\ 4 & \cancel{1} & 3 \end{vmatrix} = (-1)^3 \begin{vmatrix} 1 & 2 \\ 4 & 3 \end{vmatrix} = -(1 \cdot 3 - 2 \cdot 4)$$

$$= 5.$$

$$A_{13} = (-1)^{1+3} \begin{vmatrix} \cancel{3} & \cancel{2} & \cancel{1} \\ 1 & 0 & \cancel{2} \\ 4 & 1 & \cancel{3} \end{vmatrix} = (-1)^4 \begin{vmatrix} 1 & 0 \\ 4 & 1 \end{vmatrix} = 1 \cdot 1 - 0 \cdot 4 = 1.$$

$$A_{21} = (-1)^{2+1}\begin{vmatrix} \mathbf{3} & 2 & 1 \\ \mathbf{1} & \mathbf{0} & \mathbf{2} \\ \mathbf{4} & 1 & 3 \end{vmatrix} = (-1)^3\begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = -(2\cdot 3 - 1\cdot 1)$$
$$= -5.$$

Аналогично вычисляются другие алгебраические дополнения A_{22}=5, A_{23}=5, A_{31}=4, A_{32}= -5, A_{33}= -2.

Составим матрицу алгебраических дополнений и транспонируем ее:

$$\begin{pmatrix} -2 & 5 & 1 \\ -5 & 5 & 5 \\ 4 & -5 & -2 \end{pmatrix}^T = \begin{pmatrix} -2 & -5 & 4 \\ 5 & 5 & -5 \\ 1 & 5 & -2 \end{pmatrix}$$

Найдем обратную матрицу:

$$A^{-1} = \frac{1}{5} \times \begin{pmatrix} -2 & -5 & 4 \\ 5 & 5 & -5 \\ 1 & 5 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{2}{5} & -1 & \frac{4}{5} \\ 1 & 1 & -1 \\ \frac{1}{5} & 1 & -\frac{2}{5} \end{pmatrix}$$

Квадратная матрица Q называется **ортогональной**, если $Q \times Q^T = Q^T \times Q = E$. Для ортогональной матрицы Q, ее обратная матрица равна транспонированной: $Q^T = Q^{-1}$.

Тема 3. Системы линейных уравнений

Система m уравнений с n неизвестными $x_1\ x_2\ \ldots\ x_n$, вида

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

называется ***m*×*n*-системой линейных уравнений**; a_{ij} – коэффициенты системы, b_i – свободные члены (значения) системы. Если все $b_i = 0$, то система называется **однородной**, в противном случае – **неоднородной**. Последовательность чисел $(c_1, c_2,\ldots,c_n)$ называется **решением линейной системы,** если ее элементы, подставленные в заданном порядке вместо неизвестных, удовлетворяют каждому из m уравнений. Совокупность всех решений системы называется **множеством реше-**

ний. Две системы линейных уравнений называются **эквивалентными или равносильными**, если они имеют одинаковые множества решений.

Однородные системы линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0, \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

всегда разрешимы, так как последовательность n чисел (0, 0,…, 0) всегда удовлетворяет всем уравнения системы. Нулевое решение называют **тривиальным решением однородной системы линейных уравнений.** Решение однородных систем линейных уравнений сводится к поиску нетривиальных решений.

Систему линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

можно записать в матричном виде

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_m \end{pmatrix},$$

или же $A \times X = B$, где A – матрица коэффициентов системы, X – столбец неизвестных, B – свободные значения системы. Характер множества решений системы зависит от ранга матрицы коэффициентов системы rang(A) и от ранга так называемой **расширенной матрицы системы** rang ($A|B$):

$$(A|B) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdot & \cdot & \cdot & \cdot & \cdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right)$$

Если для неоднородной системы $AX = B$ выполняется $\text{rang}(A|B) \neq \text{rang}(A)$, то система не имеет решений, то есть **неразрешима**. Говорят также, что система **несовместна** либо **противоречива**. Если же $(A|B) = \text{rang}(A) = r$, то система $AX = B$ разрешима и имеет единственное решение при $r = n$ и бесконечное множество решений при $r < n$.

Эквивалентными преобразованиями системы линейных уравнений являются:

1) перемена местами двух уравнений в системе;

2) умножение какого-либо уравнения системы на действительное число, отличное от нуля;

3) прибавление к одному уравнению другого уравнения, умноженного на произвольное число.

Эквивалентные преобразования в системе линейных уравнений вызывают в матрице коэффициентов A и в расширенной матрице $(A|B)$ преобразования, сохраняющие ранг и приводящие к перестановке строк, умножению строки на число, отличное от нуля, и прибавление к одной строке другой, умноженной на произвольное число. Если преобразовывать матрицы A и $(A|B)$ в матрицы A' и $(A'|B')$, применяя к строкам вышеописанные преобразования, сохраняющие ранг, то системы $AX = B$ и $A'X = B'$ будут эквивалентны. Алгоритм Гаусса состоит в том, чтобы получить матрицы A' и $(A'|B')$ трапециевидной формы:

$$(A'|B') = \left(\begin{array}{ccccccc|c} a_{11} & a_{12} & a_{13} & \dots & a_{1n-2} & a_{1n-1} & a_{1n} & b_1 \\ 0 & a_{22} & a_{23} & \dots & a_{2n-2} & a_{2n-1} & a_{2n} & b_2 \\ 0 & 0 & a_{33} & \dots & a_{3n-2} & a_{3n-1} & a_{3n} & b_3 \\ 0 & 0 & 0 & \dots & a_{4n-2} & a_{4n-1} & a_{4n} & b_4 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & a_{mn-2} & a_{mn-1} & a_{mn} & b_m \end{array}\right)$$

Для простоты изложения представим метод Гаусса на конкретном примере. Решим систему линейных уравнений.

$$\begin{cases} x_1 - 2x_2 + 3x_3 + 2x_5 = 17, \\ 2x_1 + 7x_3 - 5x_4 + 11x_5 = 42, \\ -3x_1 + 9x_2 - 11x_3 - 7x_5 = -64, \\ 7x_1 - 17x_2 + 23x_3 + 15x_5 = 132. \end{cases}$$

Расширенная матрица системы будет иметь вид

$$\begin{array}{c} \\ \text{I} \\ \text{II} \\ \text{III} \\ \text{IV} \end{array}\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 2 & 0 & 7 & -5 & 11 & 42 \\ -3 & 9 & -11 & 0 & -7 & -64 \\ 7 & -17 & 23 & 0 & 15 & 132 \end{array}\right)$$

Для удобства изложения строки обозначены римскими цифрами.

Первый шаг

Обнуляем элементы первого столбца (под первой строкой), используя первую строку:

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 2 & 0 & 7 & -5 & 11 & 42 \\ -3 & 9 & -11 & 0 & -7 & -64 \\ 7 & -17 & 23 & 0 & 15 & 132 \end{array}\right) \begin{array}{c} \\ \rightarrow \\ \text{II} - 2\times\text{I} \\ \text{III} - 3\times\text{II} \\ \text{IV} - 7\times\text{II} \end{array} \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & -1 & -5 & 7 & 8 \\ 0 & 3 & -2 & 0 & -1 & -13 \\ 0 & -3 & 2 & 0 & 1 & 13 \end{array}\right)$$

Из второй строки вычитаем первую, умноженную на 2 (II - 2×I). К третьей строке прибавляем первую, умноженную на 3 (III + 3×I). Из четвертой строки вычитаем первую, умноженную на 7 (IV - 7×I).

Второй шаг

Обнуляем элементы второго столбца (под второй строкой), используя вторую строку:

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & -1 & -5 & 7 & 8 \\ 0 & 3 & -2 & 0 & -1 & -13 \\ 0 & -3 & 2 & 0 & 1 & 13 \end{array}\right) \begin{array}{c} \\ \rightarrow \\ \rightarrow \\ 4\times\text{III} - 3\times\text{II} \\ 4\times\text{IV} - 3\times\text{II} \end{array} \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & -1 & -5 & 7 & 8 \\ 0 & 0 & -11 & 15 & -25 & -76 \\ 0 & 0 & 11 & -15 & 25 & 76 \end{array}\right)$$

Третий шаг

Обнуляем элементы третьего столбца (под третьей строкой), используя третью строку:

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & 1 & -5 & 7 & 8 \\ 0 & 3 & -2 & 0 & -1 & -13 \\ 0 & -3 & 2 & 0 & 1 & 13 \end{array}\right) \quad \begin{array}{c} \to \\ \to \\ \to \\ \text{IV} + \text{III} \end{array} \quad \left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & 1 & -5 & 7 & 8 \\ 0 & 0 & -11 & 15 & -25 & -76 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Нулевую четвертую строку исключим из рассмотрения, тогда расширенная матрица трапециевидной формы системы, эквивалентной исходной, будет иметь вид:

$$\left(\begin{array}{ccccc|c} 1 & -2 & 3 & 0 & 2 & 17 \\ 0 & 4 & 1 & -5 & 7 & 8 \\ 0 & 0 & -11 & 15 & -25 & -76 \end{array}\right)$$

Запишем систему

$$\begin{cases} x_1 - 2x_2 + 3x_3 + 2x_5 = 17, \\ 4x_2 + x_3 - 5x_4 + 7x_5 = 8, \\ -11x_3 + 15x_4 - 25x_5 = -76. \end{cases}$$

В результате имеем три независимых уравнения, содержащие пять неизвестных. В этом случае три переменные выделяют как **базисные,** а оставшиеся две, как **свободные.** В нашем случае в качестве базисных выделим переменные x_1, x_2, x_3, тогда оставшиеся переменные x_4, x_5 будут свободными. Выразим базисные переменные через свободные, перенеся их в правую часть уравнений.

$$\begin{cases} x_1 - 2x_2 + 3x_3 = -2x_5 = 17, \\ 4x_2 + x_3 = 5x_4 - 7x_5 + 8, \\ -11x_3 = -15x_4 + 25x_5 - 76. \end{cases}$$

Разделим третье уравнение на -11, выразив таким образом x_3.

$$\begin{cases} x_1 - 2x_2 + 3x_3 = -2x_5 + 17, \\ 4x_2 + x_3 = 5x_4 - 7x_5 + 8, \\ x_3 = \dfrac{15}{11}x_4 - \dfrac{25}{11}x_5 + \dfrac{76}{11}. \end{cases}$$

Подставив выражение x_3 во втрое уравнение, можно выразить x_4, затем подставив выражения x_3, x_4 в первое уравнение найти x_1. Второй способ – воспользоваться так называемым обратным ходом метода Гаусса. Составим расширенную матрицу последней системы:

$$\begin{array}{c} \text{I} \\ \text{II} \\ \text{III} \end{array}\left(\begin{array}{ccc|ccc} 1 & -2 & 3 & 0 & -2 & 17 \\ 0 & 4 & 1 & 5 & -7 & 8 \\ 0 & 0 & 1 & 15/11 & -25/11 & 76/11 \end{array}\right)$$

Из второй строки вычтем третью (II - III), а из первой третью умноженную на 3 (I - 3 ×III)) получим

$$\left(\begin{array}{ccc|ccc} 1 & -2 & 0 & -45/11 & 53/11 & -41/11 \\ 0 & 4 & 0 & 40/11 & -52/11 & 12/11 \\ 0 & 0 & 1 & 15/11 & -25/11 & 76/11 \end{array}\right)$$

Разделим вторую строку на 4 (II : 4):

$$\left(\begin{array}{ccc|ccc} 1 & -2 & 0 & -45/11 & 53/11 & -41/11 \\ 0 & 1 & 0 & 10/11 & -13/11 & 4/11 \\ 0 & 0 & 1 & 15/11 & -25/11 & 76/11 \end{array}\right)$$

Прибавим к первой строке вторую умноженную на 2 (I + 2 ×II):

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -25/11 & 27/11 & -35/11 \\ 0 & 1 & 0 & 10/11 & -13/11 & 4/11 \\ 0 & 0 & 1 & 15/11 & -25/11 & 76/11 \end{array}\right)$$

Теперь выпишем решение системы

$$\begin{cases} x_1 = -25/11\,x_4 + 27/11\,x_5 - 35/11, \\ x_2 = 10/11\,x_4 - 13/11\,x_5 + 4/11, \\ x_3 = 15/11\,x_4 - 25/11\,x_5 + 76/11, \; x_4 \in R, \; x_5 \in R. \end{cases}$$

Поскольку система имеет бесконечное множество решений, полученное решение называется **общим решением** системы. Подставляя конкретные значения свободных переменных в общее решение системы, будем получать частные решения системы.

Пример. Решить систему линейных уравнений

$$\begin{cases} x_1 - 10x_2 + 3x_3 + 2x_5 = 51, \\ 3x_1 - 26x_2 + 8x_3 + 3x_4 = 141, \\ -5x_1 + 47x_2 - 15x_3 - 5x_4 = -225, \\ 6x_2 + 2x_3 - 7x_5 = -49. \end{cases}$$

Решение. Расширенная матрица системы будет иметь вид

$$\begin{array}{c} \text{I} \\ \text{II} \\ \text{III} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 3 & -26 & 8 & 3 & 141 \\ -5 & 47 & -15 & 5 & -225 \\ 0 & 6 & 2 & -7 & -49 \end{array} \right)$$

Обнуляем элементы первого столбца:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 3 & -26 & 8 & 3 & 141 \\ -5 & 47 & -15 & 5 & -225 \\ 0 & 6 & 2 & -7 & -49 \end{array} \right) \begin{array}{c} \text{I} \\ \text{II} - 3 \times \text{I} \\ \text{III} + 5 \times \text{I} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & -3 & 0 & 5 & 30 \\ 0 & 6 & 2 & -7 & -49 \end{array} \right)$$

Обнуляем элементы второго столбца:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & -3 & 0 & 5 & 30 \\ 0 & 6 & 2 & -7 & -49 \end{array} \right) \begin{array}{c} \text{I} \\ \text{II} \\ 4 \times \text{III} + 3 \times \text{II} \\ 2 \times \text{IV} - 3 \times \text{II} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 7 & -23 & -62 \end{array} \right)$$

Обнуляем элементы третьего столбца:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 7 & -23 & -62 \end{array} \right) \begin{array}{c} \text{I} \\ \text{II} \\ \text{III} \\ 3 \times \text{IV} + 7 \times \text{III} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 0 & 134 & 402 \end{array} \right)$$

Разделив последнюю строку на 134, получим:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 0 & 134 & 402 \end{array} \right) \begin{array}{c} \text{I} \\ \text{II} \\ \text{III} \\ \text{IV}/134 \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 0 & 1 & 3 \end{array} \right)$$

Обнуляем четвертый столбец:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 3 & -12 \\ 0 & 0 & -3 & 29 & 84 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) \begin{array}{c} \text{I} \\ \text{II} - 3 \times \text{IV} \\ \text{III} - 29 \times \text{IV} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 0 & -21 \\ 0 & 0 & -3 & 0 & -3 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

Разделим третью строку на (-3):

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 0 & -21 \\ 0 & 0 & -3 & 0 & -3 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) \begin{array}{c} \text{I} \\ \text{II} \\ \text{III}/(-3) \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 0 & -21 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

Обнуляем третий столбец:

$$\left(\begin{array}{cccc|c} 1 & -10 & 3 & 0 & 51 \\ 0 & 4 & -1 & 0 & -21 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) \begin{array}{c} \text{I} - 3 \times \text{III} \\ \text{II} + \text{III} \\ \text{III} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 0 & 0 & 48 \\ 0 & 4 & 0 & 0 & -20 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

Разделим вторую строку на 4:

$$\left(\begin{array}{cccc|c} 1 & -10 & 0 & 0 & 48 \\ 0 & 4 & 0 & 0 & -20 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) \begin{array}{c} \text{I} \\ \text{II}/4 \\ \text{III} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & -10 & 0 & 0 & 48 \\ 0 & 1 & 0 & 0 & -5 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

Обнулим второй столбец:

$$\left(\begin{array}{cccc|c} 1 & -10 & 0 & 0 & 48 \\ 0 & 1 & 0 & 0 & -5 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right) \begin{array}{c} \text{I} + 10 \times \text{II} \\ \text{II} \\ \text{III} \\ \text{IV} \end{array} \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & -5 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

Выпишем решения системы:

$$\begin{cases} x_1 = -2; \\ x_2 = -5; \\ x_3 = 1; \\ x_4 = 3. \end{cases}$$

Если мы имеем частный случай $n \times n$-системы линейных уравнений $A \times X = B$, такой что $rang(A) = rang(A|B) = n$, то единственное решение X представимо в виде

$$X = A^{-1} \times B.$$

Применяя алгоритм нахождения обратной матрицы A^{-1}, описанный выше, получим:

$$\begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{pmatrix} = [A^{-1}B] = \frac{1}{\det A} \times \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ A_{n1} & A_{n2} & \ldots & A_{nn} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} b_1 \\ b_2 \\ \cdot \\ b_n \end{pmatrix}.$$

Для нахождения решения неоднородной системы линейных уравнений с квадратной матрицей существует **метод Крамера**, который удобен для решения систем небольшого размера. Рассмотрим его на примере *3x3*-системы линейных уравнений:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1; \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_3; \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_1 \end{cases}$$

Матрица системы A и вектор значений B имеют вид:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

Значения неизвестных x_1, x_2, x_3 вычисляются по формулам:

$$x_1 = \frac{\Delta x_1}{\Delta}, \; x_2 = \frac{\Delta x_2}{\Delta}, \; x_3 = \frac{\Delta x_3}{\Delta}$$

где

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \qquad \Delta x_1 = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}$$

$$\Delta x_2 = \begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix} \qquad \Delta x_3 = \begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix}.$$

Пример. Решить систему линейных уравнений методом Крамера

$$\begin{cases} 2x_1 + x_2 + 3x_3 = 9; \\ x_1 - 2x_2 + x_3 = -2; \\ 3x_1 + 2x_2 + 2x_3 = 7. \end{cases}$$

Матрица системы A и вектор значений B имеют вид:

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & -2 & 1 \\ 3 & 2 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 9 \\ -2 \\ 7 \end{pmatrix}$$

$$\Delta = \begin{vmatrix} 2^{+} & 1^{-} & 3^{+} \\ 1 & -2 & 1 \\ 3 & 2 & 2 \end{vmatrix} = 2\begin{vmatrix} -2 & 1 \\ 2 & 2 \end{vmatrix} - 1\begin{vmatrix} 1 & 1 \\ 3 & 2 \end{vmatrix} + 3\begin{vmatrix} 1 & -2 \\ 3 & 2 \end{vmatrix} =$$

$$= 2(-4-2) - 1(2-3) + 3(2-(-6)) = 13.$$

$$\Delta x_1 = \begin{vmatrix} 9^{+} & 1^{-} & 3^{+} \\ -2 & -2 & 1 \\ 7 & 2 & 2 \end{vmatrix} = 9\begin{vmatrix} -2 & 1 \\ 2 & 2 \end{vmatrix} - 1\begin{vmatrix} -2 & 1 \\ 7 & 2 \end{vmatrix} + 3\begin{vmatrix} -2 & -2 \\ 7 & 2 \end{vmatrix} =$$

$$= 9(-4-2) - 1(-4-7) + 3(-4-(-14)) = -13.$$

$$\Delta x_2 = \begin{vmatrix} 2^{+} & 9^{-} & 3^{+} \\ 1 & -2 & 1 \\ 3 & 7 & 2 \end{vmatrix} = 2\begin{vmatrix} -2 & 1 \\ 7 & 2 \end{vmatrix} - 9\begin{vmatrix} 1 & 1 \\ 3 & 2 \end{vmatrix} + 3\begin{vmatrix} 1 & -2 \\ 3 & 7 \end{vmatrix} =$$

$$= 2(-4-7) - 9(2-3) + 3(7-(-6)) = 26.$$

$$\Delta x_3 = \begin{vmatrix} 2^{+} & 1^{-} & 9^{+} \\ 1 & -2 & -2 \\ 3 & 2 & 7 \end{vmatrix} = 2\begin{vmatrix} -2 & -2 \\ 2 & 7 \end{vmatrix} - 1\begin{vmatrix} 1 & -2 \\ 3 & 7 \end{vmatrix} + 9\begin{vmatrix} 1 & -2 \\ 3 & 2 \end{vmatrix} =$$

$$= 2(-14-(-4)) - 1(7-(-6)) + 9(2-(-6)) = 39.$$

$$x_1 = \frac{-13}{13} = 1,\ x_2 = \frac{26}{13} = 2,\ x_3 = \frac{39}{13} = 3.$$

Тема 4. Основные понятия теории графов

Пусть задано некоторое непустое множество

$$V = \{v_1, v_2, \dots, v_n\}$$

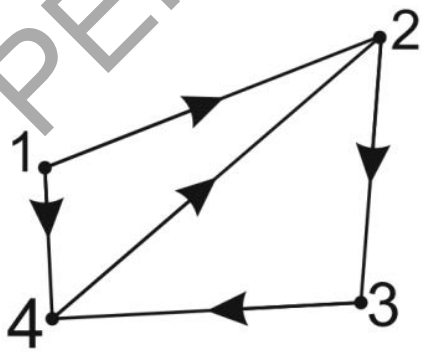
и множество пар различных элементов из V

$$E = \{(v_i, v_j): v_i \in V, v_j \in V, i \in I, j \in J\}.$$

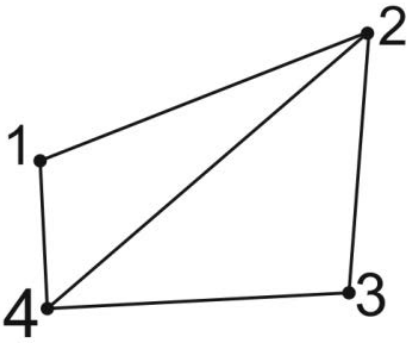
Графом называется пара (*V, E*), состоящая из множества *V*, элементы которого называются вершинами графа и множества *E*, элементы которого называются дугами (ребрами) графа. Другими словами граф – это конечное множество объектов или элементов и связей между этими элементами. Объекты или элементы представляют собой вершины графа, а связи между ними – дуги (ребра) графа.

В качестве примеров графов можно привести следующие: а) люди – вершины графа, ребрами связаны те из них, которые знакомы друг с другом; б) страны – вершины графа, ребрами связаны страны, имеющие общую границу; в) вершинами графа являются ученые и языки, если ученый владеет какими-то языками, то ученый и эти языки соединяются ребрами.

Геометрическое представление графа – это изображение на плоскости вершин графа в виде точек плоскости и дуг (ребер), соединяющих соответствующие вершины в виде линий (рис. 1.2).



а) ориентированный граф



б) неориентированный граф

Рис. 1.2. Геометрическое представление графа

Представим графом страны Южной Америки, считая, что две страны, имеющие общий участок границы, связаны (рис. 1.3). Благодаря такому способу изображения оказывается проще понять, сколько и какие у каждой страны соседи, через какие страны нужно проехать, чтобы попасть из одной страны в другую и т. д.

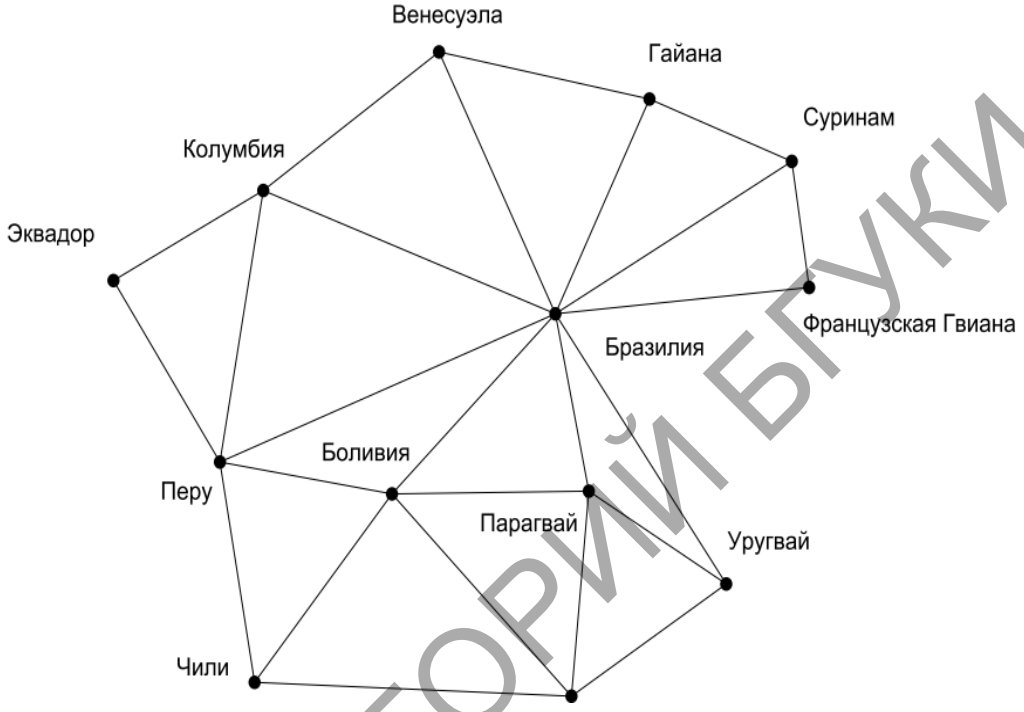


Рис. 1.3. Страны Южной Америки, имеющие общую границу

Ориентированным называется граф, вершины которого соединены ориентированными дугами, изображающимися на схеме ориентированными линиями со стрелкой (рис 1.2*а*)

Неориентированным называется граф, вершины которого соединены неориентированными ребрами, изображающимися на схеме линиями без указания направлений (рис 1.2*б*). То есть наличие соединения (v_i, v_j), означает и наличие соединения (v_j, v_i).

Пример 1. V={1, 2, 3, 4}, E={(l, 2), (2, 3), (3, 4), (1, 4), (4, 2)}.

Смежными называются две вершины графа, соединенные дугой (ребром). Вершины, между которыми нет соединения, называются **несмежными.**

Изолированной называется вершина, не соединенная ни с одной из вершин графа. Вершина, соединенная лишь с одной из вершин графа, называется **висячей.**

Вершины v_i, v_j дуги (ребра) (v_i, v_j) называются **концевыми**. Дуга (ребро), вершины которого совпадают, называется **петлей**.

Вершина и дуга (ребро) **инцидентны**, если вершина является для дуги (ребра) концевой вершиной.

Степенью вершины v_i для неориентированного графа (V, E), называется количество ребер инцидентных данной вершине. Для графа на рисунке 1.2*б* степень вершины 1 равна 2, степень вершины 4 равна 3. Вершина v_i является ***изолированной***, если ее степень равна 0.

Четной называется вершина, степень которой – четное число, в противном случае вершина называется **нечетной**.

Теорема о сумме степеней вершин графа. Сумма степеней всех вершин графа равна удвоенному количеству всех ребер.

Доказательство. Степень вершины – это количество концов ребер, сходящихся в этой вершине. Поэтому сумма степеней всех вершин графа равна количеству всех концов ребер, которые есть в графе. Но у каждого ребра два конца, значит общее количество ребер в два раза меньше количества концов всех ребер, откуда и получаем утверждение теоремы. Поскольку удвоенное количество ребер – четное число, то сумма степеней всех вершин любого графа должна также являться четным числом.

Теорема о числе нечетных вершин графа. Число нечетных вершин любого графа четно.

Доказательство. Если бы нечетных вершин в графе было бы нечетное число, то сумма степеней всех нечетных вершин выражалась бы нечетным числом. А сумма степеней любого количества четных вершин выражается четным числом. Поэтому сумма степеней всех вершин графа будет нечетным числом, что противоречит предыдущему замечанию.

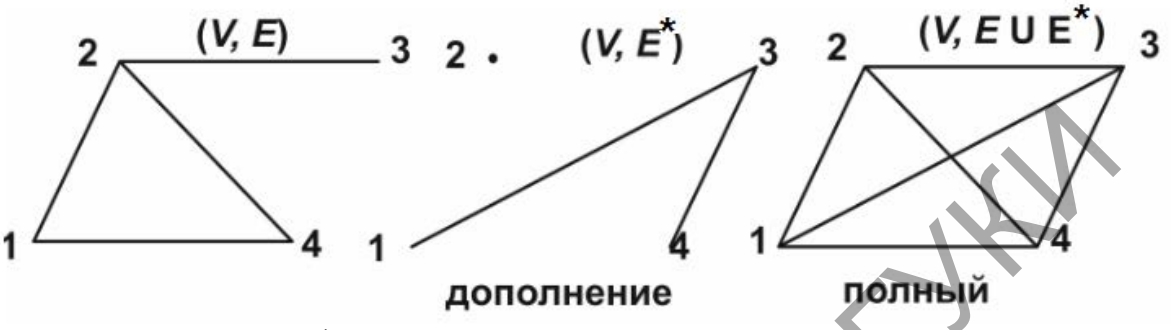
Полным графом называется граф, у которого каждая пара вершин соединена дугой (рис. 1.4).

Поскольку граф состоит из двух множеств (вершины и ребра), то различные операции над множествами естественным образом порождают соответствующие операции над графами.

Объединение двух графов (V_1, E_1) и (V_2, E_2) определяется как граф (V, E), у которого $V = V_1 \cup V_2$, $E = E_1 \cup E_2$.

Пересечение двух графов (V_1, E_1) и (V_2, E_2) определяется как граф (V, E), у которого $V = V_1 \cap V_2$, $E = E_1 \cap E_2$.

Дополнением графа (V, E) называется граф (V, E^*), такой,



что граф (V, $E \cup E^*$) является полным (рис. 1.4).

Рис. 1.4. Граф, дополнение, полный граф

Направленным путем длины n называется последовательность вершин $v_{i_1}, v_{i_2}, \ldots, v_{i_{n+1}}$, в которой каждые две соседние вершины $v_{i_k}, v_{i_{k+1}}$ соединены дугой $(v_{i_k}, v_{i_{k+1}})$. Первую вершину пути называют **начальной вершиной,** последнюю – **конечной.**

Контуром называется направленный путь, начальная и конечная вершина которого совпадают.

Цепью длины n называется последовательность вершин $v_{i_1}, v_{i_2}, \ldots, v_{i_{n+1}}$, в которой каждые две соседние вершины $v_{i_k}, v_{i_{k+1}}$ соединены ребром $(v_{i_k}, v_{i_{k+1}})$. Первая и последняя вершина пути называются концевыми.

Циклом называется цепь, концевые вершины которой совпадают.

Связным называется граф, две любые вершины которого соединены по крайней мере одним путем (цепью). В противном случае граф называется **несвязным.**

Подграфом графа (V, E) называется граф (V^*, E^*), такой что $V^* \subseteq V$, $E^* \subseteq V$.

Компонента связности графа – максимальный связный подграф графа (рис. 1.5).

Мостом графа называется ребро, удаление которого увеличивает число компонент связности (например ребро (6, 7) на рис. 1.5).

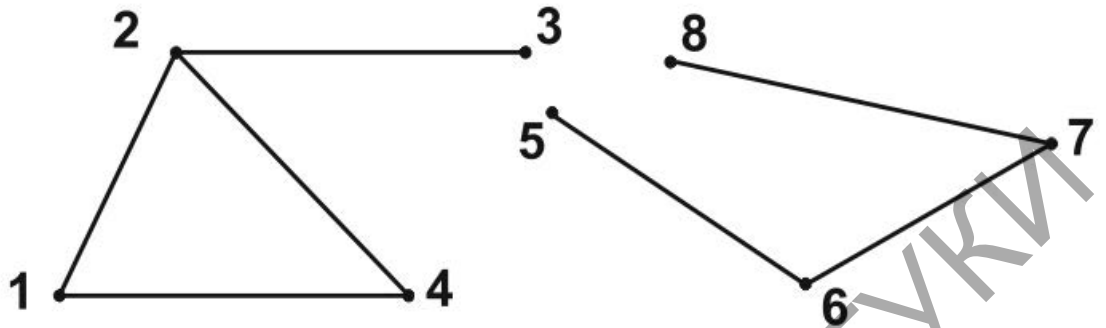


Рис. 1.5. Граф с двумя компонентами связности

Теорема о мосте. Ребро является мостом тогда и только тогда, когда оно не принадлежит ни одному циклу.

Доказательство. Достаточно провести для связного графа. Если ребро (v_i, v_j) принадлежит циклу, то вершины v_i, v_j связаны цепью, не содержащей этого ребра. Этой цепью можно заменить все вхождения ребра (v_i, v_j) в цепи. Следовательно, удаление ребра (v_i, v_j) не нарушает связности вершин.

Обратно, если после удаления ребра (v_i, v_j) получается связный граф, то в нем существуют цепь, не содержащая ребра (v_i, v_j), что значит, что в исходном графе это ребро принадлежит простому циклу.

Эйлерова цепь – это цепь графа, проходящая через каждое ребро графа ровно по одному разу. Аналогично определяется **Эйлеров цикл.**

Теорема об Эйлеровом цикле и Эйлеровой цепи. В связном (неориентированном) графе существует Эйлеров цикл (соответственно Эйлерова цепь) тогда и только тогда, когда в нем нет вершин (соответственно 2 вершины) нечетной степени.

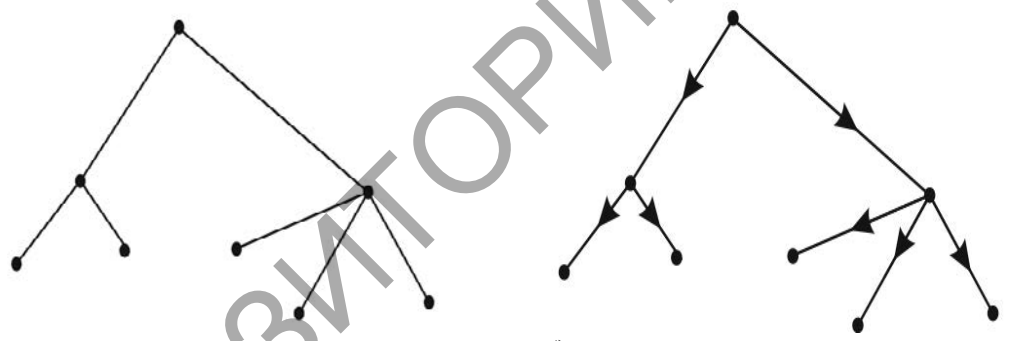
Доказательство. Проведем доказательство для Эйлеровой цепи:

1. Эйлерова цепь проходит каждую промежуточную вершину, используя два инцидентных ей ребра, следовательно степени всех вершин, кроме начала и конца, четны. Аналогично для цикла.

2. Рассмотрим в графе цепь между двумя вершинами нечетной степени. Удалим ее. Граф, возможно, распадется на компоненты связности, в каждой из которых степени всех вершин будут четными, а значит, по индукционному предположению, в каждой из компонент будут существовать Эйлеровы циклы. Будем двигаться в исходном графе по удаленной цепи. Каждый раз, встречая вершину из очередной необойденной компоненты, будем обходить ее по Эйлеровому циклу этой компоненты и продолжать движение по пути.

Деревом называется неориентированный связный граф без циклов (рис. 1.6*а*).

Ориентированный граф называется **деревом**, если он связен и не имеет циклов и единственный путь между вершиной, называемой корнем дерева, и любой другой вершиной графа является направленным путем с началом (концом) в корне дерева (рис. 1.6*б*).



а) неориентированное б) ориентированное

Рис. 1.6. Дерево

Покрывающим деревом для некоторого графа (*V, E*) называется дерево (*V, E*$_t$), содержащее все вершины графа (*V, E*) (рис. 1.7).

Рис. 1.7. Граф и два покрывающих дерева

Остов (каркас) связного графа – дерево, содержащее все вершины графа. Определяется неоднозначно.

Циклический ранг графа – это число $v = m - n + c$, где n – число вершин, m – число ребер, c – число компонент связности графа.

Теорема о цикломатическом ранге графа. Число ребер неориентированного графа, которые необходимо удалить для получения остова, не зависит от последовательности их удаления и равно цикломатическому рангу графа.

Тема 5. Матричное представление графов

Матрицей смежности называется матрица A размерности $n \times n$, где n – число вершин графа, каждый элемент которой $a_{ij} = 1$, если вершины v_i, v_j соединены дугой (ребром) (v_i, v_j) и $a_{ij} = 0$ в противном случае. На рисунке 1.8*а* изображена матрица ориентированного графа, представленного на рис. 1.2*а*, на рис. 1.8*б* – матрица неориентированного графа (рис. 1.2*б*).

$$A_{4\times4} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

а) матрица смежности графа, изображенного на рис. 1.2*а*

$$A_{4\times4} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

б) матрица смежности графа, изображенного на рис. 1.2*б*

Рис. 1.8 Матрица смежности

Матрица инциденций B графа (V, E) с n-числом вершин, m-числом дуг – это матрица размерности $n \times m$, где каждой i-й строке поставлена в соответствие вершина графа v_i и каждому j-му столбцу поставлена в соответствие дуга графа e_j, а элемент $b_{ij} = -1$, если в вершину заходит дуга, $b_{ij} = 1$, если из вершины v_i исходит дуга e_j, и равен 0, если дуга e_j и вершина v_i не являются инцидентными.

Вершина v_j, называется **достижимой** из вершины v_i, если существует направленный путь (цепь) из вершины v_i в вершину v_j.

Матрицей достижимости R называется матрица размерности $n \times n$, где n – число вершин графа, каждый элемент которой $r_{ij} = 1$, если вершина v_j достижима из вершины v_i, и $r_{ij} = 0$ в противном случае, причем вершина v_i считается достижимой из вершины v_i посредством пути длины 0.

$$R_{4\times4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

а) матрица достижимости графа на рис. 1.2*а*

$$R_{4\times4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

а) матрица достижимости графа на рис. 1.2*б*

Рис. 1.9. Матрица достижимости

Обозначим через A^k матрицу достижимости с использованием пути длины k. Таким образом матрица смежности А представляет из себя матрицу достижимости с использованием пути длины 1, а единичная матрица Е – матрицу достижимости с использованием пути длины 0. Для графа на рис. 1.2*а* матрицы A^k будут иметь следующий вид:

$$A^0 = E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad A^1 = A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad A^3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Матрица A^k равна матрице $\underbrace{A \times A \times \ldots \times A}_{k}$, в которой все элементы большие 1, заменены на 1. Таким образом, матрицу достижимости R для графа с n вершинами можно вычислить найдя сумму матриц $E + A^0 + A^1 + A^2 + \ldots + A^{n-1}$, и заменив все элементы результирующей матрицы большие 1 на 1.

Тема 6. Задачи оптимизации на графах

Задачами оптимизации на графах являются задачи определения кратчайших (минимальных) путей между вершинами графа, а также поиск минимальных покрывающих деревьев. При решении таких задач используются взвешенные графы.

Взвешенным называется граф с заданной числовой функцией на вершинах или на дугах (или на тех и других одновременно).

Веса, или значения, дуг и вершин в различных задачах имеют различный смысл. Например, в задачах минимизации расстояний на графах значение дуги интерпретируется как протяженность соответствующей структурной связи системы, описываемой данным графом.

Для заданного графа (V, E) значения весов дуг (ребер) графа $p(v_i, v_j)$ задаются с помощью **матрицы весов** $\boldsymbol{P}$, каждый элемент которой $p_{ij} = p(v_i, v_j)$, если вершины v_i, v_j соединены дугой (ребром) (v_i, v_j) и $p_{ij} = \infty$ в противном случае.

Алгоритм построения покрывающего дерева.

I. Выберем одну из вершин графа (V, E), например v_1. Выбираем ребро (дугу) (v_1, v_{j^*}), соединяющее дерево (V_1, E_1), $V_1 = \{v_1\}$ и $E_1 = \varnothing$, с одной из вершин $V_2 = V \setminus \{v_1\}$ из числа ребер (дуг), инцидентных вершине v_1 с минимальным значением веса

$$p_{1j^*} = \min_{v_j \in V_2} p(v_1, v_j).$$

II. Добавляем вершину v_{j^*} в множество вершин V_1: $V_1 = V_1 \cup \{v_{j^*}\}$ и исключаем ее из множества V_2: $V_2 = V_2 / \{v_{j^*}\}$. Добавляем ребро (дугу) (v_1, v_{j^*}) в множество E_1:

$$V_1 = V_1 \cup V_1 = V_1 \cup E_1 = E_1 \cup (v_1, v_{j^*}).$$

III. Выбираем ребро (дугу) (v_{i^*}, v_{j^*}) с минимальным значением веса из множества ребер инцидентных множеству вершин V_1:

$$p_{i^* j^*} = \min_{\substack{v_i \in V_1, \\ v_j \in V_2}} p(v_i, v_j).$$

IV. Добавляем вершину v_j в множество вершин V_1: $V_1=V_1 \cup \{v_{j*}\}$ и исключаем ее из множества V_2: $V_2=V_2/\{v_{j*}\}$. Добавляем ребро (дугу) (v_i, v_{j*}) в множество E_1: $E_1=E_1 \cup (v_i, v_{j*})$.

Для графа с n вершинами шаги III, IV повторяем до тех пор, пока не будет выбрано $n-1$ ребро.

Минимальным путем из вершины v_s в вершину v_t называется путь, значение которого минимально.

Алгоритм Дейкстры нахождения минимального пути в графе.

В ходе выполнения алгоритма каждой вершине v_j присваивается число q_j, равное значению минимального пути от вершины v_s до вершины v_j.

I. Пометить вершину v_s. Положить $q_s = 0$, $q_j = \infty$ $(j \neq s)$.

II. Положить $i = s$.

III. Для каждой неотмеченной вершины j вычислить значение $q_j = \min\{ q_i, q_i + p_{ij}\}$.

IV. Проверить условие $q_j < \infty$. Если $q_j = \infty$, процедуру закончить, так как $(s\text{-}t)$-пути в исходном графе не существует. Если $q_j < \infty$, отметить ту из вершин v_j, у которой минимальное значение q_j, и отметить дугу, выбранную на данном шаге.

V. Положить $i = j$.

VI. Проверить условие $i = t$. Если условие выполняется, $(s\text{-}t)$-путь найден. Этот путь состоит из отмеченных дуг и является минимальным. При $j \neq t$ перейти к шагу III.

Для нахождения минимальных путей графа от некоторой фиксированной вершины до всех остальных вершин, необходимо модифицировать шаг VI алгоритма следующим образом: проверить, есть ли неотмеченные вершины, если таких вершин нет, то процесс завершить, если неотмеченные вершины есть, то перейти к шагу III. Таким образом можно построить покрывающее **дерево минимальных путей**.

Сеть – это ориентированный граф, в котором выделены две вершины – **источник *s*** и **сток *t***. Из источника дуги могут лишь выходить, а в сток – лишь входить. Каждой дуге (v_i, v_j) сопоставлено положительное целое число c_{ij} – **пропускная способность дуги**.

Потоком в сети называется функция f, заданная на дугах сети, принимающая целые значения и удовлетворяющая условиям:

1) $0 \le f_{ij} \le c_{ij}$,

2) $\sum_{i:v_i \to v_j} f_{ij} = \sum_{l:v_i \to v_l} f_{jl}$, для любой промежуточной вершины j (то есть, неравной s, t).

Число f_{ij} называется величиной потока по дуге (v_i, v_j).

Задача о максимальном потоке заключается в нахождении потока, величина которого **максимальна**.

Пусть некоторый поток f в сети уже имеется, например, поток с нулевыми значениями на всех дугах. **Алгоритм Форда – Фалкерсона** состоит из двух чередующихся процедур – помечивания вершин и изменения потока.

Помечивание вершин. Вершины снабжаются метками, состоящими из двух элементов. Источник s получает условную метку $(-, \infty)$. Пусть имеется некоторое множество помеченных вершин. Выбираем любую из них и обрабатываем ее. Обработка v_i-й вершины с меткой (x, ε) состоит в помечивании из вершины v_i смежных непомеченных вершин по следующему правилу:

если $v_i \to v_j$ и $f_{ij} < c_{ij}$, то вершине v_j присваивается метка $(i^+, \min(\varepsilon, c_{ij} - f_{ij}))$;

если $v_i \leftarrow v_j$ и $f_{ji} > 0$, то вершине v_j присваивается метка $(i^-, \min(\varepsilon, f_{ji}))$.

Затем обрабатывается другая помеченная вершина и так далее. Процесс помечивания заканчивается в двух случаях:

1) ни одну вершину больше нельзя пометить, но сток не помечен. Тогда алгоритм останавливается;

2) сток помечен. Тогда производится изменение потока.

Изменение потока. Пусть сток получил метку (m^+, δ). Тогда прибавляем δ к f_{mt} и переходим в вершину v_m. Общий шаг: если мы находимся в вершине v_j с меткой (i^+, x), то прибавляем δ к f_{ij} и переходим в v_i. А если метка v_j равна (i^-, x), то вычитаем δ из f_{ij} и переходим в v_i. Заметим, что правило формирования меток таково, что после прибавления δ новое значение по-

тока не превышает пропускной способности дуги, а при вычитании δ не получается отрицательной величины. Продолжаем изменение потока, пока не достигнем источника.

Величина измененного потока на δ > 1 больше, чем у исходного потока. Теперь снова переходим к помечиванию. Схема алгоритма имеет следующий вид (рис. 1.10).

Поскольку поток увеличивается не меньше, чем на единицу, а величина потока не может превышать пропускной способности, то алгоритм останавливается после конечного числа шагов.

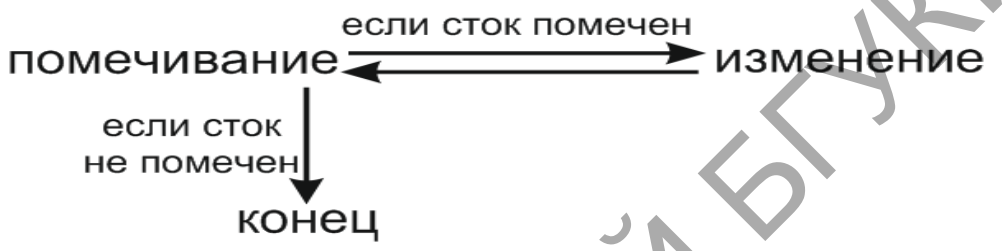


Рис. 1.10. Схема алгоритма Форда – Фалкерсона

Тема 7. Пространство событий

Предметом теории вероятностей является изучение законов, управляющих случайными событиями (явлениями). К основным понятиям теории вероятностей относятся испытание и событие.

Под *испытанием* (*опытом*) понимают реализацию данного комплекса условий, в результате которого непременно произойдет какое-либо *событие*.

Примеры:

1. Брошена монета – испытание. Появление герба или цифры – событие.

2. Произведен выстрел по мишени – испытание. Попадание или промах – событие.

3. В коробке имеются цветные карандаши. Из коробки наудачу берут один карандаш. Извлечение карандаша из коробки – испытание. Появление карандаша определенного цвета – событие.

Случайным событием называется событие, связанное с данным испытанием, которое при осуществлении этого испытания может произойти, а может и не произойти. Прилагательное «случайное» для краткости часто опускают и говорят просто «событие».

Примеры:

1. Брошена игральная кость (кубик, на гранях которого отмечено от одного до шести очков). Выпадение четырех очков – случайное событие.

2. В коробке имеются белые и черные шары. Из коробки наугад берут два шара. Оба шара белые – случайное событие.

Достоверным событием называется событие, которое в результате данного испытания непременно произойдет.

Пример. Брошена игральная кость. Выпадение не более шести очков – достоверное событие.

Невозможным событием называется событие, которое заведомо не произойдет в результате данного испытания.

Примеры:

1. Брошена игральная кость. Выпадение десяти очков – невозможное событие.

2. Камень брошен вверх. Камень остается висеть в воздухе – невозможное событие.

Случайные события обозначаются большими буквами латинского алфавита *A, B, C,* … . Например, событие *A* – попадание в мишени при стрельбе, событие *B* – появление герба при бросании монеты. Достоверное событие будем обозначать буквой *U*, невозможное – *V*.

Отметим, что всякое случайное событие является следствием очень многих причин. Например, выпадение герба или цифры при бросании монеты зависит от силы, с которой брошена монета, ее формы, сплава и многих других причин. Попадание или промах при стрельбе зависят от расстояния до мишени, веса пули (снаряда), от направления и силы ветра и других случайных причин. В связи с этим невозможно заранее предсказать, произойдет единичное событие или нет. Иначе

обстоит дело при изучении многократно повторяющихся событий. Оказывается, что однородные случайные события при многократном повторении подчиняются определенным закономерностям. Изучением этих закономерностей и занимается теория вероятностей.

Пусть произведено испытание, в результате которого возможны события A_1, A_2, …, A_n. События A_1, A_2, …, A_n называются *несовместными*, если осуществление одного из них исключает осуществление других.

Примеры:

1. В ящике имеются стандартные и нестандартные детали. Наудачу берут одну деталь. События A_1 – «появилась стандартная деталь» и A_2 – «появилась нестандартная деталь» являются несовместными событиями.

2. Брошена игральная кость. Событие A_1 – «появление двух очков» и событие A_2 – «появление четного числа очков» совместны, так как появление одного из них не исключает появление другого.

События A_1, A_2, …, A_n называются *равновозможными*, если условия испытания обеспечивают одинаковую возможность осуществления каждого из них.

Примеры:

1. Появление того или иного числа очков при бросании игральной кости есть события равновозможные, так как игральная кость изготавливается из однородного материала и имеет строго симметричную форму.

2. Появление герба и появление цифры при бросании симметричной монеты есть события равновозможные.

События A_1, A_2, …, A_n образуют *полную группу событий*, если в результате данного испытания непременно произойдет хотя бы одно из них.

Пример. В коробке имеются три белых шара, пронумерованных цифрами 1, 2, 3, и пять черных шаров, пронумерованных цифрами 1, 2, … , 5. Из коробки наугад берут один шар. События: A_1 – «появление шара с цифрой 1», A_2 – «появ-

ление шара с цифрой 2», … , A_5 – «появление шара с цифрой 5» – образуют полную группу.

Важную роль играет *полная группа несовместных событий*, т. е. такая группа событий, что в результате данного испытания непременно произойдет одно и притом только одно событие данной группы.

Пример. При бросании игральной кости события: A_1 – «появление одного очка», A_2 – «появление двух очков», … , A_6 – «появление шести очков» – образуют полную группу несовместных событий.

Два случайных события называются *противоположными*, если одно из них происходит в том и только том случае, когда не происходит другое.

Событие, противоположное событию A, обозначают через $\bar{A}$ (читают «не A»).

Примеры:

1. Попадание и промах при выстреле по мишени – противоположные события. Если A – попадание, то $\bar{A}$ – промах.

2. Появление четного числа очков при бросании игральной кости – событие, противоположное появлению нечетного числа очков.

Очевидно, что противоположные события образуют полную группу событий.

Отметим, что любое случайное событие может быть представлено в виде некоторого множества.

Пример. При бросании игральной кости непременно произойдет одно из событий A_1, A_2, …, A_6 . Каждое из этих событий назовем *элементарным событием*. Все элементарные события A_i (i=1, 2, …, 6) *образуют множество элементарных событий* $A=\{A_1, A_2, \ldots, A_6\}$.

Очевидно, что: 1) событие B – «появление четного числа очков» – может быть представлено в виде множества $B = \{A_2, A_4, A_6\}$; 2) событие C – «появление числа очков не большего трех» – может быть представлено множеством $C = \{A_1, A_2, A_3\}$; 3) событие D – «появление числа очков, которое делится на 3» – может быть представлено множеством $D = \{A_3, A_6\}$ и т. д.

Нетрудно заметить, что множества B, C и D являются подмножествами множества элементарных событий A. Таким образом, любое случайное событие может быть представлено подмножеством множества всех элементарных событий данного испытания.

Операции над событиями

Рассмотрим события: A – «появление трех очков при бросании игральной кости», B – «появление нечетного числа очков при бросании игральной кости».

Очевидно, что если произошло событие A, то непременно произошло и событие B. В этом случае говорят «A влечет за собой B» (или «B является следствием A») и записывают $A \subset B$ (или $B \supset A$).

Если события A и B таковы, что $A \subset B$ и $B \supset A$, то они называются *равными* (*равносильными*), при этом пишут $A = B$.

Пример. Брошена симметричная монета. Событие A – «появление герба», событие B – «непоявление цифры». Очевидно, что $A \subset B$ и $B \subset A$ и, следовательно, $A = B$.

Отметим, что событие A может быть частью события B только в том случае, когда элементарные события, представляющие событие A, принадлежат подмножеству элементарных событий, представляющих событие B.

Пример. В коробке имеются пять белых шаров, пронумерованных от 1 до 5, и семь черных шаров, пронумерованных от 6 до 12. Очевидно, что событие A – «появление шара с номером 8» влечет за собой событие B – «появление черного шара». Поэтому $A \subset B$.

Так как события могут быть представлены в виде подмножеств множества элементарных событий, то действия над событиями выполняются аналогично действиям над множествами.

Суммой, или объединением, двух событий A и B называется событие C, состоящее в осуществлении хотя бы одного из событий A или B (безразлично, какого именно, или обоих, если это возможно).

Символически записывают так: $C=A+B$ или $C=A\cup B$.

Сумма событий интерпретируется как объединение (сумма) множеств (подмножеств множества элементарных событий; рис. 1.11).

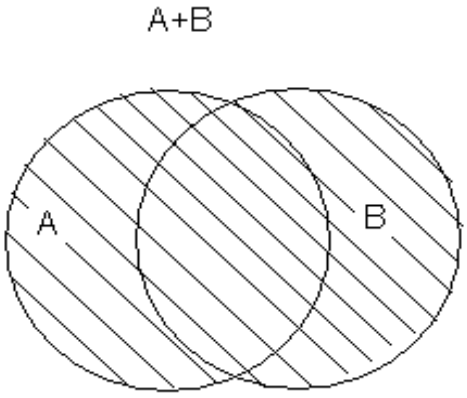


Рис. 1.11. Сумма событий A и B

Суммой, или объединением, нескольких событий A_1, A_2, ..., A_n называется событие C, состоящее в осуществлении хотя бы одного из событий A_1, A_2, ..., A_n.

Символическая запись:

$$C=\sum_{i=1}^{n}A_i \text{ или } C=\bigcup_{i=1}^{n}A_i .$$

Пример. Найти сумму событий: A – «появление одного очка при бросании игральной кости» и B – «появление двух очков при бросании игральной кости».

Суммой $A+B$ является событие C – «появление не больше двух очков при бросании игральной кости», поэтому $A+B=C$.

Если события A и B – несовместные, то сумма $A+B$ является событием, состоящим в осуществлении одного из этих событий, безразлично какого (их совместное осуществление невозможно).

Непосредственно из определения суммы событий вытекают следующие свойства сложения:

1) $A+B=B+A$ (коммутативность);

2) $(A+B)+C=A+(B+C)$ (ассоциативность);

3) $A+\bar{A}=U$.

Произведением, или пересечением, двух событий A и B называется событие C, состоящее в одновременном осуществлении A и B.

Символически произведение записывают так:

$C = AB$ или $C = A \cap B$.

Теоретико-множественная интерпретация произведения событий дана на рис. 1.12.

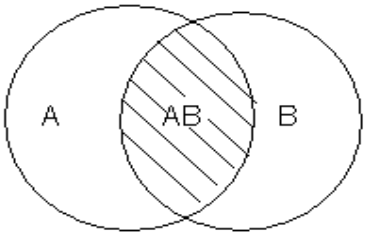


Рис. 1.12. Произведение событий A и B

Произведением, или пересечением, нескольких событий $A_1, A_2, \ldots, A_n$ называется событие C, состоящее в одновременном осуществлении всех событий. Символически представляется следующим образом:

$$C = \prod_{i=1}^{n} A_i \text{ или } C = \bigcap_{i=1}^{n} A_i .$$

Пример. Найти произведение событий A – «студенту попался экзаменационный билет с четным номером» и B – «студенту попался экзаменационный билет с номером, кратным пяти».

Решение. Произведением AB является событие C – «студенту попался экзаменационный билет с номером, кратным десяти», поэтому $AB=C$.

Если события A и B – несовместные, то $AB=V$, т. е. произведение AB – невозможное событие.

Можно показать, что для умножения событий имеют место свойства:

1) $AB = BA$ (коммутативность);

2) $A(BC) = (AB)C$ (ассоциативность);

3) $A(B + C) = AB + AC$ (дистрибутивность);

4) $A\bar{A}=V$.

Тема 8. Способы задания вероятностей

Известно, что случайное событие в результате испытания может произойти, а может и не произойти. Однако объективная возможность различных событий в одном и том же испытании может, вообще говоря, быть различной.

Рассмотрим **пример**. В урне 12 одинаковых, тщательно перемешанных шаров, причем 3 из них белые и 9 – черные. Из урны наудачу вынимают один шар. Очевидно, что возможность появления черного шара «больше», чем возможность появления белого шара. В этом случае говорят: «вероятность появления черного шара больше вероятности появления белого шара».

Под **вероятностью события** понимают численную меру объективной возможности появления этого события.

Поставим своей задачей научиться находить эту численную меру объективной возможности события, т. е. находить вероятность события, причем ограничимся лишь вычислением вероятностей в классической модели.

Под **классической моделью** понимают такое множество элементарных событий, которое образует полную группу несовместных событий и все элементарные события равновозможны.

Например, при бросании игральной кости множество элементарных событий: A_1 – «появление одного очка», A_2 – «появление двух очков», … , A_6 – «появление шести очков» – образуют классическую модель. Вероятность каждого из этих элементарных событий A_i (i = 1, 2, …, 6) считаем равной 1/6.

Рассмотрим теперь события: A – «появление четного числа очков», B – «появление не больше двух очков». Нетрудно заметить, что событие A произойдет, если произойдет по крайней мере одно из событий A_2, A_4, A_6. В этом случае говорят, что событию A благоприятствуют события A_2, A_4, A_6. Очевидно, что событию B благоприятствуют события A_1 и A_2.

То элементарное событие, при котором интересующее нас событие наступит, называется *благоприятствующим* этому событию.

При бросании игральной кости имеем 6 элементарных событий, из них 3 благоприятствуют событию A. Вероятность события A считаем равной 3/6=1/2. Аналогично, вероятность события B равна 2/6=1/3.

Кратко это записывается так:

$$P(A)=\frac{1}{2},\quad P(B)=\frac{1}{3}.$$

Вероятностью $P(A)$ события A называется отношение числа m элементарных событий, благоприятствующих этому событию, к общему числу n равновозможных событий:

$$P(A)=\frac{m}{n}. \qquad (1)$$

Это определение носит название **классического** определения вероятности.

Из (1) следует, что $P(U)=1$ и $P(V)=0$, т. е. вероятность достоверного события равна единице, а вероятность невозможного события равна нулю. Если $A\neq U$ и $A\neq V$, то $0<P(A)<1$.

Итак, вероятность любого события A удовлетворяет неравенствам

$$0\le P(A)\le 1.$$

Рассмотрим ряд примеров непосредственного вычисления вероятностей.

Пример. В коробке 3 белых и 9 черных шаров. Из коробки наугад вынимают один шар. Какова вероятность того, что вынутый шар окажется черным (событие A)?

Решение. Имеем $m = 9$, $n = 12$, и поэтому $P(A)=\frac{9}{12}=\frac{3}{4}$.

Пусть задано пространство элементарных событий E и каждому событию $A\subset E$ поставлено в соответствие единственное число $P(A)$ такое, что:

1) $0\le P(A)\le 1$,

2) для каждой пары несовместных событий A, $B \subset E$ имеет место равенство: $P(A \cup B) = P(A) + P(B)$,

3) $P(E) = 1$.

Тогда говорят, что на событиях в множестве E задана **вероятность**, а число $P(A)$ называется **вероятностью события А**. Такое определение вероятности называется **аксиоматическим.**

В определении **статистической вероятности** используется понятие относительной частоты события A. Относительной частотой W события A называют отношение числа наблюдений m, в которых наблюдается A, к числу всех наблюдений n:

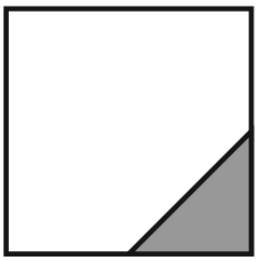
$$W = \frac{m}{n}.$$

Преимущество статистического способа определения вероятности состоит в том, что он опирается на реальный эксперимент. Недостаток – необходимость выполнения большого числа опытов для установления более точного значения относительной частоты, что очень часто связано с материальными затратами.

Недостаток классического определения вероятности состоит в том, что оно неприменимо к испытаниям с бесконечным числом исходов. Для преодоления этого в теории вероятности вводят понятие **геометрической вероятности** – вероятности попадания точки в некоторую область $d \in D$, которая определяется как отношение меры области $mes(d)$ к мере области $mes(D)$:

$$P = \frac{mes(d)}{mes(D)}.$$

Пример. В квадрат со стороной $2a$ наугад брошена точка, найти вероятность того, что она попадет в правый нижний угол квадрата, представляющий из себя треугольник, два катета которого являются половинами сторон квадрата.



Решение. Площадь квадрата равна $4a^2$. Сторона искомого треугольника равна половине стороны квадрата, то есть a, следовательно его площадь треугольника равна $0{,}5a^2$. Чтобы найти вероятность попадания точки в треугольник необходимо его площадь разделить на площадь квадрата:

$$P = 0{,}5a^2/4a^2 = 0{,}125.$$

Элементы комбинаторики

При решении задач теории вероятности нередко возникает необходимость осуществлять перебор возможных вариантов или хотя бы подсчитывать их количество. Таково рода задачи называют *комбинаторными.*

Комбинаторика (комбинаторный анализ) – раздел математики, изучающий дискретные объекты, множества и отношения на множествах. Термин «комбинаторика» происходит от латинского слова «combina», что в переводе на русский язык означает – «сочетать», «соединять».

Знание комбинаторики необходимо представителям самых разных специальностей. С комбинаторными задачами приходится иметь дело физикам, химикам, биологам, информатикам, лингвистам, культурологам и другим специалистам. Комбинаторные методы лежат в основе решения многих задач теории вероятностей и ее приложений.

Термин «комбинаторика» был введен в математический обиход известным немецким ученым Готфридом Вильгельмом Лейбницем (1.07.1646–14.11.1716). В 1666 г. он опубликовал свой труд «Рассуждения о комбинаторном искусстве», в котором ввел специальные символы, термины для подмножеств и операций над ними, нашел все k-сочетания из n элементов и вывел свойства сочетаний.

Комбинаторика рассматривает задачи о перечислении или подсчете количества различных соединений (например, перестановок), образуемых элементами конечных множеств, на которые могут накладываться определенные ограничения, такие как различимость или неразличимость элементов, возможность повторения одинаковых элементов и т. п.

Особая примета комбинаторных задач – вопрос, который можно сформулировать таким образом, что он начинался бы словами:

Сколькими способами..?

Сколько вариантов..?

Для того чтобы решить задачу по комбинаторике, необходимо сначала понять ее смысл, то есть представить мысленно процесс или действие, описанное в задаче. Нужно четко определить тип соединений в задаче, а для этого надо, составив несколько различных комбинаций, проверить, повторяются ли элементы, меняется ли их состав, важен ли порядок элементов.

Если же комбинаторная задача содержит ряд ограничений, налагающихся на соединения, то нужно понять, как влияют или не влияют эти ограничения на соединения. В том случае, если трудно сразу определить какие-либо важные моменты задачи, то неплохо было бы попытаться разобраться в более легкой задаче, например в той, в которой не учитываются ограничения. Если ограничения есть в исходной задаче или же в задаче, в которой рассматривается меньшее количество элементов, тогда проще будет понять принцип образования выборок.

Когда комбинаторная задача состоит из различных комбинаций элементарных задач, то нужно просто разбить задачу на подзадачи.

Количество соединений, образованных несколькими манипуляциями над множеством, подсчитывается согласно правилам *сложения* и *умножения.*

Правило сложения. Если некоторый объект A можно выбрать m способами, а другой объект B можно выбрать n способами, то выбор «либо A, либо B» можно осуществить $(m+n)$ способами.

При использовании правила сложения надо следить, чтобы ни один из способов выбора объекта A не совпадал с каким-либо способом выбора объекта B. Если такие совпадения есть, правило сложения утрачивает силу, и мы получаем лишь $(m + n - k)$ способов выбора, где k – число совпадений.

Пример. Сколько чисел в первой сотне, делящихся на два или на три?

Решение. Каждое второе число в натуральном ряде делится на 2, каждое третье – на 3. Поэтому в первой сотне есть 50 чисел, делящихся на 2, и 33 числа, делящихся на 3. Но среди первых и вторых имеются числа, делящиеся и на 2, и на 3, т. е. делящиеся на 6. Если 100 разделить на 6, то неполное частное будет равняться 16, т. е. 16 чисел в первой сотне делится на 6. Итак, количество чисел в первой сотне, делящихся на 2 или на 3, равно 50+33–16=67.

Правило умножения. Если объект A можно выбрать m способами и если после каждого такого выбора объект B можно выбрать n способами, то выбор пары (A, B) в указанном порядке можно осуществить $m \cdot n$ способами. При этом число способов выбора второго элемента не зависит от того, как именно выбран первый элемент.

Правило умножения справедливо для выбора любого конечного числа объектов. В общем случае его можно сформулировать так:

Если объект A_1 может быть выбран n_1 различными способами, A_2 – n_2 различными способами и т. д., A_k – n_k различными способами, то k объектов A_1, $A_2 \ldots A_k$ в указанном порядке можно выбрать $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ способами.

Примеры:

1. В студенческой группе 25 человек. Сколькими способами в этой группе можно выбрать старосту и профорга?

Решение. Старостой может стать любой из 25 студентов. После выбора старосты на роль профорга могут претендовать 24 оставшихся студентов. Таким образом, всего есть 25·24=600 различных вариантов выбора.

2. В саквояжах часто применяют секретные замки, которые открываются, когда набран шифр. В замке имеется несколько дисков. Пусть на каждом диске имеется 12 букв, а секретное слово-шифр состоит из 4 букв. Вычислите, сколько существует вариантов для набора шифра.

Решение. Для набора первой буквы слова существует 12 способов и набор буквы на следующем диске не зависит от того, какая буква была набрана на предыдущем диске. Поэтому, применяя правило умножения, получаем 12·12·12·12= 20736 вариантов набора шифра.

Перестановки

Для формулировки и решения комбинаторных задач используют различные модели комбинаторных соединений. ***Комбинаторные соединения*** – это комбинации из каких-либо элементов. В комбинаторных соединениях может играть существенную роль или порядок элементов, или их состав, или то и другое. В зависимости от этого комбинаторные соединения имеют определенное название. Основными типами комбинаторных соединений являются: ***перестановки***, ***размещения*** и ***сочетания***.

Возьмем n различных элементов: a_1, a_2, $a_3 \ldots a_n$. Будем переставлять их всеми возможными способами, сохраняя их количество и меняя лишь порядок их расположения. Каждая из полученных таким образом комбинаций называется ***перестановкой***. Общее количество перестановок из n элементов обозначается P_n. Это число равно произведению всех целых чисел от 1 до n:

$$P_n = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n! \ .$$

Символы $n!$ (читаются *n-факториал*) – сокращенная запись произведения: $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

Эта функция определяется для значения n, равного 0 и 1, следующим образом: 0! = 1; 1! = 1.

Пример 1. Найти число перестановок из трех элементов: a, b, c.

Решение. В соответствии с приведенной выше формулой P_n получим, что $P_3 = 1 \cdot 2 \cdot 3 = 6$. Действительно, мы имеем 6 перестановок: *abc, acb, bac, bca, cab, cba.*

Пример 2. Сколькими способами можно расставить на пятиместной полке пять различных книг?

Решение. На первое место можно поставить любую из пяти книг, на второе место – любую из четырех оставшихся книг, на третье – любую из трех оставшихся книг и т. д. Таким образом, всего получается 5·4·3·2·1=120 способов.

Перестановки с повторениями – комбинаторные соединения, в которых среди образующих элементов имеются одинаковые. В таких соединениях участвуют несколько типов объектов, причем имеется некоторое количество объектов каждого типа. Поэтому в выборках встречаются одинаковые элементы.

Рассмотрим перестановку

$$\underbrace{a,a,...,a}_{n_1};\underbrace{b,b,...,b}_{n_2};...;\underbrace{z,z,...,z}_{n_k}$$

Элементы 1-го типа можно переставлять $n_1!$ способами. Поскольку эти элементы одинаковые, получим ту же перестановку из n элементов. Также ничего не изменяют $n_2!$ перестановок элементов 2-го типа, … , $n_k!$ перестановок k-го типа. Перестановки элементов 1-го типа, 2-го типа и т. д. можно выполнять независимо друг от друга. Поэтому одинаковые элементы любой перестановки из n элементов можно переставлять $n_1!\ n_2!\ \dots\ n_k!$ способами так, что она не изменяется. Таким образом, совокупность всех перестановок содержит $n_1!\ n_2!\ \dots\ n_k!$ одинаковых перестановок. Отсюда получаем, что количество различных перестановок с повторениями определяется следующей формулой:

$$P_n(n_1, n_2, ..., n_k) = \frac{n!}{n_1! n_2! ... n_k!}.$$

Пример. Сколько перестановок можно образовать из букв слова «задача»?

Решение. Если бы в слове все буквы были различными, то число всех перестановок равнялось бы 6!=720. Но в слове «задача» содержится три одинаковых буквы «а». Поэтому число всех перестановок из букв слова «задача» равно $\frac{6!}{3!} = 120.$

Размещения и сочетания

Будем составлять группы из m различных элементов, взятых из множества, состоящего из n элементов, располагая эти m взятых элементов в различном порядке. Полученные комбинации называются ***размещениями*** из n элементов по m.

Их общее количество обозначается A_n^m. Найдем, чему равняется A_n^m.

Первый элемент для размещения можно выбрать n различными способами. Для размещения второго элемента остается n-1 возможность и т. д. Последний m-й элемент размещают после извлечения $(m-1)$-го элемента, т. е. из $[n-(m-1)]$ оставшихся элементов. Применяя правило умножения, получим, что число размещений из n элементов по m равно

$$A_n^m = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot [n-(m-1)]$$

Полученную формулу иногда записывают в следующем, более кратком виде

$$A_n^m = \frac{n!}{(n-m)!}$$

Очевидно, что из этой формулы можно получить предыдущую формулу делением ее числителя и знаменателя на величину $(n\text{-}m)!$

Пример. Найти число размещений из четырех элементов *a, b, c, d* по два.

Решение. В соответствии с формулой получим: $A_4^2 = 4 \cdot 3 = 12$.

Вот эти размещения: *ab, ba, ac, ca, ad, da, bc, cb, bd, db, cd, dc.*

Будем составлять группы из m различных элементов, взятых из множества, состоящего из n элементов, не принимая во внимание порядок расположения этих m элементов. Тогда мы получим ***сочетания*** из n элементов по m.

Их общее количество обозначается C_n^m. Вычислим это количество.

Из каждой неупорядоченной выборки, состоящей из различных элементов, можно получить $m!$ упорядоченных выбо-

рок. По правилу умножения число всех упорядоченных выборок из *n* по *m* равно

$$n(n-1)(n-2)...(n-m+1) = C_n^m = m!$$

Таким образом,

$$C_n^m = \frac{n(n-1)(n-2)...(n-m+1)}{m!}.$$

Заметим, что можно составить только одно сочетание из *n* элементов по *n*, которое содержит все *n* элементов. Формула числа сочетаний дает это значение, если только принять, что 0!=1. Ранее мы отмечали, что эта формула есть определение 0!.

В соответствии с этим определением получим:

$$C_n^n = C_n^0 = 1.$$

Если в формуле для вычисления C_n^m числитель и знаменатель умножить на (*n*-*m*)!, то получим другую формулу

$$C_n^m = \frac{n!}{m!\cdot(n-m)!}.$$

Из этой формулы ясно, что

$$C_n^m = C_n^{n-m}.$$

Общее число сочетаний можно вычислить, пользуясь и другим выражением:

$$C_n^m = A_n^m / P_m.$$

Пример. Найдите число сочетаний из пяти элементов: *a, b, c, d, e* по три.

Решение.

$$C_5^3 = \frac{5\cdot 4\cdot 3}{3!} = 10.$$

Эти сочетания: *abc, abd, abe, acd, ace, ade, bcd, bce, bde, cde.*

Сочетания с повторениями – комбинаторные соединения из *n* элементов по *m*, составленные из этих элементов без учета порядка с возможностью многократного повторения пред-

метов. Найти количество сочетаний с повторениями можно по формуле

$$\widetilde{C}_n^m = C_{n+m-1}^m.$$

Покажем, что эта формула является верной. Каждой неупорядоченной выборке с возвращением из n элементов по m можно поставить в соответствие последовательность из n-1 нулей и m единиц, т. е. последовательность длиной $n+m-1$. Верно и обратное утверждение: каждая последовательность из n-1 нулей и m единиц однозначно определяет такую выборку. Между выборками и последовательностями имеется взаимно однозначное соответствие. Поэтому число неупорядоченных выборок без возвращения из n элементов по m равно числу таких последовательностей, что, в свою очередь, равно числу способов выбора m мест для единиц или, что то же самое, n-1 мест для нулей из общего числа $n+m-1$ мест. Это и требовалось доказать.

Пример. Подсчитайте количество костей в домино.

Решение. Каждую кость домино можно рассматривать как выборку, образованную из семи элементов 0, 1, 2, 3, 4, 5, 6, содержащую два элемента. Эти выборки являются выборками с возвращением (среди костей домино есть дубли 0 : 0, 1 : 1 и т. д.) и неупорядоченные (кости 0 : 1 и 1 : 0 неразличимы). Поэтому для подсчета числа костей в домино можно применить формулу числа сочетаний с повторениями

$$\widetilde{C}_7^2 = C_{7+2-1}^2 = C_8^2 = \frac{8 \cdot 7}{2} = 28.$$

Бином Ньютона

Бином Ньютона – это формула, представляющая выражение $(a+b)^n$ при положительном целом n в виде многочлена:

$$(a+b)^n = a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + C_n^3 a^{n-3} b^3 + \ldots + C_n^{n-1} a b^{n-1} + b^n.$$

Числа $C_n^1, C_n^2, C_n^3, \ldots, C_n^{n-1}$ называются биномиальными коэффициентами. Заметим, что сумма показателей степеней для a и b постоянна и равна n.

Пример. Запишите формулу суммы кубов двух чисел.

Решение. Запишем формулу бинома Ньютона для n, равного 3, и вычислим биномиальные коэффициенты:

$$(a+b)^3 = a^3 + C_3^1 a^2 b + C_3^2 ab^2 + b^3 = a^3 + \frac{3!}{1!\cdot 2!} a^2 b + \frac{3!}{2!\cdot 1!} ab^2 + b^3 =$$
$$= a^3 + 3a^2 b + 3ab^2 + b^3.$$

Биномиальные коэффициенты можно вычислить, применяя только сложение, если пользоваться следующей схемой. В верхней строке пишем две единицы. Все последующие строки начинаются и заканчиваются единицей. Промежуточные числа в этих строках получаются суммированием соседних чисел из предыдущей строки. Эта схема называется ***треугольником Паскаля*** (рис. 1.13).

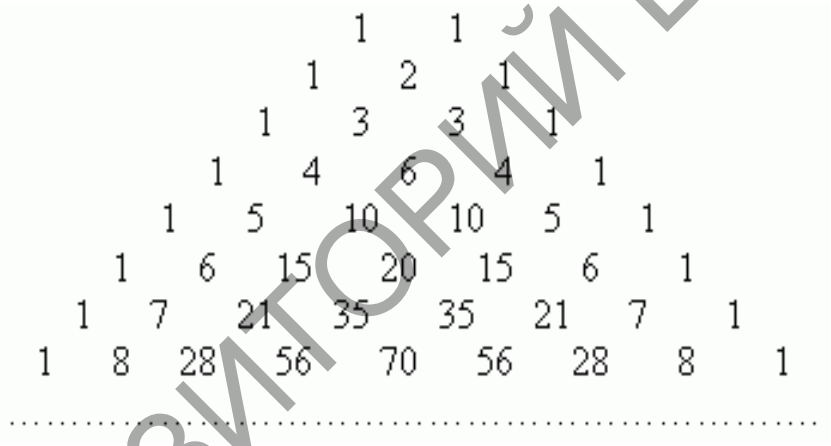


Рис. 1.13. Треугольник Паскаля

Первая строка в этой таблице содержит биномиальные коэффициенты для n = 1; вторая – для n = 2; третья – для n = 3 и т. д. Поэтому, если необходимо, например, разложить выражение $(a+b)^7$, мы можем получить результат моментально, используя треугольник Паскаля:

$$(a+b)^7 = a^7 + 7a^6 b + 21a^5 b^2 + 35a^4 b^3 + 35a^3 b^4 + 21a^2 b^5 + 7ab^6 + b^7 .$$

Биномиальные коэффициенты обладают следующими свойствами:

1. Сумма коэффициентов разложения $(a+b)^n$ равна 2^n .

Для доказательства достаточно положить $a=b=1$. Тогда в правой части разложения бинома Ньютона мы будем иметь сумму биномиальных коэффициентов, а слева $(1+1)^n=2^n$.

2. Коэффициенты членов, равноудаленных от концов разложения, равны. Это свойство следует из соотношения:

$$C_n^k = C_n^{n-k}.$$

3. Сумма коэффициентов четных членов разложения равна сумме коэффициентов нечетных членов разложения; каждая из них равна 2^{n-1}.

Для доказательства воспользуемся биномом: $(1-1)^n = 0^n = 0$. Здесь четные члены имеют знак «+», а нечетные – «–». Так как в результате разложения получается 0, то, следовательно, суммы их биномиальных коэффициентов равны между собой, поэтому каждая из них равна: 2^n: $2=2^{n-1}$, что и требовалось доказать.

Формулу бинома Ньютона можно использовать для приближенного вычисления степеней. Положив в формуле бинома Ньютона $a=1$, $b=x$, получим

$$(1+x)^n = 1 + C_n^1 x + C_n^2 x^2 + \ldots + C_n^{n-1} x^{n-1} + x^n.$$

Если значение x мало, то значения x^2, x^3, …, x^n тем более малы. Поэтому если в последнем равенстве отбросить все слагаемые, начиная с третьего, и учесть, что $C_n^1 = n$, то получим приближенную формулу

$$(1 + x)^n \approx 1 + nx.$$

При малых значениях x она дает удовлетворительный результат.

Тема 9. Операции над вероятностями

Теорема 1. Вероятность суммы двух несовместных событий A и B равна сумме вероятностей этих событий, т. е.

$$P(A+B) = P(A) + P(B).$$

Доказательство. Пусть n – общее число равновозможных несовместных элементарных событий испытания, в результате которого может произойти одно из событий A или B, m_A – число элементарных событий, благоприятствующих событию A, m_B – число элементарных событий, благоприятствующих событию B. Тогда, так как события A и B несовместны, имеем:

$$P(A+B)=\frac{m_A+m_B}{n}=\frac{m_A}{n}+\frac{m_B}{n}=P(A)+P(B),$$

что и требовалось доказать.

Следствия:

1. Вероятность суммы нескольких событий A_1, A_2, ... , A_n равна сумме вероятностей этих событий, т. е.

$$P(A_1+A_2+\ldots+A_n)=P(A_1)+P(A_2)+\ldots+P(A_n).$$

Это следствие получается из теоремы 1 применением метода математической индукции.

2. Если события A_1, A_2, ..., A_n несовместны и образуют полную группу, то сумма их вероятностей равна единице:

$$P(A_1)+P(A_2)+\ldots+P(A_n)=1.$$

3. Сумма вероятностей противоположных событий равна единице, т. е.

$$P(A)+P(\bar{A})=1.$$

Это непосредственно следует из формулы пункта 2, так как противоположные события образуют полную группу.

Примеры:

1. Военный летчик получил задание уничтожить два рядом расположенных склада боеприпасов противника. На борту самолета осталась лишь одна бомба. Вероятность попадания в первый склад равна 0,225, во второй – 0,325. В результате детонации любое попадание взрывает оба склада. Какова вероятность того, что склады будут уничтожены?

Решение. События A – «попадание в первый склад» и B – «попадание во второй склад» несовместны, поэтому вероятность попадания хотя бы в один из складов

$$P(A + B) = P(A) + P(B) = 0{,}225 + 0{,}325 = 0{,}55.$$

2. На заочное отделение университета поступают контрольные работы по математике из городов A, B и C. Вероятность поступления контрольной работы из города A равна 0,6, из города B – 0,1. Найти вероятность того, что очередная контрольная работа поступит из города C.

Решение. События «контрольная работа поступила из города A», «контрольная работа поступила из города B» и «контрольная работа поступила из города C» образуют полную группу, поэтому сумма их вероятностей равна единице:

$$0{,}6 + 0{,}1 + p = 1 \Leftrightarrow p = 0{,}3.$$

3. Вероятность того, что день будет ясным, $p = 0{,}85$. Найти вероятность q того, что день будет облачным.

Решение. События «день ясный» и «день облачный» противоположные, поэтому

$$p + q = 1 \Leftrightarrow q = 1 - p = 1 - 0{,}85 = 0{,}15.$$

Теорема. Если события A и B совместны, то вероятность их суммы выражается формулой

$$P(A + B) = P(A) + P(B) - P(AB),$$

т. е. вероятность суммы двух совместных событий равна сумме вероятностей этих событий без вероятности их произведения (совместного осуществления).

Доказательство. Пусть m – число равновозможных элементарных событий, благоприятствующих событию A, k – число равновозможных элементарных событий, благоприятствующих событию B. Допустим, что среди $m+k$ элементарных событий содержится l таких, которые благоприятствуют как

событию A, так и событию B. Тогда, если n – общее число равновозможных элементарных событий,

$$P(A)=\frac{m}{n},\qquad P(B)=\frac{k}{n},\qquad P(AB)=\frac{l}{n}.$$

Таким образом, событие $A+B$ состоит в том, что произошло или событие A, или событие B, или и то и другое, то ему благоприятствуют $m+k-l$ элементарных событий. Поэтому

$$P(A+B)=\frac{m+k-l}{n}=\frac{m}{n}+\frac{k}{n}-\frac{l}{n},$$

или

$$P(A+B)=P(A)+P(B)-P(AB),$$

что и требовалось доказать.

Пример. Найти вероятность того, что при бросании двух игральных костей хотя бы один раз выпадет 6 очков.

Решение. Обозначим события:

A – «выпадение шести очков при бросании первой игральной кости»;

B – «выпадение шести очков при бросании второй игральной кости».

Так как события A и B совместны, то

$$P(A+B)=P(A)+P(B)-P(AB).$$

Но $P(A)=\frac{1}{6}, P(B)=\frac{1}{6}, P(AB)=\frac{1}{36}$, поэтому

$$P(A+B)=\frac{1}{6}+\frac{1}{6}-\frac{1}{36}=\frac{11}{36}.$$

Умножение

Два события A и B называются **независимыми**, если вероятность одного из них не зависит от того, произошло или не произошло другое.

Пример. Игральная кость брошена два раза. Вероятность появления трех очков в первом испытании (событие A) не зависит от появления или непоявления трех очков во втором испытании (событие B). Аналогично, вероятность появления трех очков во втором испытании не зависит от результата первого испытания. Следовательно, события A и B – независимые.

Теорема. Вероятность произведения двух независимых событий равна произведению вероятностей этих событий, т. е.

$$P(AB)=P(A)\cdot P(B).$$

Доказательство. Пусть n_1 – число равновозможных элементарных событий испытания, в результате которого событие A может произойти или не произойти; m_1 – число элементарных событий, благоприятствующих событию A ($m_1 \le n_1$), n_2 – число равновозможных элементарных событий испытания, в результате которого может произойти событие B, m_2 – число элементарных событий, благоприятствующих событию B ($m_2 \le n_2$).

Нетрудно заметить, что общее число элементарных событий испытания, в результате которого может произойти (или не произойти) событие AB, равно $n_1 \cdot n_2$, так как события A и B независимы, то число элементарных событий, благоприятствующих событию AB, равно $m_1 \cdot m_2$. Поэтому

$$P(AB)=\frac{m_1 m_2}{n_1 n_2}=\frac{m_1}{n_1}\cdot\frac{m_2}{n_2}=P(A)\cdot P(B),$$

что и требовалось доказать.

Если имеем n попарно независимых событий $A_1, A_2, \ldots, A_n$, то можно доказать, что

$$P(A_1 A_2 \ldots A_n)=P(A_1)\cdot P(A_2)\cdot \ldots \cdot P(A_n).$$

Пример. Два стрелка стреляют по одной и той же цели. Вероятность попадания в цель для первого стрелка равна 0,9, для второго – 0,8. Найти вероятность того, что оба стрелка попадут в цель.

Решение. Обозначим события: A – «попадание в цель первым стрелком», B – «попадание в цель вторым стрелком». Так как события A и B независимы, то

$$P(AB) = P(A) \cdot P(B) = 0{,}9 \cdot 0{,}8 = 0{,}72.$$

Два события A и B называются **зависимыми**, если вероятность одного из них зависит от того, произошло или не произошло другое.

Пример. В ящике имеется 90 стандартных деталей и 10 нестандартных. Из ящика наудачу берут одну за другой две детали. Вероятность появления стандартной детали при первом испытании (событие A) равна

$$P(A)=\frac{90}{100} = 0{,}9.$$

Вероятность появления стандартной детали при втором испытании (событие B) зависит от результата первого испытания: если в первом испытании событие A произошло, то

$$P(B)=\frac{90}{99}=\frac{10}{11}.$$

Следовательно, события A и B – зависимые.

Вероятность события A, вычисленная при условии, что событие B произошло, называется **условной вероятностью события A при условии B** и обозначается $P(A \mid B)$.

Пример. В коробке a белых и b черных шаров. Из коробки наудачу последовательно вынимают два шара. Найти вероятность того, что второй шар окажется черным при условии, что первый шар был черным.

Решение. Обозначим события: A – «первый шар черный»; B – «второй шар черный».

Если произошло событие A, то в урне осталось всего $a = b - 1$ черных. Поэтому условная вероятность события B при условии, что произошло событие A, есть:

$$P(B \mid A) = \frac{b-1}{a+b-1}.$$

Для зависимых событий справедлива следующая теорема.

Теорема. Вероятность произведения двух зависимых событий A и B равна произведению вероятности одного из этих событий на условную вероятность другого, вычисленную при условии, что первое событие произошло:

$$P(AB) = P(A) \cdot P(B \mid A) \Leftrightarrow P(AB) = P(B) \cdot P(A \mid B). \quad (*)$$

В случае n произвольных событий A_1, A_2, ... , A_n справедлива формула

$$P(A_1 A_2 \ \ldots A_n) = P(A_1) \cdot P(A_2 \mid A_1) \cdot P(A_3 \mid A_1 A_2) \cdot \ldots \cdot P(A_n \mid A_1 A_2 \ldots A_{n-1}),$$

где $P(A_n \mid A_1 A_2 \ldots A_{n-1})$ – вероятность события A_n, вычисленная при условии, что произошли события A_1, A_2, ..., A_{n-1}.

Примеры:

1. В цехе изготавливаются детали на трех станках. Вероятность изготовления на первом станке равна 0,6. Вероятность появления годной детали на первом станке равна 0,8. Найти вероятность того, что годная деталь изготовлена на первом станке.

Решение. Обозначим события: A – «деталь изготовлена на первом станке», B – «деталь годная».

Имеем: $P(A)$=0,6, $P(B|A)$=0,8. По первой формуле (*) находим:

$$P(AB) = P(A) \cdot P(B|A) = 0{,}6 \cdot 0{,}8 = 0{,}48.$$

2. В ящике находится 7 деталей первого сорта, 5 – второго сорта и 3 – третьего. Из ящика последовательно вынимают три детали. Найти вероятность того, что первая наугад вынутая деталь окажется первого сорта (событие A_1), вторая деталь – второго сорта (событие A_2) и третья деталь – третьего сорта (событие A_3).

Решение. Очевидно, что

$$P(A_1)=\frac{7}{15},\ P(A_2 \mid A_1)=\frac{5}{14}\ \text{и}\ P(A_3 \mid A_1A_2)=\frac{3}{13}.$$

По формуле (*) находим

$$P(A_1A_2A_3)=P(A_1)\cdot P(A_2 \mid A_1)\cdot P(A_3 \mid A_1A_2)=\frac{7}{15}\cdot\frac{5}{14}\cdot\frac{3}{13}=\frac{1}{26}.$$

Формула полной вероятности

Операции над вероятностями представляют собой правила, служащие для вычисления вероятностей случайных событий через вероятности элементарных событий. При решении многих задач оказывается полезным одно следствие из этих правил, известное под названием ***формулы полной вероятности.*** Выведем эту формулу.

Пусть событие A может произойти только с одним из событий H_1, H_2, …, H_n, образующих полную группу несовместных равновозможных событий. Тогда вероятность события A вычисляется по формуле полной вероятности:

$$P(A)=P(H_1)\cdot P(A \mid H_1)+P(H_2)\cdot P(A \mid H_2)+\ldots+P(H_n)\cdot P(A \mid H_n),$$

или

$$P(A)=\sum_{i=1}^{n}P(H_i)\cdot P(A \mid H_i). \qquad (**)$$

В самом деле, так как событие A может произойти только с одним из событий $H_1, H_2, \ldots, H_n$, образующих полную группу, то

$$A=AH_1+AH_2+\ldots+AH_n.$$

Из несовместности событий $H_1, H_2, \ldots, H_n$ следует несовместность событий $AH_1, AH_2, \ldots, AH_n$. Поэтому

$$P(A)=P(AH_1)+P(AH_2)+\ldots+P(AH_n).$$

Применив к каждому слагаемому последнего равенства правило умножения вероятностей $P(AH_i)=P(H_i)\cdot P(AH_i)$, получим требуемую формулу (**).

Пример. В учебных мастерских на станках *a*, *b* и *c* изготавливают соответственно 25, 35 и 40 % всех деталей. В их продукции брак составляет соответственно 15, 12 и 6 %. Найти вероятность того, что наугад взятая деталь дефектна.

Решение. Обозначим события: A – «наугад взятая деталь дефектна», H_1 – «деталь изготовлена на станке *a*», H_2 – «деталь изготовлена на станке *b*», H_3 – «деталь изготовлена на станке *c*».

Очевидно, что события H_1, H_2, H_3 образуют полную группу и $P(H_1) = 0{,}25$, $P(H_2) = 0{,}35$, $P(H_3) = 0{,}4$. Кроме того, числа 0,15; 0,12; 0,06 (15 %, 12 %, 6 %) являются условными вероятностями события A при выполнении событий (гипотез) H_1, H_2, H_3 соответственно, т. е.

$$P(A|H_1)=0{,}15,\ P(A|H_2,)=0{,}12,\ P(A|H_3)=0{,}06.$$

По формуле (1) находим

$$P(A)=\sum_{i=1}^{3}P(H_i)\cdot P(A\mid H_i)=P(H_1)\cdot P(A\mid H_1)+P(H_2)\cdot P(A\mid H_2)+$$

$$+P(H_3)\cdot P(A\mid H_3)=0{,}25\cdot 0{,}15+0.35\cdot 0{,}12+0{,}4\cdot 0{,}06=0{,}1035.$$

Формула Бейеса

С помощью формулы полной вероятности можно доказать **формулу Бейеса:**

$$P(H_i\mid A)=\frac{P(H_i)\cdot P(A\mid H_i)}{P(H_1)\cdot P(A\mid H_1)+P(H_2)\cdot P(A\mid H_2)+\ldots+P(H_n)\cdot P(A\mid H_n)}.$$

Доказательство. Из теоремы о вероятности произведения двух зависимых событий A и B имеем

$$P(AH_i)=P(H_i\mid A)\cdot P(A)\ \Leftrightarrow\ P(H_i\mid A)=\frac{P(AH_i)}{P(A)}\ \Leftrightarrow\ P(H_i\mid A)=\frac{P(H_i)\cdot P(A\mid H_i)}{P(A)}.$$

Заменив в последнем равенстве $P(A)$ его значением из формулы (*), получаем формулу Бейеса.

Формула Бейеса позволяет переоценивать вероятности гипотез, принятые до испытания, по результатам уже произведенного испытания.

Пример. Имеются три одинаковые по виду урны. В первой урне 15 белых шаров, во второй – 10 белых и 5 черных, в третьей – 15 черных шаров. Из выбранной наугад урны вынули белый шар. Найти вероятность того, что шар вынут из первой урны.

Решение. Введем обозначения: событие А – «появление белого шара»; гипотезы: H_1 – «выбор первой урны», H_2 – «выбор второй урны», H_1 – «выбор третьей урны».

Имеем:

$$P(H_1) = P(H_2) = P(H_3) = \frac{1}{3}.$$

$$P(A \mid H_1) = 1, \quad P(A \mid H_2) = \frac{10}{15} = \frac{2}{3}, \quad P(A \mid H_3) = 0.$$

Искомую вероятность находим по формуле (2):

$$P(H_1 \mid A) = \frac{P(H_1) \cdot P(A \mid H_1)}{P(H_1) \cdot P(A \mid H_1) + P(H_2) \cdot P(A \mid H_2) + P(H_3) \cdot P(A \mid H_3)} =$$

$$= \frac{\frac{1}{3} \cdot 1}{\frac{1}{3} \cdot 1 + \frac{1}{3} \cdot \frac{2}{3} + \frac{1}{3} \cdot 0} = \frac{3}{5} = 0{,}6.$$

Формула Бернулли

Пусть производится n независимых испытаний, в каждом из которых вероятность того, что произойдет событие A, равна p, а следовательно, вероятность того, что оно не произойдет, равна q=1–p. Требуется найти вероятность того, что при n повторных испытаниях событие A произойдет m раз. Искомую вероятность обозначим $p_{m,\,n}$.

Событие, состоящее в том, что событие А происходит при каждом из m первых испытаний и не происходит при остальных n-m испытаниях, можно записать в виде

$$\underbrace{A \cdot A \cdot \ldots \cdot A}_{m} \cdot \underbrace{\overline{A} \cdot \overline{A} \cdot \ldots \cdot \overline{A}}_{n-m}.$$

Так как все n испытаний, по условию, независимы, то можно применить правило вычисления вероятности произведения независимых событий; получим

$$P(\underbrace{A\cdot A\cdot\ldots\cdot A}_{m}\cdot\underbrace{\overline{A}\cdot\overline{A}\cdot\ldots\cdot\overline{A}}_{n-m})=p^m q^{n-m}\ .$$

Событие A может произойти m раз при n испытаниях, но при этом может получиться и другая последовательность чередований событий A и $\bar{A}$, однако каждый раз получим одну и ту же вероятность $p^m q^{n-m}$. Очевидно, что число чередований событий A и равно числу сочетаний C_n^m из n элементов по m, поэтому по теореме сложения вероятностей для несовместных событий искомая вероятность вычисляется по формуле

$$p_{m,n}=C_n^m p^m q^{n-m}\ .$$

Эта формула называется ***формулой Бернулли.***

Примеры:

1. В урне 20 шаров: 15 белых и 5 черных. Вынули подряд 5 шаров, причем каждый вынутый шар возвращается в урну, и перед извлечением следующего шары в урне тщательно перемешиваются. Найти вероятность того, что из пяти вынутых шаров будет два белых.

Решение. Вероятность появления белого шара в каждом испытании равна $p=\frac{15}{20}=\frac{3}{4}$, а вероятность непоявления белого шара равна $q=1-p=\frac{1}{4}$. По формуле Бернулли находим

$$p_{2,5}=C_5^2 p^2 q^{5-2}=\frac{5\cdot 4}{1\cdot 2}\left(\frac{3}{4}\right)^2\cdot\left(\frac{1}{4}\right)^3=\frac{45}{512}.$$

2. Вероятность того, что расход электроэнергии в университете в течение одних суток не превысит установленной нормы, равна p=0,85. Найти вероятность того, что в бли-

жайшие 25 суток расход электроэнергии в течение 20 суток не превысит нормы.

Решение. Так как вероятность нормального расхода электроэнергии на протяжении каждых из 25 суток постоянна и равна p=0,85, то вероятность перерасхода электроэнергии в каждые сутки также постоянна и равна $q = 1 - p = 1 - 0{,}85 = 0{,}15$.

По формуле Бернулли находим искомую вероятность:

$$p_{20,25} = C_{25}^{20} p^{20} q^{25-20} = C_{25}^{5} (0{,}85)^{20} (0{,}15)^{5} \approx 0{,}156.$$

Тема 10. Дискретная случайная величина

Случайной величиной называется переменная X, которая в результате испытания может принять одно и только одно значение, не известное заранее и зависящее от исхода испытания.

Примеры:

1. При бросании игральной кости случайной является величина X – число очков, которое выпадет на верхней грани. Возможными значениями величины X служат числа 1, 2, 3, 4, 5, 6.

2. Число родившихся мальчиков среди ста новорожденных есть случайная величина X, возможными значениями которой являются числа 0, 1, 2, …, 100.

Величина X называется **дискретной случайной величиной**, если множество ее возможных значений представляет собой конечную или бесконечную последовательность чисел $x_1, x_2, \ldots, x_n, \ldots$ и если каждое соотношение $X = x_i$ (i = 1,2, …) является элементарным случайным событием и имеет определенную вероятность $p_i = P(X = x_i)$. Под $X = x_i$ понимается событие, состоящее в том, что величина X принимает значение x_i.

Мы будем рассматривать дискретные случайные величины лишь с конечными множествами значений.

Законом распределения дискретной случайной величины X называется соответствие между возможными значениями x_i и их вероятностями p_i .

Закон распределения (как и всякую функцию) можно задать **таблично, аналитически** и **графически**. Если случайная ве-

личина X может принимать лишь конечное число различных значений $x_1, x_2, \ldots, x_n$, то элементарные события $X = x_1$, $X = x_2$, …, $X = x_n$ образуют полную группу и поэтому сумма их вероятностей равна единице, т. е.

$$p_1 + p_2 + \ldots + p_n = 1.$$

Закон распределения такой величины может быть представлен в виде таблицы:

X	x_1	x_2	…	x_i	…	x_n
p	p_1	p_2	…	p_i	…	p_n

Вот, например, как выглядит таблица распределения вероятностей дискретной случайной величины X – числа очков, выпадающего при бросании правильной игральной кости:

X	1	2	3	4	5	6
p	1/6	1/6	1/6	1/6	1/6	1/6

Математическим ожиданием $M(X)$ дискретной случайной величины X называется сумма произведений всех ее возможных значений x_i на их вероятности p_i:

$$M(X) = x_1\, p_1 + x_2\, p_{21} + \ \ldots\ + x_m\, p_m.$$

Пример. Найти математическое ожидание случайной величины X, зная ее закон распределения:

X	–1	0	1	2	3
p	0,2	0,1	0,25	0,15	0,3

Решение. По формуле определения математического ожидания находим

$$M(X) = -1 \cdot 0{,}2 + 0 \cdot 0{,}1 + 1 \cdot 0{,}25 + 2 \cdot 0{,}15 + 3 \cdot 0{,}3 = 1{,}25.$$

Пусть при проведении n независимых испытаний дискретная случайная величина X может принимать m_1 раз – значение x_1,

m_2 раз – значение x_2, …, m_k раз значение x_k. Тогда сумма всех значений величины X равна

$$x_1m_1 + x_2m_2 + \ldots + x_km_k .$$

Найдем среднее арифметическое $\overline{X}$ значений, принимаемых величиной X:

$$\overline{X} = \frac{x_1m_1 + x_2m_2 + \ldots + x_km_k}{n} = x_1\frac{m_1}{n} + x_2\frac{m_2}{n} + \ldots + x_k\frac{m_k}{n}.$$

Но

$$\frac{m_1}{n} = P(X = x_1) = p_1, \qquad \frac{m_2}{n} = P(X = x_2) = p_2, \quad \ldots, \quad \frac{m_k}{n} = P(X = x_k) = p_k,$$

поэтому

$$\overline{X} = x_1p_1 + x_2p_2 + \ldots + x_kp_k = \mathrm{M}(X).$$

Таким образом, $M(X) = \overline{X}$, т. е. математическое ожидание дискретной случайной величины X равно среднему арифметическому полученных значений этой величины.

Пример. Найти среднее значение количества очков при бросании двух игральных костей.

Решение. Значениями дискретной случайной величины X в нашем примере являются числа 2, 3, 4, … , 12. Поскольку среднее значение равно математическому ожиданию, то получим

$$M(X) = 2\times\frac{1}{36} + 3\times\frac{2}{36} + 4\times\frac{3}{36} + 5\times\frac{4}{36} + 6\times\frac{5}{36} + 7\times\frac{6}{36} + 8\times\frac{5}{36} +$$

$$+ 9\times\frac{4}{36} + 10\times\frac{3}{36} + 11\times\frac{2}{36} + 12\times\frac{1}{36} = 7.$$

Математическое ожидание обладает следующими свойствами:

1. Математическое ожидание постоянной величины C равно самой постоянной:

$$M(C) = C.$$

2. Математическое ожидание суммы случайных величин равно сумме математических ожиданий слагаемых:

$$M(X+Y) = M(X) + M(Y).$$

3. Математическое ожидание произведения независимых случайных величин равно произведению математических ожиданий этих величин:

$$M(X \cdot Y) = M(X) \cdot M(Y).$$

4. Постоянный множитель можно выносить за знак математического ожидания:

$$M(CX) = C \cdot M(Y).$$

Рассмотрим следующий пример. Найти математическое ожидание случайных величин X и Y, зная законы их распределения:

X	–8	–4	–1	1	3	7
p	1/12	1/6	1/4	1/6	1/12	1/4

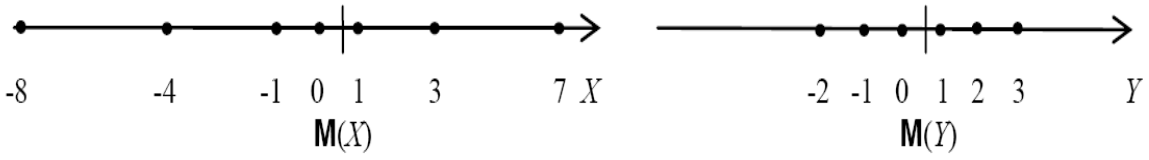
Y	–2	–1	0	1	2	3
p	1/6	1/6	1/12	1/3	0	1/4

Решение. По формуле определения математического ожидания имеем:

$$M(X) = -\frac{8}{12} - \frac{4}{6} - \frac{1}{4} + \frac{1}{6} + \frac{3}{12} + \frac{7}{4} = \frac{7}{12},$$

$$M(Y) = -\frac{2}{6} - \frac{1}{6} + 0 + \frac{1}{3} + 0 + \frac{3}{4} = \frac{7}{12}.$$

Мы получили любопытный результат: законы распределения величин X и Y разные, а их математические ожидания одинаковы. Из рис. 1.14 видно, что значения величины Y сосредоточены около математического ожидания $M(Y)$ (рис. 1.14*б*), а значения величины X разбросаны (рассеяны) подальше от математического ожидания $M(X)$ (рис. 1.14*а*).



а) *б*)

Рис. 1.14. Дискретные величины
с одинаковым математическим ожиданием

Основной числовой характеристикой рассеяния возможных значений случайной величины X служит **дисперсия** $D(X)$, которая определяется по формуле

$$D(X) = M\big(X - M(X)\big)^2$$

Преобразуем формулу следующим образом:

$$D(X) = M(X - M(X))^2 = M(X^2 - 2X \cdot M(X) + M^2(X)) =$$

$$= M(X^2) - 2M(X)M(X) + M^2(X) = M(X^2) - M^2(X) .$$

При преобразовании использовались свойства математического ожидания и тот факт, что $M(X)$ – величина постоянная.

Таким образом, получим альтернативную **формулу вычисления дисперсии,**

$$D(X) = M(X^2) - M^2(X).$$

Величина $\sigma = \sqrt{D(X)}$ называется **средним квадратическим отклонением** случайной величины X.

Пример. Дискретная случайная величина распределена по закону:

X	–1	0	1	2
p	0,2	0,1	0,3	0,4

Найти $D(X)$.

Решение. Сначала найдем

$$M(X) = -1 \cdot 0{,}2 + 0 \cdot 0{,}1 + 1 \cdot 0{,}3 + 2 \cdot 0{,}4 = 0{,}9,$$

а затем

$$M(X^2) = 1 \cdot 0{,}2 + 0 \cdot 0{,}1 + 1 \cdot 0{,}3 + 4 \cdot 0{,}4 = 2{,}1.$$

Используя формулу вычисления дисперсии получим:

$$D(X) = M(X^2) - M^2(X) = 2{,}1 - 0{,}81 = 1{,}29.$$

Мода дискретной случайной величины $Mo(X)$ – это значение случайной величины, которое имеет наибольшую вероятность.

Случайная величина называется **непрерывной,** если значения, которые она может принимать, заполняют конечный или бесконечный промежуток числовой оси. Каждому промежутку (a, b) из множества значений случайной величины непрерывного типа отвечает определенная вероятность $P(a < X < b)$ того, что значение, принятое случайной величиной, попадает в этот промежуток.

Закон распределения непрерывной случайной величины задается с помощью плотности распределения вероятности $f(x)$. Вероятность $P(a < X < b)$ того, что значение, принятое непрерывной случайной величиной X, попадает в промежуток (a, b), определяется равенством

$$P(a < X < b) = \int_a^b f(x)dx.$$

График функции $f(x)$ называется *кривой распределения.* Геометрически вероятность попадания случайной величины в промежуток (a, b) равна площади соответствующей криволинейной трапеции, ограниченной кривой распределения, осью Ox и прямыми $x = a$ *и* $x = b$. На рисунке приведен пример для $a = -1$, $b = 1$.

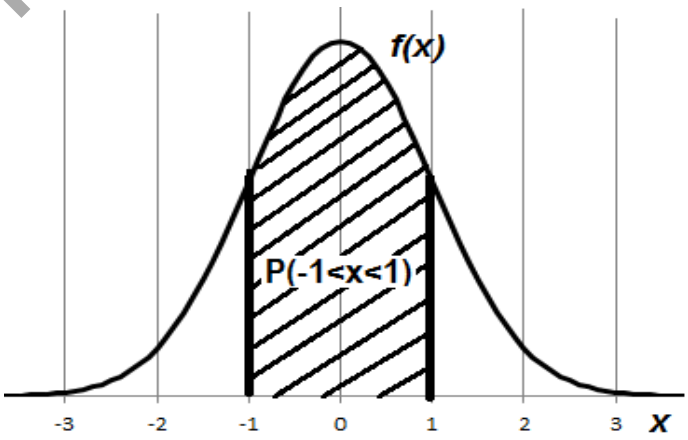


Рис. 1.15. Вероятность попадания случайной величины в промежуток (-1, 1)

Свойства плотности распределения:

$$1)\ f(x) > 0;\ 2)\ \int_{-\infty}^{\infty} f\ (x)\ d\ x = 1.$$

Функцией распределения вероятности случайной величины называется функция

$$F(x) = \mathrm{P}(\mathrm{X} < x) = \int_{-\infty}^{x} f(x)dx.$$

Из последнего равенства следует, что $f(x) = F'(x)$. Иногда $f(x)$ называют дифференциальной функцией распределения вероятности, а $F(x)$ – интегральной. Чтобы найти вероятность $P(a < X < b)$ того, что значение, принятое случайной величиной X, принадлежит промежутку (a, b), определяется равенством:

$$P(a < X < b) = F(b) - F(a).$$

Свойства функции распределения вероятности:

1) $F(x)$ – неубывающая функция;

2) $F(-\infty) = 0$;

3) $F(\infty) = 1$.

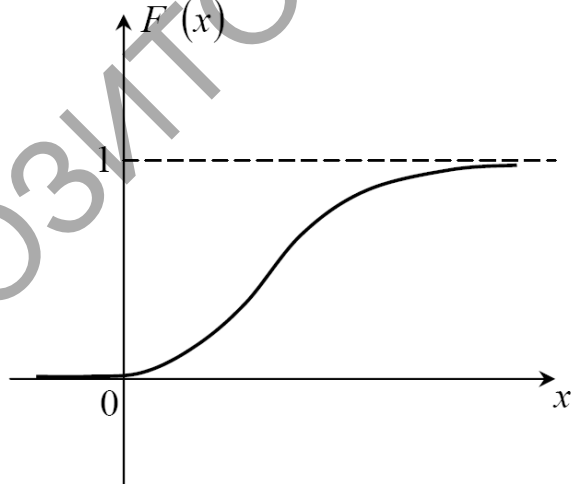


Рис. 1.16. Пример функции распределения

Математическое ожидание непрерывной случайной величины определяется равенством

$$M(X) = \int_{-\infty}^{x} f(x)dx.$$

при условии, что интеграл абсолютно сходится.

Модой *Mo*(*X*) непрерывной случайной величины X называют то ее возможное значение, которому соответствует локальный максимум плотности распределения. Если распределение имеет два одинаковых максимума, его называют *бимодальным*.

Медианой *Me*(*X*) непрерывной случайной величины X называют то ее возможное значение, которое определяется равенством

$$P(X< Me(X)) = P(X > Me(X)) = 0{,}5.$$

Дисперсия непрерывной случайной величины X определяется равенством:

$$D(X) = \int_{-\infty}^{+\infty} x^2 f(x) dx - (M(X))^2.$$

Среднее квадратическое отклонение непрерывной случайной величины определяется равенством $\sigma = \sqrt{D(X)}$:

Свойства математического ожидания и дисперсии для дискретных случайных величин верны и для непрерывных величин.

Начальным моментом порядка *k* случайной величины X называют математическое ожидание величины X^k:

$$v_k = M(X^k).$$

В частности, начальный момент первого порядка равен математическому ожиданию: $v_1 = M(X)$.

Центральным моментом порядка *k* случайной величины X называют математическое ожидание величины $(X - M(X))^k$:

$$v_k = M((X - M(X))^k).$$

В частности, центральный момент первого порядка равен нулю, а центральный момент второго порядка равен дисперсии. Центральные моменты можно вычислять с помощью начальных моментов. Если распределение симметрично относительно математического ожидания, то все **центральные моменты нечетного порядка** равны нулю

Отношение центрального момента третьего порядка к кубу среднего квадратического отклонения называется **асимметрией:**

$$As = \mu_3/\sigma_3.$$

Если распределение симметрично относительно математического ожидания, то $As = 0$.

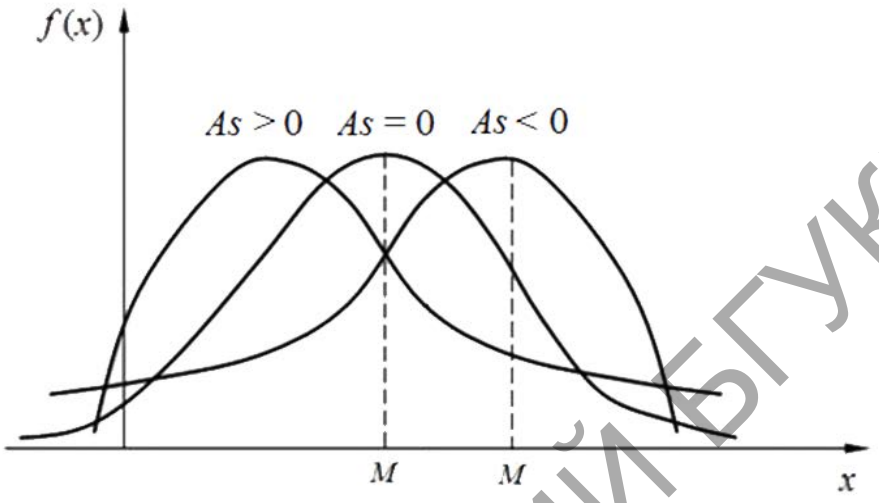


Рис. 1.17. Примеры асимметрий случайных величин

Эксцессом случайной величины X называется величина E, определяемая равенством $E = \frac{\mu_4}{\sigma^4} - 3$.

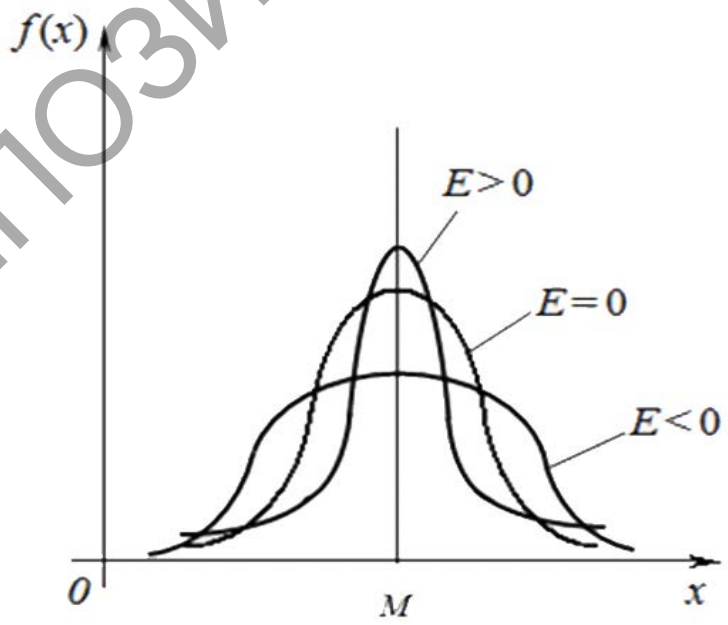


Рис. 1.18. Примеры кривых распределения
с различными значениями эксцесса

Для нормального распределения $E = 0$. Кривые, более островершинные, чем нормальная, имеют положительный эксцесс, более плосковершинные – отрицательный.

Закон больших чисел

Основная особенность случайной величины состоит в том, что нельзя заранее предвидеть, какое из возможных значений она примет в результате испытания. Однако, при достаточно большом числе испытаний суммарное поведение случайных величин почти утрачивает случайный характер и становится закономерным. Весьма важным при этом является знание условий возникновения закономерностей случайной величины. Эти условия составляют содержание ряда теорем, получивших общее название закона больших чисел. Впервые этот закон (в простейшей его форме) был сформулирован Якобом Бернулли в виде теоремы, устанавливающей связь между вероятностью случайного события и его относительной частотой.

Относительной частотой $W(A)$ случайного события A называют отношение числа m_n испытаний, в результате которых событие произошло, к общему числу n проведенных испытаний:

$$W(A) = \frac{m_n}{n}.$$

Оказывается, что при многократном повторении испытания относительная частота случайного события принимает значения, близкие к вероятности того, что оно произошло в результате одного испытания. Например, знаменитый статистик К. Пирсон бросил монету 24 000 раз и получил при этом 12 012 гербов, что дает относительную частоту, очень близкую к вероятности, равной 1/2, появления герба в одном испытании.

Теорема Бернулли. С вероятностью, сколь угодно близкой к единице, можно утверждать, что при достаточно большом числе независимых испытаний относительная частота случайного события как угодно мало отличается от его вероятности при отдельном испытании.

Наиболее общим законом больших чисел является теорема П. Л. Чебышева.

Теорема Чебышева. Если $X_1, X_2, \ldots, X_n$ – независимые случайные величины, причем дисперсии их равномерно ограничены (не превышают постоянного числа C), то последовательность $\{\overline{X}_n - M(\overline{X}_n)\}$ сходится по вероятности к нулю при $n \to \infty$, т. е.

$$\left\{\overline{X}_n - M(\overline{X}_n)\right\} \xrightarrow[n\to\infty]{} 0,$$

или

$$\overline{X}_n \xrightarrow[n\to\infty]{} M(\overline{X}_n), \qquad (*)$$

где

$$\overline{X}_n = \frac{X_1 + X_2 + \ldots + X_n}{n},$$

$$M(\overline{X}_n) = \frac{M(X_1) + M(X_2) + \ldots + M(X_n)}{n}.$$

Отметим, что если все случайные величины X_n имеют одно и то же математическое ожидание a:

$$M(X_n)=a, \quad (n = 1, 2, \ldots),$$

то математическое ожидание среднего арифметического $\overline{X}_n$ также совпадает с a:

$$M(\overline{X}_n) = a, \quad (n = 1, 2, \ldots).$$

В этом случае соотношение (*) принимает вид

$$\overline{X}_n \xrightarrow[n\to\infty]{} a.$$

Сущность теоремы Чебышева состоит в том, что среднее арифметическое достаточно большого числа независимых случайных величин с равномерно ограниченными дисперсиями утрачивает характер случайной величины.

Тема 11. Основные распределения случайных величин

Биномиальным называется закон распределения дискретной случайной величины *X,* отражающей число появлений *k* наблюдаемого события в *n* независимых испытаниях, в каждом из которых вероятность появления события равна *p.* Вероятность значения *X= k* вычисляют по *формуле Бернулли*:

$$P_n(k) = C_n^k p^k (1-p)^{n-k}$$

Математическое ожидание и дисперсия для биномиального распределения соответственно имеют вид:

$$M(X) = np \text{ и } D(X) = np(1-p).$$

Пример. Вероятность попадания стрелком в мишень равна 0.7. Стрелок делает 4 выстрела. Построить закон распределения случайной величины *X* – числа попаданий в мишень, функцию распределения $F(x) = P(X < x)$, найти математическое ожидание и дисперсию.

Подставляя в формулу $P_n(k) = C_n^k p^k (1-p)^{n-k}, C_n^k = \frac{n!}{k!\cdot(n-k)!}$

поочередно возможные значения количества попаданий k = 0, 1, 2, 3, 4, найдем значения $P_4(0) = 0{,}0081$, $P_4(1) = 0{,}0756$, $P_4(2) = 0{,}2646$, $P_4(3) = 0{,}4116$, $P_4(4) = 0{,}2401$. Таким образом, закон распределения случайной величины *X* будет иметь вид:

X	0	1	2	3	4
P	0,0081	0,0756	0,2646	0,4116	0,2401

Построим функцию распределения.

P(X<0) = 0, следовательно $F(x) = 0$, при $x<0$;

$F(x) = P(X< x) = P_4(0) = 0{,}0081$ при $0 < x \le 1$;

$F(x) = P(X< x) = P_4(0) + P_4(1) = 0{,}0837$ при $1 < x \le 2$;

$F(x) = P(X< x) = P_4(0) + P_4(1) + P_4(2) = 0{,}3483$ при $2 < x \le 3$;

$F(x) = P(X< x) = P_4(0) + P_4(1) + P_4(2) + P_4(3) = 0{,}7599$ при $2 < x \le 4$;

$F(x) = \mathrm{P}(\mathrm{X} < x) = P_4(0) + P_4(1) + P_4(2) + P_4(3) + P_4(4) = 1$ при $4 < x$.

График функции распределения приведен на рис. 1.19.

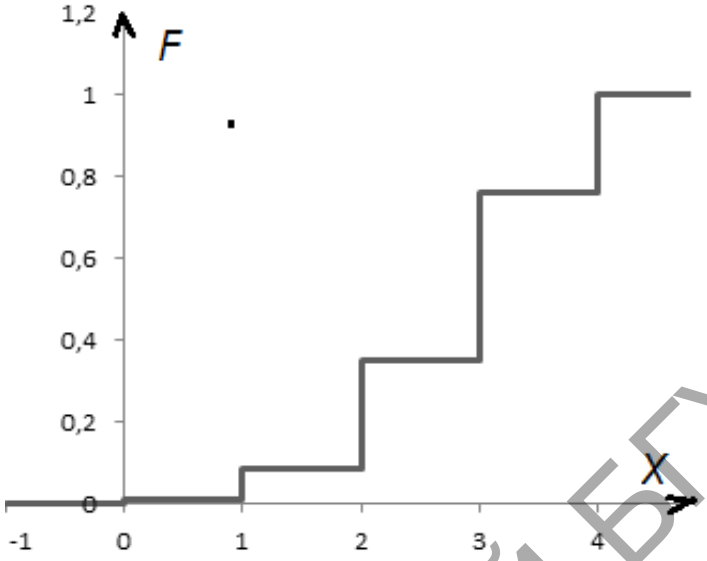


Рис. 1.19. График функции распределения

Вычислим математическое ожидание и дисперсию:

$M(X) = np = 0{,}7 \times 4 = 2{,}8$; $D(X) = npq = 0{,}7 \times 0{,}3 \times 4 = 0{,}84$.

Равномерным называется распределение таких случайных величин, все значения которых лежат на некотором отрезке $[a, b]$ и имеют постоянную плотность вероятности на этом отрезке.

Функция и плотность равномерного распределения приведены на рис 1.20.

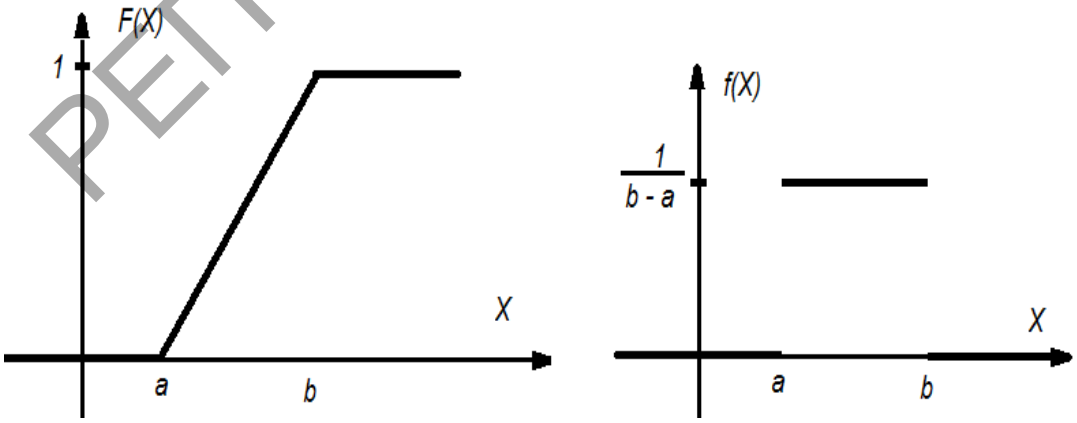


Рис. 1.20. Функция и плотность равномерного распределения

Математическое ожидание, дисперсия и среднеквадратическое отклонение имеют вид

$$M(X)=\frac{a+b}{2}, D(X)=\frac{(b-a)^2}{12}, \sigma(X)=\frac{b-a}{2\sqrt{3}}.$$

Экспоненциальный закон распределения имеет функцию плотности распределения вида

$$f(x)=\begin{cases}0, x<0,\\ \lambda e^{-\lambda x}, x\geq 0,\end{cases}$$

и функцию распределения вида

$$F(x)=\begin{cases}0, x<0,\\ 1-e^{-\lambda x}, x\geq 0.\end{cases}$$

Математическое ожидание, дисперсия и среднеквадратическое отклонение для экспоненциального распределения имеют вид

$$M(X)=\frac{1}{\lambda}, \quad D(X)=\frac{1}{\lambda^2}, \quad \sigma(X)=\frac{1}{\lambda}.$$

Нормальный закон распределения – закон распределения с плотностью распределения, задаваемой функцией Гаусса (рис.1.21):

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-(x-a)^2/(2\sigma^2)}$$

Математическое ожидание, дисперсия и среднеквадратическое отклонение для нормального распределения имеют вид:

$$M(X)=a, \quad D(X)=\sigma^2, \quad \sigma(X)=\sigma.$$

Мода и медиана нормального распределения равны математическому ожиданию: $Mo(X) = Me(X) = a$.

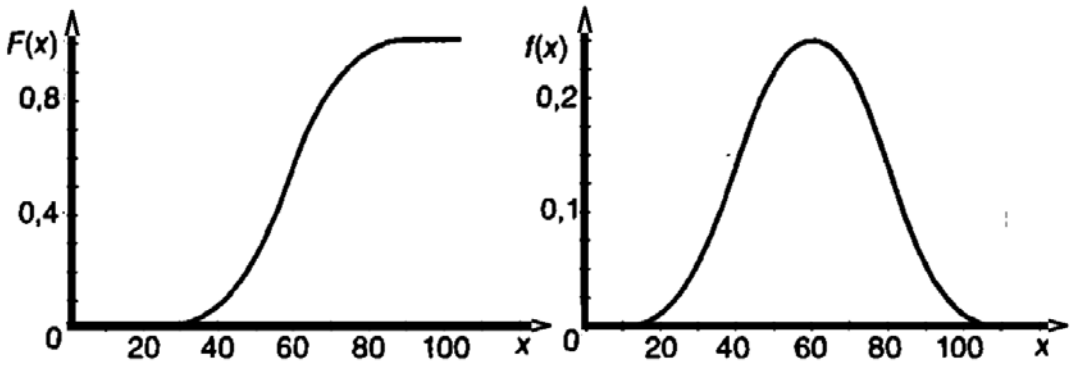


Рис. 1.21. Примеры функции распределения
и плотности вероятности нормального распределения

Вероятность того, что X примет значение, принадлежащее интервалу (α, β):

$$P(\alpha < X < \beta) = \Phi\left(\frac{\beta - \alpha}{\sigma}\right) - \Phi\left(\frac{\alpha - a}{\sigma}\right),$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-z^2/2}$ – функция Лапласа.

Функция Лапласа обладает следующими свойствами:

$$1)\ \Phi(0) = 0;\ 2)\ \Phi(+\infty) = 1;\ 3)\ \Phi(-x) = -\Phi(x).$$

Вероятность, того что модуль отклонения меньше δ:

$$P(|X - a| < \delta) = 2\Phi(\delta/\sigma) \qquad (*)$$

Значения функции Лапласа можно найти с помощью специальных таблиц [Павлов, ТВиМС] или, например, вычислить в Excel, введя в строку формул:

«=НОРМСТРАСП(x) - 0,5»

В статистическом анализе данных, часто используется **правила «3σ», «2σ»**. Определим вероятность попадания нормально распределенной случайной величины ξ с математическим ожиданием a и дисперсией σ^2 в интервал $(a - 3\sigma;\ a + 3\sigma)$, воспользовавшись формулой (*):

$$P(a - 3\sigma < \xi < a + 3\sigma) = P(|\xi - a| < 3\sigma) = 2\Phi(3).$$

По таблице находим Ф(3) = 0,49865. Таким образом, вероятность отклонения нормальной случайной величины ξ от ее математического ожидания a менее, чем на 3σ равна 2Ф(3) = 0,9973. Аналогично $P(|\xi - a| < 2\sigma) = 2\Phi(2) = 0{,}954$. Например, для нормальной случайной величины с математическим ожиданием $a = 2$ и среднеквадратическим отклонением $y = 1$ вероятность попадания в диапазон $(a - 2\sigma;\ a + 2\sigma)$ или (0, 4) равна 0,954, а за его пределы -0,046 (рис. 1.22).

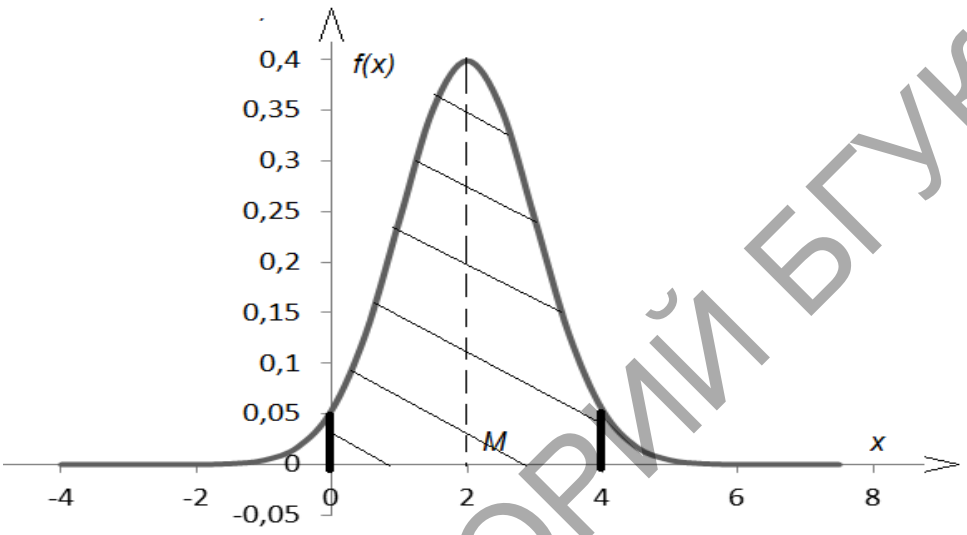


Рис. 1.22. Вероятность попадания в диапазон $(a - 2\sigma;\ a + 2\sigma)$ для нормальной случайной величины с математическим ожиданием $a = 2$ и среднеквадратическим отклонением σ = 1

Гамма-распределение неотрицательной случайной величины X определяется функцией плотности распределения вида:

$$\Gamma_{\lambda,k}(x) = f(x) = \frac{\lambda^k x^{k-1} e^{-\lambda x}}{\Gamma(k)}, (x > 0),$$

где $\lambda > 0$, $k > 0$ – параметры распределения; $\Gamma(k)$ – гамма-функция

$$\Gamma(k) = \int_0^\infty e^{-t} t^{k-1}\, dt.$$

Основные свойства гамма-функции:

1) $\Gamma(k+1) = k\,\Gamma(k)$; 2) $\Gamma(1) = 1$;

3) для целых неотрицательных k: $\Gamma(k+1) = k!$.

Математическое ожидание, дисперсия и среднеквадратическое отклонение случайной величины, имеющей гамма-распределение, имеют вид:

$$M(X)=\frac{k}{\lambda}, D(X)=\frac{k}{\lambda^2}, \sigma(X)=\frac{\sqrt{k}}{\lambda}.$$

Пусть случайная величина Y распределена по нормальному закону с математическим ожиданием a и средним квадратическим отклонением σ. Случайная величина

$$X^2=\left(\frac{Y-a}{\sigma}\right)^2$$

называется **случайной величиной хи-квадрат χ^2 с одной степенью свободы.**

Случайная величина

$$\chi^2=\left(\frac{\mathrm{Y}_1-a_1}{\sigma_1}\right)^2+\left(\frac{\mathrm{Y}_2-a_2}{\sigma_2}\right)^2+\ldots+\left(\frac{\mathrm{Y}_n-a_n}{\sigma_n}\right)^2,$$

где Y_1, Y_2, ... Y_n – нормально распределенные случайные величины с математическими ожиданиями и среднеквадратическими отклонениями $(a_1;\ \sigma_1)$, $(a_2;\ \sigma_2)$ … $(a_\mathrm{n};\ \sigma_\mathrm{n})$ соответственно, называется **случайной величиной хи-квадрат χ^2 с *n* степенями свободы**. Плотность распределения случайной величины χ^2 подчиняется гамма-распределению $\Gamma_{\frac{1}{2},\frac{n}{2}}$ и имеет вид

$$f(\chi)=\frac{1}{2^{\frac{n}{2}}\Gamma\left(\frac{n}{2}\right)}\left(\chi^2\right)^{\frac{n}{2}-1}e^{-\frac{\chi^2}{2}}$$

Функция распределения χ^2:

$$F(\chi^2)=F(\chi^2<\chi_0^2)=\frac{1}{2^{\frac{n}{2}}\Gamma\left(\frac{n}{2}\right)}\int_0^{\chi^2}\left(\chi^2\right)^{\frac{n}{2}-1}e^{-\frac{\chi^2}{2}}d\left(\chi^2\right)$$

Квантилем $\chi^2_{a,n}$**,** отвечающим заданному уровню вероятности σ, называется такое значение $\chi^2 = \chi^2_{a,n}$**,** при котором

$$P(\chi^2 > \chi^2_{\alpha,n}) = \int_{\chi^2_{\alpha,n}}^{\infty} f(\chi^2) d(\chi^2) = \alpha.$$

Распределение Стьюдента (t-распределение) используется при статистических вычислениях, связанных с нормальным законом, когда среднее квадратическое отклонение неизвестно и подлежит определению по опытным данным.

Пусть Y, Y_1, Y_2, ... Y_n – нормально распределенные случайные величины с математическими ожиданиями равными M = 0 и среднеквадратическими отклонениями равными $y = 1$. Случайная величина

$$t_n = \frac{Y}{\sqrt{\frac{1}{n}\sum_{i=1}^{n} Y_i^2}} = \frac{Y}{\sqrt{\frac{1}{n}\chi_n^2}}$$

называется случайной величиной, имеющей распределение Стьюдента с n степенями свободы. Плотность распределения случайной величины t имеет вид:

$$f(t) = S(t,n) = \frac{\Gamma\left(\frac{n+1}{2}\right)}{\sqrt{\pi n}\,\Gamma\left(\frac{n}{2}\right)}\left(1 + \frac{t^2}{n}\right)^{-\frac{n+1}{2}}, \quad -\infty < t < \infty.$$

Математическое ожидание и дисперсия случайной величины t соответственно равны:

$$M(t) = 0;\ D(t) = n/(n - 2).$$

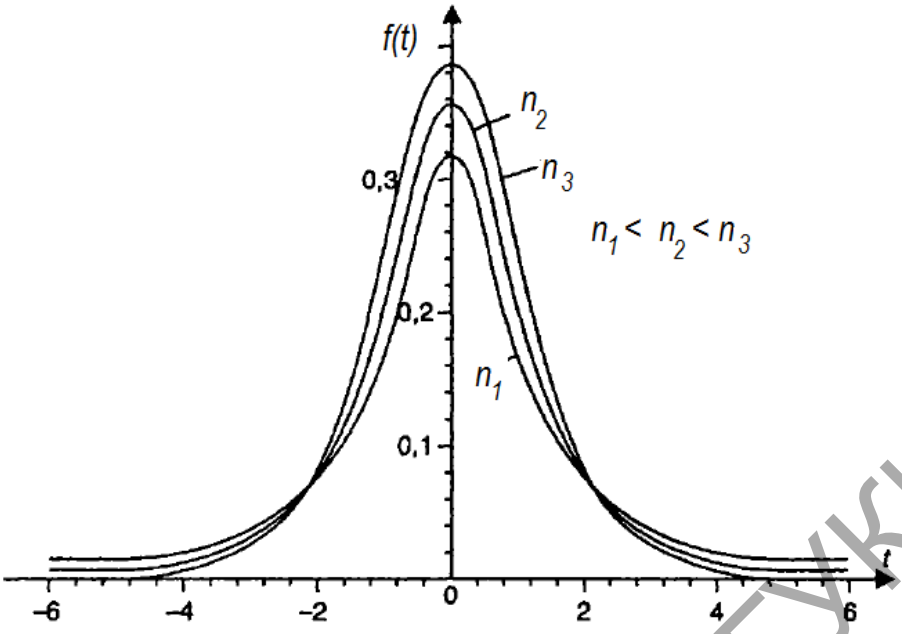


Рис. 1.23. График распределения функции Стьюдента при различных степенях свободы

При увеличении числа степеней свободы n график приближается к кривой Гаусса (рис. 1.23).

В статистических расчетах используются квантили t–распределения $t_{\frac{a}{2},n}$, значения которых находятся из уравнения:

$$P(|t| > t_{\frac{\alpha}{2},n}) = 2\int_{t_{\frac{\alpha}{2},n}}^{\infty} f(t)\,d(t) = \alpha$$

Важные приложения имеет в статистике случайная величина

$$X = \frac{Y_1/k_1}{Y_2/k_2},$$

где Y_1 – случайная величина, распределенная по закону χ^2 с k_1 степенями свободы, а Y_2 – случайная величина, распределенная по закону χ^2 с k_2 степенями свободы.

$$f(x) = \begin{cases} \dfrac{\sqrt{\dfrac{(k_1x)^{k_1}k_2^{k_2}}{(k_1x+k_2)^{k_1+k_2}}}}{xB\left(\frac{k_1}{2},\frac{k_2}{2}\right)}, x > 0, \\ 0, x \le 0 \end{cases}$$

где B – бета-функция, имеющая вид

$$B\left(\frac{k_1}{2},\frac{k_2}{2}\right)=\int_0^1 x^{\frac{k_1}{2}-1}(1-x)^{\frac{k_2}{2}-1}dx.$$

Тема 12. Основные понятия математической статистики

Сутью математической статистики является выявление закономерностей, которым подчинены массовые случайные явления. Совокупность всех объектов, по которым проводится статистическое исследование, называют **генеральной совокупностью**. **Выборочная совокупность** (выборка) – это совокупность случайно отобранных объектов. **Объем совокупности** (объем выборки) – число объектов этой совокупности.

Выборка называется **репрезентативной** (представительной), если она достаточно хорошо представляет количественные соотношения генеральной совокупности.

Пусть для изучения количественного (дискретного или непрерывного) признака X из генеральной совокупности извлечена выборка $x_1, x_2, ..., x_к$ объема k. Наблюдаемые значения x признака X называются вариантами, а последовательность вариант, записанных в возрастающем порядке,– **вариационным рядом**. Если значение x_i признака X наблюдалось n_i раз, то объем выборки

$$n=\sum_{i=1}^{k} n_i$$

Числа $n_1, n_2, ..., n_к$ называются **частотами**, а их отношения к объему выборки $w_i = n_i / n$, – **относительными частотами** соответствующих вариант.

Накопленная, или **кумулятивная**, частота $v_i = n_1 + n_2 + ... + n_{i-1}$ показывает, сколько наблюдалось элементов выборки со значениями признака, меньшими x_i. Отношение накопленной частоты к общему объему выборки, v_i / n, называется относительной накопленной частотой. **Статистическое распределение выборки** – перечень вариант x_i и соответствующих им

частот n_i (или) относительных частот w_i. Статистическое распределение выборки можно записать в виде таблицы, в первой строке которой указаны значения вариант выборки x_i, а во второй – значения частот, либо значения относительных частот.

При большом числе наблюдений варианты группируют по отдельным интервалам их значений. Шкала признака разделяется на некоторое количество интервалов определенной ширины, и частота интервала равна сумме частот вариант, принадлежащих интервалу. Для непрерывной случайной величины интервал наблюдаемых значений случайной величины разбивается на k частичных интервалов равной длины $[x_0, x_1)$, $[x_1, x_2)$, ... , $[x_{k-1}, x_k]$ и подсчете частоты n_i/n попадания наблюдаемых значений в частичные интервалы. Количество интервалов выбирается произвольно – обычно не менее 5 и не более 15.

x_i	5	10	15	20	25	30	35	40
$_i$	6	5	10	12	15	12	7	3

Для наглядности используют графическое представление статистических данных. Рассмотрим примеры такого представления.

Пример. Имеется распределение 70 фирм по количеству работающих на них менеджеров, заданное таблицей частот.

Признак X – число, работающих на фирме менеджеров является дискретным. Построим таблицу распределения относительных частот, полигон частот и полигон относительных частот.

Таблица распределения относительных частот получается из таблицы частот делением строки частот n_i на 70.

x_i	5	10	15	20	25	30	35	40
w_i	3/35	1/14	1/7	6/35	3/14	6/35	1/10	3/70

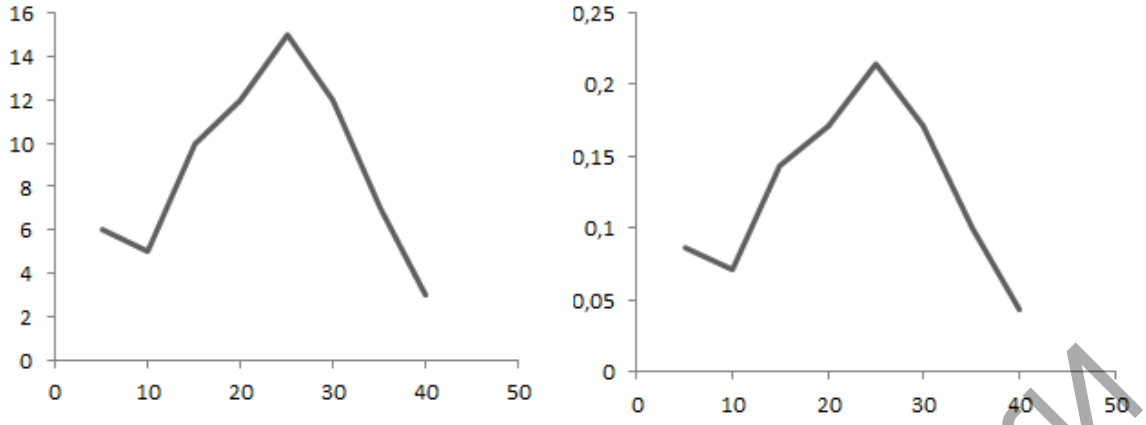


Рис. 1.24. Полигон частот и полигон относительных частот

Интервальный ряд изображают в виде **гистограммы частот**, основаниями прямоугольников которой служат частичные интервалы длины Δ, а высотами – величины n_i / Δ, называемые плотностями частот (рис. 1.24).

Пример. Дано распределение 50 кассиров магазинов по затратам времени на обслуживание одного покупателя.

x_{i-1}- x_i	2-4	4-6	6-8	8-10	10-12
n_i	2	11	25	8	4

Построим гистограммы частот. Признак X – затраты времени на обслуживание покупателя – непрерывный, ряд распределения – интервальный. Длина частичного интервала $\Delta = (x_k - x_0)/k = (12 - 2)/5 = 2$. Тогда плотность частот равна n_i / Δ и плотность относительных частот равна w_i / Δ .

x_{i-1}- x_i	2-4	4-6	6-8	8-10	10-12
n_i / Δ	1	5,5	11,5	4	2
w_i / Δ	0,2	1,1	2,5	0,8	0,4

Гистограмма частот и **гистограмма относительных частот** имеют вид, приведенный на рис. 1.25.

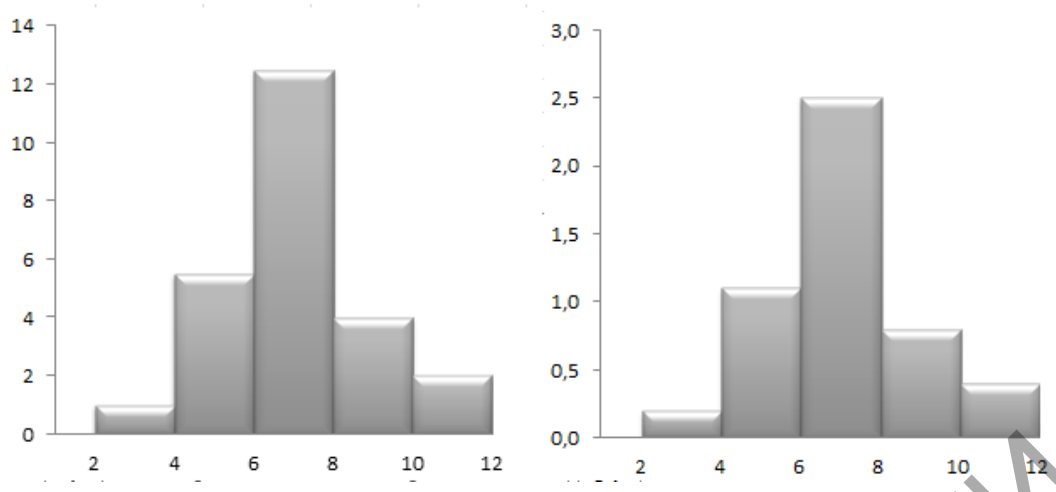


Рис. 1.25. Гистограмма частот
и гистограмма относительных частот

Площадь гистограммы частот S_n складывается из сумм площадей ее прямоугольников $S_i = \Delta \times (n_i / \Delta) = n_i$. Таким образом, $S_n = n_1 + n_2 + \ldots + n_k = n$ – объем выборки. Аналогично вычисляется площадь гистограммы относительных частот, ее значение $S_w = 1$.

В теории вероятностей гистограмме относительных частот соответствует график плотности распределения вероятностей $f(x)$, таким образом, гистограмму используют для подбора закона распределения генеральной совокупности.

Эмпирической функцией распределения или функцией распределения выборки называют функцию $F^*(x)$, которая для каждого значения x определяет относительную накопленную частоту события $X < x$:

$$F^* = \frac{v_i}{n} = \frac{n_1 + n_2 + \cdots + n_i}{n}$$

Свойства эмпирической функции:

1. Значения эмпирической функции распределения принадлежат отрезку [0, 1].

2. $F^*(x)$ – неубывающая функция.

3. Если x_i – наименьшая варианта, *а* x_k – наибольшая, то $F^*(x) = 0$ при $x \le x_k$ и $F^*(x) = 1$ при $x > x_k$.

Выборочной средней $\bar{x}$ выборки объема n называется величина

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i .$$

Выборочной взвешенной средней называется величина

$$\bar{x}^* = \frac{1}{n}\sum_{i=1}^{k} x_i n_i .$$

Частоты n_i в этом случае называются весами.

Выборочной дисперсией случайной величины называется выражение

$$D = \frac{1}{n}\sum_{i=1}^{k}(x_i - \bar{x}^*)^2 n_i .$$

Выборочной взвешенной дисперсией называется величина

$$D^* = \sum_{i=1}^{k}(x_i - \bar{x})^2 w_i = \frac{1}{n}\sum_{i=1}^{k}(x_i - \bar{x})^2 n_i .$$

Величина $\sigma(x) = \sqrt{D(x)^*}$ называется средним квадратическим отклонением.

Пример. Дано распределение n=85 преподавателей факультета вуза по возрасту

x_{i-1}- x_i	25-	30-	35-	40-	45-	50-	55-	60-	65-
n_i	6	10	12	9	15	10	12	7	4

Построим таблицу накопленных относительных частот

i	x_{i-1}-x_i	n_i	v_i=n_1+n_2+..+n_i	$F^*(x) = v_i$/n
0	-∞–25	0	0	0
1	25–30	6	6	0,071
2	30–35	10	16	0,188
3	35–40	12	28	0,329
4	40–45	9	37	0,435
5	45–50	15	52	0,612
6	50–55	10	62	0,729
7	55–60	12	74	0,871
8	60–65	7	81	0,953
9	65–70	4	85	1

Пример. Дано распределение 60 тестируемых по набранному количеству баллов. Найдем оценки – выборочное взвешенное среднее (средний балл), дисперсию и среднее квадратическое отклонение, а также построим график эмпирической функции распределения.

Кол-во баллов x_i	Кол-во тестируемых n_i, набравших балл x_i	$x_i n_i$	v_i	$\underbrace{(x_i - \overline{x^*})^2 n_i}_{\tilde{x}_i}$	$x_i^2 n_i$
3	5	15	0	64,8	45
4	4	16	5	27,04	64
5	6	30	9	15,36	150
6	10	60	15	3,6	360
7	15	105	25	2,4	735
8	12	96	40	23,52	768
9	6	54	52	34,56	486
10	2	20	58	23,12	200
	$n = \sum n_i = 60$	$\sum x_i n_i = 396$		$\sum \tilde{x}_i^2 n_i$ 194,4	$\sum x_i^2 n_i = 2808$
	Средний балл $\overline{x^*} = (\sum x_i n_i)/n = 6,6$			$\overline{x^2} = (\sum x_i^2 n_i)/n = 46,8$	

Дисперсия *(вычисляется двумя разными способами)*

$$D = \overline{x^2} - (\overline{x^*})^2 = 46,8 - (6,6)^2 = 3,24$$

$$D = \frac{1}{n}\sum_i^k (x_i - \overline{x^*})^2 n_i = 3,24$$

$$\sigma = \sqrt{D} = 1,8$$

График эмпирической функции распределения представлен на рис. 1.26.

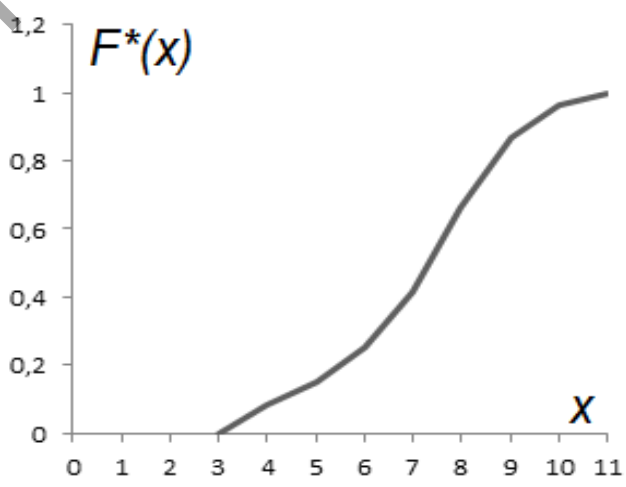


Рис. 1.26. График эмпирической функции распределения

Тема 13. Основы фрактальной геометрии

Фракталом принято называть объект, которые состоят из частей, подобных самому объекту. Фракталы подразделяют на **геометрические, алгебраические**, **стохастические.**

Приведем алгоритмы геометрического построения основных геометрических фракталов (рис. 1.27–1.30).

Рис. 1.27. Снежинка Коха

Рис. 1.28. Дерево Пифагора

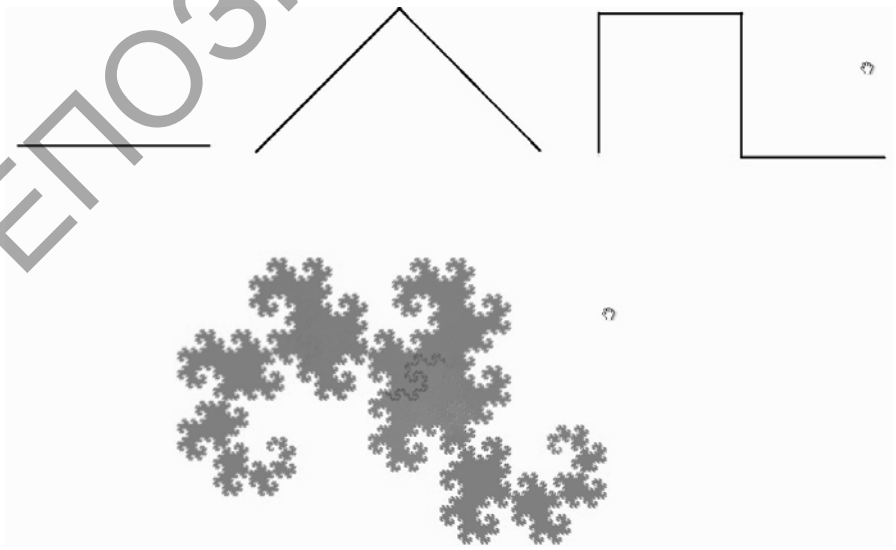


Рис.1.29. Кривая Дракона

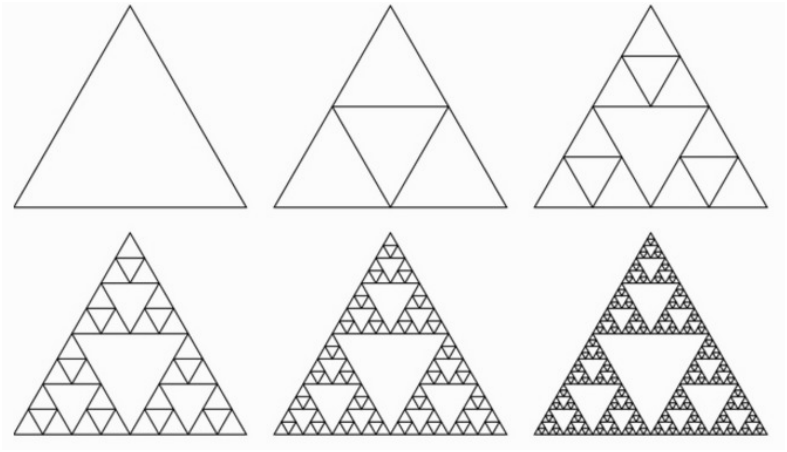


Рис. 1.30. Треугольник Серпинского

Под термином **размерность,** как правило, понимают число координат, необходимых для задания положения точки внутри фигуры. Любая линия (например, окружность или прямая) одномерна, так как достаточно одной координаты, чтобы точно указать точку на ней. Плоскость и поверхность шара двумерны. Однако в математике существуют объекты, к которым это определение неприменимо, среди них и фракталы.

Фрактальную размерность определяют следующим образом.

Допустим, что фигура F, размерность которой мы хотим найти, расположена на плоскости, которая покрыта сеткой из квадратиков со стороной д. Через $N(\delta)$ обозначим число квадратиков, которые пересекаются с фигурой F (объединение всех таких квадратиков содержит в себе F). Число $N(\delta)$ зависит от размера квадратиков: чем они меньше, тем больше их нужно, чтобы покрыть фигуру. Пусть эта зависимость выражается степенным законом: число $N(\delta)$ пропорционально некоторой степени $(1/\delta)^D$, будем считать, что фигура F имеет размерность D (для фракталов число D не является целым). Изложенный алгоритм является определением фрактальной размерности по Минковскому. Для «хороших» фигур оно дает тот же результат, что и интуитивное представление о размерности. Например, посчитаем размерность квадрата со стороной 1 (располагая его на плоскости так, что стороны квадрата каждый раз лежат на линиях сетки): $N(1) = 1$, $N(1/2) = 4$, $N(1/3) = 9$,

$N(1/4) = 16$ и т. д. Видно, что в этом случае D=2, то есть квадрат двумерен, как и должно быть.

Для построения фракталов используют рекурсивные алгоритмы. Функция внутри себя может содержать вызов других функций. Например, функция $f(x)=x^2$ может содержать вызов $g(y)=sin(y)$: $f(sin(y))=sin^2(y)$. В том числе функция может вызвать саму себя. Такая функция называется рекурсивной.

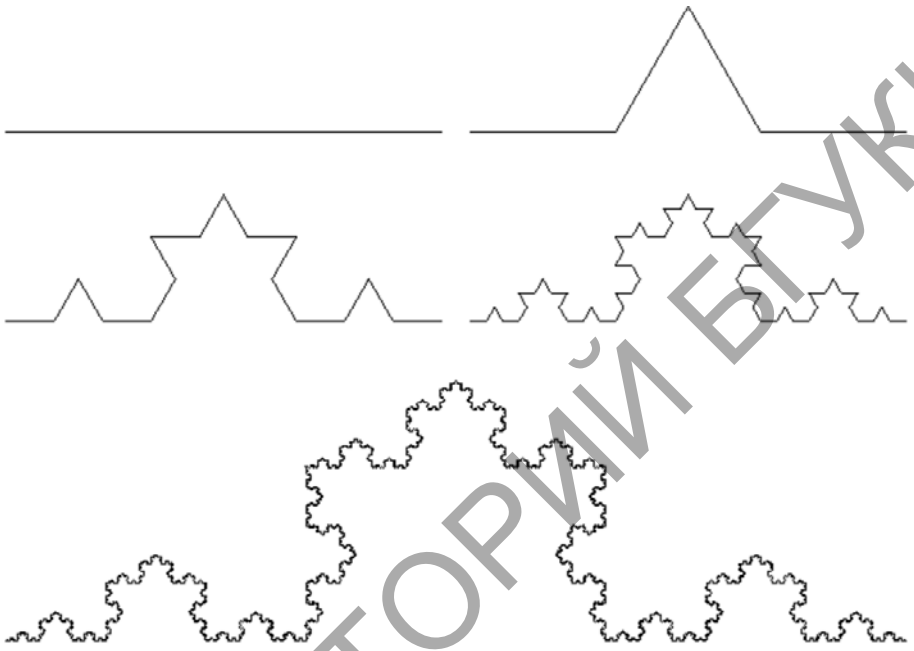


Рис.1.31. Кривая Коха

Классическим примером рекурсивных алгоритмов является построение фракталов. Например, кривая Коха (рис. 1.31). Изначально берется отрезок прямой. Он делится на три части, средняя часть изымается и вместо нее строится угол, стороны которого равны длине изъятого отрезка, а именно 1/3 от длины исходного отрезка. Такая операция повторяется с каждым из получившихся 4-х отрезков. Процесс продолжается и после бесконечного числа таких итераций получается Кривая Коха.

Тема 14. Алгебраические и стохастические фракталы

Комплексное число – это выражение вида $a + bi$, где a, b – действительные числа, а i – так называемая *мнимая единица*, для которой выполняется: $i^2 = -1$. Число a называется *действительной частью*, а число bi – *мнимой частью* комплексного числа $z = a + bi$. Если $b = 0$, то вместо $a + 0i$ пишут просто a. Действительные число – это частный случай комплексных чисел.

Арифметические действия над комплексными числами те же, что и над действительными: их можно складывать, вычитать, умножать и делить друг на друга. Сложение и вычитание происходят по правилу:

$$(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i.$$

Правило умножения имеет следующий вид:

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Число $\bar{z} = a - bi$ называется *комплексно-сопряженным* к $z = a + bi$. Легко убедиться, что $z \cdot \bar{z} = a^2 + b^2$.

Из последнего равенства выводятся правила деления комплексных чисел:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

$$= \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}$$

Геометрическое представление комплексных чисел

Число $z = a + bi$ изображается вектором с координатами $(a; b)$ на декартовой плоскости или точкой – концом вектора с этими координатами (рис. 1.32).

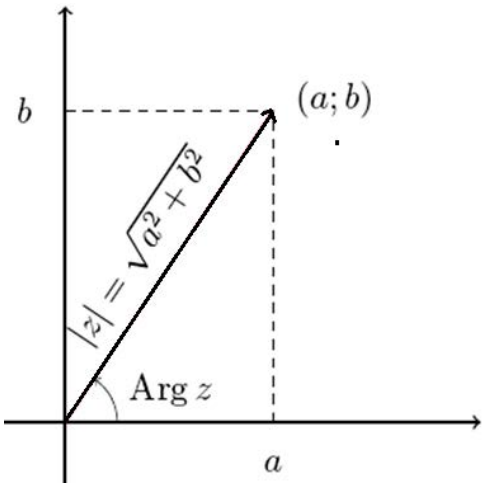


Рис. 1.32. Геометрическое представление комплексного числа

Сумма двух комплексных чисел изображается как сумма соответствующих векторов. По теореме Пифагора длина вектора с координатами (a; b) равна $\sqrt{a^2+b^2}$. Эта величина называется **модулем** комплексного числа $z = a + bi$ и обозначается

$$|z| = \sqrt{a^2+b^2}$$

Угол, который вектор образует с положительным направлением оси абсцисс, называется **аргументом** комплексного числа z и обозначается $\mathrm{Arg}\, z$. Аргумент определен не однозначно, а лишь с точностью до прибавления величины, кратной $2p$ радиан (или 360 градусов).

Если вектор длины r образует угол φ с положительным направлением оси абсцисс, то его координаты равны ($r\cos\varphi$; $r\sin\varphi$). Отсюда получается **тригонометрическая форма записи** комплексного числа:

$$z = |z| \cdot (\cos(\mathrm{Arg}\, z) + i \sin(\mathrm{Arg}\, z)).$$

Умножение комплексных чисел в тригонометрической форме:

$$z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot (\cos(\mathrm{Arg}\, z_1 + \mathrm{Arg}\, z_2) + i \sin(\mathrm{Arg}\, z_1 + \mathrm{Arg}\, z_2)),$$

то есть при умножении двух комплексных чисел их модули перемножаются, а аргументы складываются. Отсюда следует **формула Муавра**:

$$z^n = |z|^n \cdot (\cos(n \cdot (\operatorname{Arg} z)) + i \sin(n \cdot (\operatorname{Arg} z))).$$

С помощью этих формул легко извлекать корни любой степени $n \in N$ из комплексных чисел. *Корень n-й степени из числа* z – это такое комплексное число w, что $w^n = z$. Тогда

$$|w| = \sqrt[n]{|z|}$$

$$\operatorname{Arg} w = \frac{1}{n} \operatorname{Arg} z + \frac{2\pi k}{n}$$

где k может принимать любое значение из множества $\{0, 1, ..., n - 1\}$. Это означает, что всегда есть ровно n корней n-й степени из комплексного числа. На плоскости они располагаются в вершинах правильного n-угольника.

Множество Мандельброта – это множество точек c на комплексной плоскости, для которых последовательность z_n, определяемая итерациями $z_0 = 0$,

$$z_1 = z_0^2 + c,$$

...

$$z_{n+1} = z_n^2 + c,$$

конечна (то есть не уходит в бесконечность). Визуально множество Мандельброта выглядит набором бесконечного количества различных фигур, самая большая из которых называется кардиоидой, которая окружена все уменьшающимися кругами, каждый из которых окружен еще меньшими кругами и т. д. до бесконечности (рис. 1.33*а*). При любом увеличении этого фрактала будут выявляться все более и более мелкие детали изображения, дополнительные ветки с более мелкими кардиоидами, кругами. И этот процесс можно продолжать бесконечно.

Для построения графического изображения множества Мандельброта можно использовать алгоритм, называемый **escape-time**. Доказано, что все множество целиком расположено внутри круга радиуса 2 на плоскости. Если для точки c последовательность итераций функции $z_{n+1} = z_n^2 + c$ с начальным значением $z_0 = 0$ после некоторого большого их числа N не вышла за пределы этого круга, то точка принадлежит множеству и кра-

сится в черный цвет. Если на каком-то этапе, меньшем N, элемент последовательности по модулю стал больше 2, то точка множеству не принадлежит и остается белой. Таким образом, можно получить черно-белое изображение множества, что и было сделано Мандельбротом. Чтобы сделать его цветным, можно, например, каждую точку не из множества красить в цвет, соответствующий номеру итерации, на котором ее последовательность вышла за пределы круга.

При итерациях функции $z_{n+1} = z_n^2 + c$ любая точка z комплексной плоскости имеет свой характер поведения (остается конечной, стремится к бесконечности, принимает фиксированные значения), а вся плоскость делится на части. Точки, лежащие на границах этих частей, обладают таким свойством: при сколь угодно малом смещении характер их поведения резко меняется (такие точки называют *точками бифуркации*). При этом множества точек, имеющих один конкретный тип поведения, а также множества бифуркационных точек часто имеют фрактальные свойства. Это и есть **множества Жюлиа** для функции $z_{n+1} = z_n^2 + c$ (рис. 1.33*б*).

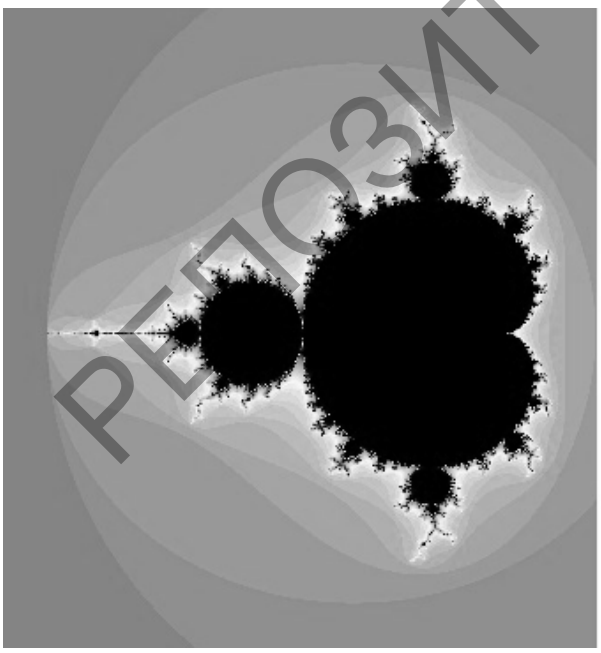


Рис. 1.33а. Множество Мандельброта

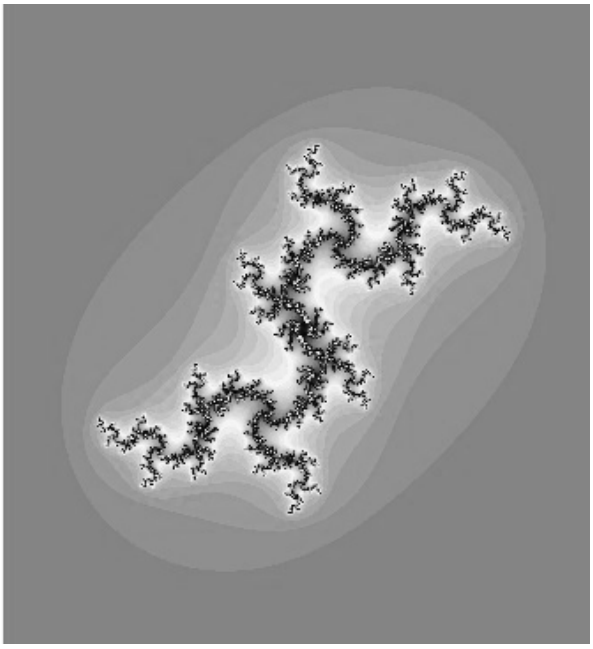


Рис. 1.33б. Множество Жюлиа

Множества Мандельброта и Жюлиа являются **динамическими фракталами**. Еще одним известным классом фракталов являются **стохастические фракталы**, которые получаются в том случае, если в итерационном процессе случайным образом менять какие-либо его параметры. При этом получаются объекты очень похожие на природные – несимметричные деревья, изрезанные береговые линии и т. д. Двумерные стохастические фракталы используются при моделировании рельефа местности и поверхности моря.

Система итерируемых функций (Iterated functions system) – это средство получения фрактальных структур путем итераций. IFS представляет собой систему функций из некоторого фиксированного класса функций, отображающих одно многомерное множество на другое. Наиболее простая IFS состоит из аффинных преобразований плоскости: суперпозиции, масштабирования, поворота, параллельного переноса и зеркального отображения. Приведем пример алгоритма IFS для кривой Коха. Расположим первое поколение этого фрактала на сетке координат дисплея 640 x 350 (рис. 1.34, 1.35).

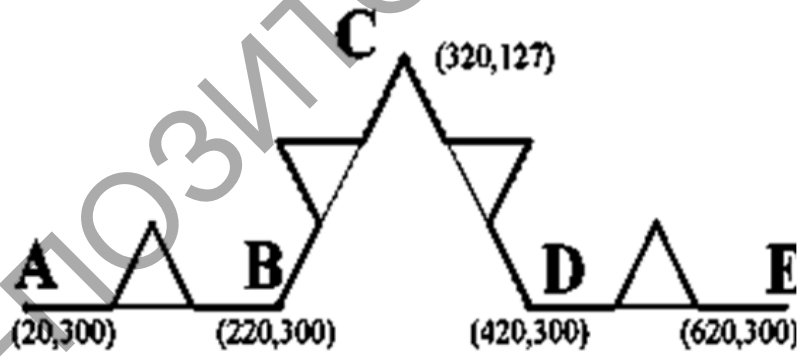


Рис. 1.34. Первое поколение кривой Коха

Для ее построения требуется набор аффинных преобразований, состоящий из четырех преобразований:

1) X' = 0,333*X + 13,333
Y' = 0,333*Y + 200

2) X' = 0,333*X + 413,333
Y' = 0,333*Y + 200

3) X' = 0,167*X + 0,289*Y + 130
Y' = -0,289*X + 0,167*Y + 256

4) X' = 0,167*X - 0,289*Y + 403
Y' = 0,289*X + 0,167*Y + 71

Рис. 1.35. Результат десяти итераций построения кривой Коха

Мультифрактал определяется не одним единственным алгоритмом построения, а несколькими последовательно сменяющими друг друга алгоритмами. Каждый такой алгоритм генерирует фрагмент своей фрактальной размерности. Природные объекты описываются мультифракталами.

Области применения фракталов

Фракталы широко применяются в компьютерной графике для сжатия изображений, построения ландшафтов, деревьев, растений и генерирования фрактальных текстур. Фракталы давно применяют в механике, акустике, физике благодаря уникальному свойству повторять очертания многих объектов природы, позволяют приближать деревья, горные поверхности, молнии, трещины с более высокой точностью, чем приближения наборами отрезков или многоугольников. Фрактальные модели, как и природные объекты, обладают «шероховатостью», сохраняя это свойство при сколь угодно больших увеличениях модели.

Последнее время фракталы стали популярным инструментом у трейдеров для анализа состояния биржевых рынков. Фракталы рынка являются одним из индикаторов в торговой системе Била Вильямса.

Использование фрактальной геометрии при проектировании антенных устройств было впервые применено американским инженером Натаном Коэном. Он вырезал из алюминиевой фольги фигуру в форме кривой Коха и наклеил ее на лист бумаги, затем присоединил к приемнику. Оказалось, что такая

антенна работает не хуже обычной. И хотя физические принципы работы такой антенны не изучены до сих пор, это не помешало Коэну основать собственную компанию и наладить их серийный выпуск.

Система назначения IP-адресов в сети Netsukuku использует принцип фрактального сжатия информации для компактного сохранения информации об узлах сети. Каждый узел сети Netsukuku хранит всего 4 Кб информации о состоянии соседних узлов, при этом любой новый узел подключается к общей сети без необходимости в центральном регулировании раздачи IP-адресов, что, например, характерно для сети Интернет. Таким образом, принцип фрактального сжатия информации гарантирует полностью децентрализованную, а следовательно, максимально устойчивую работу всей сети.

II. ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ И КРИПТОЛОГИИ

Тема 15. Введение в теорию информации

Понятие *«информация»* является центральным понятием кибернетики. Оно используется и в теории информации, хотя основным понятием классической теории информации следует признать «количество информации».

Имеется множество определений понятия информации от наиболее общего философского (информация есть отражение реального мира) до наиболее узкого практического (информация есть все сведения, являющиеся объектом хранения, передачи и преобразования).

Некоторыми авторами информация трактуется с идеалистических позиций в отрыве от материи как некоторая субстанция, занимающая промежуточное положение между материей и сознанием.

С позиций объективистской (немецкой классической) и материалистической философий информация рассматривается как характеристика такого всеобщего свойства материи, как разнообразие. Такая трактовка находится в полном соответствии с известным положением Гегеля о том, что вся материя обладает свойством отражения (рефлексии). Она четко выявляет взаимоотношения понятий «информация» и «отражение».

Информация – это отраженное разнообразие, отношение между материальными объектами. В понятии «отражение» акцентируется внимание на воспроизведении содержания в целом, а в понятии «информация» – на воспроизведении одной его стороны – разнообразия. Следовательно, понятие «отражение» более широкое, более содержательное.

В рамках философской исходной посылки при конкретизации понятия «информация» имеют место расхождения по ряду существенных вопросов: информация – это свойство индивидуального объекта (процесса) или результат взаимодействия объектов (процессов)? Присуща ли информация всем видам материи или лишь определенным образом организованной материи? Существует ли информация в любых процессах или возникает только в процессах управления? Выдвинутое академиками В. М. Глушковым и А. Н. Колмогоровым, а также английским профессором У. Эшби и развиваемое советскими учеными понятие информации как характеристики внутренней организованности материальной системы (по множеству состояний, которые она может принимать) позволяет оценивать потенциальные возможности систем независимо от процесса передачи или восприятия информации. Здесь подчеркивается мысль о том, что информация существует независимо от того, воспринимается она или нет. Однако справедливо отмечается, что информация проявляется только при взаимодействии объектов (процессов).

Противоречия не возникает, если информацию рассматривать как свойство объекта в потенциальном смысле – свойство, которое проявляется лишь при взаимодействии объектов (процессов). Так, в куске каменного угля содержится информация о событиях, произошедших в далекие времена, однако эта информация проявляется лишь при взаимодействии с человеком. В книге Н. Винера «Кибернетика» подчеркивается, что «информация есть информация, а не материя и не энергия». В отличие от них информация может возникать и исчезать. В указанном примере (информация в куске каменного угля) она исчезнет, если этот кусок каменного угля сгорит.

Весьма распространенным является также мнение о том, что информация присуща лишь определенным образом организованной материи, в которой возможны процессы управления. Сторонники этой точки зрения под информацией подразумевают только то, что воспринято и осмысленно, т. е. то, что це-

лесообразно использовать для управления. Нетрудно заметить, что вопрос о существовании информации здесь неправомерно отождествляется с вопросом о способности объекта к восприятию и использованию информации. При таком подходе легко сойти на позиции субъективизма, ставящего объективно существующее в зависимость от воспринимающего субъекта.

При всех различиях в трактовке понятия информации, бесспорно то, что проявляется информация всегда в материально-энергетической форме в виде сигналов. Информацию, представленную в формализованном виде, позволяющем осуществить ее обработку с помощью технических средств, называют *данными*.

Совокупность средств информационной техники и людей, объединенных для достижения определенных целей или для управления, образует *автоматизированную информационную систему*, к которой по мере надобности подключаются абоненты (люди или устройства), поставляющие и использующие информацию.

Информационные системы, действующие без участия человека, называют *автоматическими*. За человеком в таких системах остаются функции контроля и обслуживания.

Автоматизированная информационная система становится *автоматизированной системой управления* (АСУ), если поставляемая информация извлекается из какого-либо объекта (процесса), а выходная используется для целенаправленного изменения состояния того же объекта (процесса), причем абонентом, использующим информацию для выбора основных управляющих воздействий (принятия решения), является человек. Объектом могут быть техническая система, экологическая среда, коллектив людей. Существуют АСУ, в которых отдельные функции управления возлагаются на технические средства, в основном на ЭВМ и микропроцессоры.

Автоматизированные информационные системы и АСУ нашли широкое применение во всех отраслях народного хозяйства, в первую очередь как информационно-справочные и ин-

формационно-советующие системы, системы управления технологическими процессами и коллективами людей. Большинство из них являются локальными системами и функционируют на уровне предприятий и учреждений. В настоящее время происходит интенсивный процесс интеграции таких систем в системы производственных объединений и далее – в отраслевые и ведомственные системы.

Системы более высокого уровня становятся территориально рассредоточенными, иерархичными как по функциональному принципу, так и по реализации их техническими средствами. Обеспечение взаимодействия территориально рассредоточенных систем требует протяженных высокоскоростных и надежных каналов связи, а увеличение объема обрабатываемой информации – ЭВМ высокой производительности. Это привело к необходимости коллективного использования дорогостоящих средств автоматизации (ЭВМ и линий связи) и обрабатываемой информации (банков и баз данных). Техническое развитие как самих электронных вычислительных машин, так и средств связи позволило решить эту проблему путем перехода к созданию распределенных информационно-вычислительных сетей коллективного пользования.

Централизация различных видов информации в одной сети дает возможность использовать ее для решения широкого спектра задач, связанных с административным управлением, планированием, научными исследованиями, конструкторскими разработками, технологией производства, снабжением, учетом и отчетностью. Использование информационно-вычислительных сетей позволяет отказаться от традиционных форм массового общения, таких как телефон, телеграф, почта, отдельные справочные службы. Они заменяются новыми формами передачи информации: электронной почтой, сотовой связью, различными интернет-сервисами.

Наиболее распространенными информационными системами являются системы, обеспечивающие передачу информации из одного места в другое (*системы связи*) и от одного момента

времени до другого (*системы хранения информации*). Обе разновидности систем передачи информации имеют много общего в принципиальных вопросах обеспечения эффективности функционирования. Их применяют как самостоятельные системы и как подсистемы в составе любых более сложных информационных систем. Совокупность таких подсистем в информационно-вычислительной сети образует ее основное ядро – сеть передачи данных.

Последующее изложение будем вести в основном применительно к системам связи, подразумевая возможность интерпретации основных понятий и выводов к другим информационным системам.

Хотя роль информации может ограничиваться неопределенным эмоциональным воздействием на человека, в чисто технических (*автоматических*) и человеко-машинных (*автоматизированных*) системах она чаще всего используется для выработки управляющих воздействий. При обращении информации в системах можно выделить отдельные этапы. Так как материальным носителем информации является сигнал, то реально это будут *этапы обращения и преобразования сигналов* (рис. 2.1).

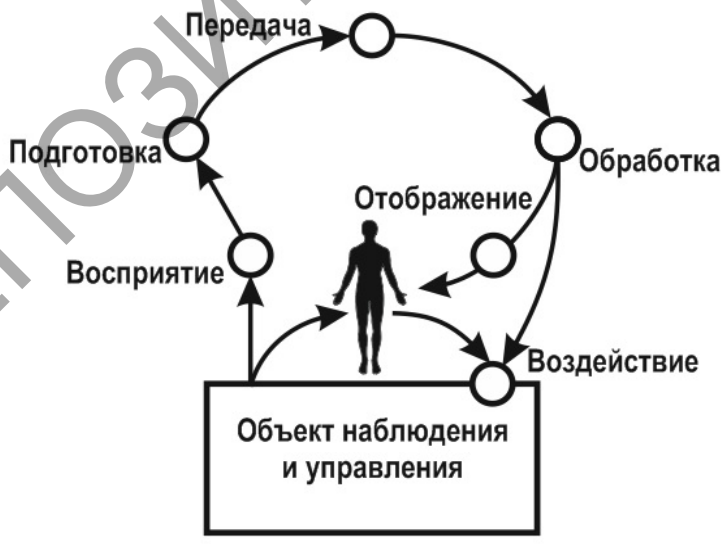


Рис. 2.1. Обращение информации

На этапе *восприятия* информации осуществляется целенаправленное извлечение и анализ информации о каком-либо

объекте (процессе), в результате чего формируется образ объекта, проводятся его опознание и оценка. При этом необходимо отделить интересующую нас в данном случае информацию от мешающей (шумов), что в ряде случаев связано со значительными трудностями. Простейшим видом *восприятия* является различение двух противоположных состояний: наличия («да») и отсутствия («нет»), более сложным – измерение.

На этапе *подготовки* информации проводятся такие операции, как нормализация, аналого-цифровое преобразование, шифрование. Иногда этот этап рассматривается как вспомогательный на этапе восприятия. В результате восприятия и подготовки получается сигнал в форме, удобной для передачи или обработки.

На этапах *передачи и хранения* информация пересылается либо из одного места в другое, либо от одного момента времени до другого. Поскольку теоретические задачи, возникающие на этих этапах, близки друг другу, этап хранения информации часто в самостоятельный этап не выделяется. При этом передача информации получает более широкое толкование. Для передачи на расстояние используются каналы различной физической природы, самыми распространенными из которых являются электрические и электромагнитные. В последнее десятилетие получил признание также перспективный оптический канал. Для хранения информации используются в основном полупроводниковые и магнитные носители. Извлечение сигнала на выходе канала, подверженного действию шумов, носит характер вторичного восприятия.

На этапах *обработки* информации выявляются ее общие и существенные взаимозависимости, представляющие интерес для системы. Преобразование информации на этапе обработки (как и на других этапах) осуществляется либо средствами информационной техники, либо человеком. Если процесс обработки формализуем, он может выполняться техническими средствами. В современных сложных системах эти функции возлагаются на ЭВМ и микропроцессоры. Если процесс обра-

ботки не поддается формализации и требует творческого подхода, обработка информации осуществляется человеком. В системах управления важнейшей целью обработки является решение задачи выбора управляющих воздействий (этап *принятия решения*).

Этап *отображения* информации должен предшествовать этапам, связанным с участием человека. Цель этапа отображения – предоставить человеку нужную ему информацию с помощью устройств, способных воздействовать на его органы чувств.

На этапе *воздействия* информация используется для осуществления необходимых изменений в системе.

Тема 16. Система передачи информации

Структурная схема *одноканальной системы передачи информации* приведена на рис. 2.2. Информация поступает в систему в форме сообщений. Под *сообщением* понимают совокупность знаков или первичных сигналов, содержащих информацию. *Источник сообщений* в общем случае образует совокупность *источника информации* (ИИ) – исследуемого или наблюдаемого объекта и *первичного преобразователя* (ПП) – датчика, человека-оператора и т. п., воспринимающего информацию о состоянии объекта или протекающем в нем процессе. Различают дискретные и непрерывные сообщения.

Дискретные сообщения формируются в результате последовательной выдачи источником отдельных элементов – знаков. Множество различных знаков называют *алфавитом источника* сообщений, а число знаков – *объемом алфавита*. В частности, знаками могут быть буквы естественного или искусственного языка, удовлетворяющие определенным правилам взаимосвязи. Распространенной разновидностью дискретных сообщений являются *данные*.

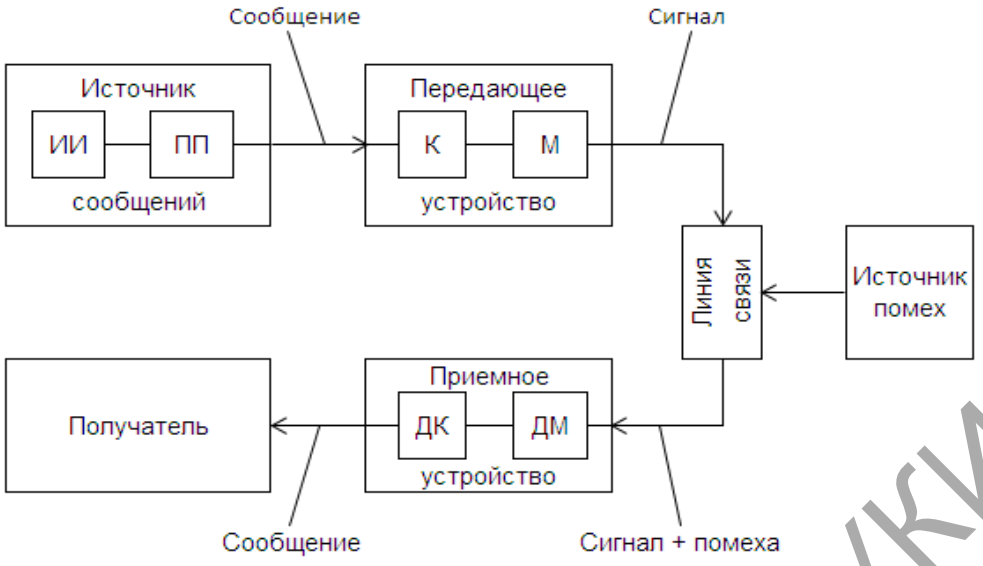


Рис. 2.2. Структурная схема передачи информации

Непрерывные сообщения не разделимы на элементы. Они описываются функциями времени, принимающими непрерывное множество значений. Типичными примерами непрерывных сообщений могут служить речь, телевизионное изображение. В ряде систем связи непрерывные сообщения с целью повышения качества передачи преобразуются в дискретные.

Для передачи сообщения по каналу связи ему необходимо поставить в соответствие определенный *сигнал*. В информационных системах под сигналом понимают физический процесс, отображающий (несущий) сообщение. Преобразование сообщения в сигнал, удобный для передачи по данному каналу связи, называют *кодированием* в широком смысле слова. Операцию восстановления сообщения по принятому сигналу называют *декодированием*.

Так как число возможных дискретных сообщений при неограниченном увеличении времени стремится к бесконечности, а за достаточно большой промежуток времени весьма велико, то ясно, что создать для каждого сообщения свой сигнал практически невозможно. Однако, поскольку дискретные сообщения складываются из знаков, имеется возможность обойтись конечным числом *образцовых сигналов*, соответствующих отдельным знакам алфавита источника.

Для обеспечения простоты и надежности распознавания образцовых сигналов их число целесообразно сократить до минимума. Поэтому, как правило, прибегают к операции представления исходных знаков в другом алфавите с меньшим числом знаков, называемых символами. При обозначении этой операции используется тот же термин «кодирование», рассматриваемый в узком смысле. Устройство, выполняющее такую операцию, называют *кодирующим* или кодером (К). Так как алфавит символов меньше алфавита знаков, то каждому знаку соответствует некоторая последовательность символов, которую назовем *кодовой комбинацией*. Число символов в кодовой комбинации называют ее значностью, число ненулевых символов – *весом*.

Аналогично, для операции сопоставления символов со знаками исходного алфавита используется термин «*декодирование*». Техническая реализация ее осуществляется *декодирующим устройством*, или декодером (ДК). В простейшей системе связи кодирующее, а следовательно, и декодирующее устройство может отсутствовать.

Передающее устройство осуществляет преобразование непрерывных сообщений или знаков в сигналы, удобные для прохождения по конкретной линии связи (либо для хранения в некотором запоминающем устройстве). При этом один или несколько параметров выбранного носителя изменяют в соответствии с передаваемой информацией. Такой процесс называют модуляцией. Он осуществляется модулятором (М). Обратное преобразование сигналов в символы производится демодулятором (ДМ).

Под линией связи понимают любую физическую среду (воздух, металл, магнитную ленту и т. п.), обеспечивающую поступление сигналов от передающего устройства к приемному. Сигналы на выходе линии связи могут отличаться от переданных вследствие затухания, искажения и воздействия помех. Помехами называют любые мешающие возмущения, как внешние (атмосферные помехи, промышленные помехи), так и

внутренние (источником которых является сама аппаратура связи), вызывающие случайные отклонения принятых сигналов от переданных. Эффект воздействия помех на различные блоки системы стараются учесть эквивалентным изменением характеристик линии связи. Поэтому источник помех условно относят к линии связи.

Из смеси сигнала и помех приемное устройство выделяет сигнал и посредством декодера восстанавливает сообщение, которое в общем случае может отличаться от посланного. Меру соответствия принятого сообщения посланному называют верностью передачи. Обеспечение заданной верности передачи сообщений – важнейшая цель системы связи.

Принятое сообщение с выхода системы связи поступает к абоненту-получателю, которому была адресована исходная информация.

Совокупность средств, предназначенных для передачи сообщений, называют каналом связи. Для передачи информации от группы источников, сосредоточенных в одном пункте, к группе получателей, расположенных в другом пункте, часто целесообразно использовать только одну линию связи, организовав на ней требуемое число каналов. Такие системы называют многоканальными.

Обмен информацией предполагает использование некоторой системы знаков, например, естественного или искусственного (формального) языка. Информация о непрерывных процессах также может быть выражена посредством знаков.

Изучение знаковых систем наукой о знаках, словах и языках (семиотикой) проводится, по крайней мере, на четырех уровнях:

– *морфологическом* – рассматривается алфавит сообщений, форма представления сигналов или данных (аналоговые, дискретные);

– *синтактическом* – рассматривают внутренние свойства текстов, т. е. отношения между знаками, отражающие структуру данной знаковой системы. Внешние свойства текстов изучают на семантическом и прагматическом уровнях;

– *семантическом* – анализируют отношения между знаками и обозначаемыми ими предметами, действиями, качествами, т. е. смысловое содержание текста, его отношение к источнику информации;

– *прагматическом* – рассматривают отношения между текстом и теми, кто его использует, т. е. потребительское содержание текста, его отношение к получателю.

Учитывая определенную взаимосвязь *проблем передачи информации* с уровнями изучения знаковых систем, их разделяют на проблемы морфологического, синтактического, семантического и прагматического уровней.

Проблемы синтактического уровня касаются создания теоретических основ построения систем связи, основные показатели функционирования которых были бы близки к предельно возможным, а также совершенствования существующих систем с целью повышения эффективности их использования. Это чисто технические проблемы совершенствования методов передачи сообщений и их материального воплощения – сигналов. Иначе говоря, на этом уровне решаются проблемы доставки получателю сообщений как совокупности знаков, при этом полностью абстрагируемся от их смыслового и прагматического содержания.

Основу интересующей нас теории информации составляют результаты решения ряда проблем именно этого уровня. Она опирается на понятие «количество информации», являющееся мерой частоты употребления знаков, которая никак не отражает ни смысла, ни важности передаваемых сообщений. В связи с этим иногда говорят, что теория информации находится на синтактическом уровне.

Проблемы семантического уровня связаны с формализацией смысла передаваемой информации, например, введением количественных оценок близости информации к истине, т. е. оценок ее качества. Эти проблемы чрезвычайно сложны, так как смысловое содержание информации больше зависит от получателя, чем от семантики сообщения, представленного в ка-

ком-либо языке. Информация заложена в сообщении, но проявляется она только при взаимодействии с получателем, так как может быть зашифрована. Из полученной телеграммы адресат может извлечь совершенно другую информацию по сравнению с той, которая будет доступна работнику телеграфа. Если получатель – человек, то и незашифрованное (или правильно расшифрованное) сообщение может быть понято поразному. Основная причина состоит в том, что различное понимание того или иного слова может сильно изменить смысл переданной информации. Кроме того, восприятие человеком информации зависит от его эмоционального состояния, накопленного жизненного опыта и других факторов.

Следует отметить, что мы еще не умеем измерять семантическую информацию. Имевшие место подходы к ее измерению пока носили весьма частный характер.

На прагматическом уровне интересуют последствия от получения и использования данной информации абонентом. Проблемы этого уровня – это проблемы эффективности. Основная сложность здесь состоит в том, что ценность или потребительская стоимость информации может быть совершенно различной для различных получателей. Кроме того, она существенно зависит от истинности и прогностичности информации, своевременности ее доставки и использования. Высокие требования к скорости доставки информации часто диктуются тем, что управляющие воздействия должны осуществляться в реальном масштабе времени, т. е. со скоростью изменения состояния управляемых объектов или процессов. Задержки в доставке или использовании информации могут иметь катастрофические последствия.

В направлении количественного определения прагматического содержания информации сделаны лишь первые шаги. Предложен ряд количественных мер, которые еще недостаточно конструктивны, чтобы найти широкое практическое применение. В связи с созданием информационно-вычислительных сетей ведутся интенсивные исследования в области оценки старения информации, т. е. потери ее ценности в процессе доставки.

Возникновение теории передачи информации связывают обычно с появлением фундаментальной работы американского ученого К. Шеннона «Математическая теория связи» (1948 г.). Однако в теорию информации органически вошли и результаты, полученные другими учеными, например Р. Хартли, впервые предложившим количественную меру информации (1928 г.), академиком В. А. Котельниковым, сформулировавшим важнейшую теорему о возможности представления непрерывной функции совокупностью ее значений в отдельных точках отсчета (1933 г.) и разработавшим оптимальные методы приема сигналов на фоне помех (1946 г.), академиком А. Н. Колмогоровым, внесшим огромный вклад в статистическую теорию колебаний, являющуюся математической основой теории передачи информации (1941 г.).

В последующие годы теория информации получила дальнейшее развитие в трудах советских ученых (А. Н. Колмогорова, А. Я. Хинчина, В. И. Сифорова, Р. Л. Добрушина, М. С. Пинскера, А. Н. Железнова, Л. М. Финка и др.), а также ряда зарубежных ученых (В. Макмиллана, А. Файнстейна, Д. Габора, Р. М. Фано, Ф. М. Вудворта, С. Гольдмана, Л. Бриллюэна и др.).

К *теории передачи информации* в ее узкой классической постановке относят результаты решения ряда фундаментальных теоретических вопросов, касающихся повышения эффективности функционирования систем связи. Это в первую очередь:

– анализ сигналов как средства передачи сообщений, включающий вопросы оценки переносимого ими «количества информации»;

– анализ информационных характеристик источников сообщений и каналов связи и обоснование принципиальной возможности кодирования и декодирования сообщений, обеспечивающих предельно допустимую скорость передачи сообщений по каналу связи, как при отсутствии, так и при наличии помех.

Прикладные результаты приводятся здесь только для пояснения основ теории. При более широкой трактовке теории ин-

формации результаты рассмотрения указанных вопросов составляют ее основу.

Если расширение связано с приложением теории в технике связи – рассмотрением проблемы разработки конкретных методов и средств кодирования сообщений, то совокупность излагаемых вопросов называют теорией информации и кодирования, или прикладной теорией информации.

Другая точка зрения состоит в том, что глобальной проблемой теории передачи информации следует считать разработку принципов оптимизации системы связи в целом. В этом случае к ней относят все локальные проблемы систем связи, включая, например, проблему оптимального приема и др.

С широкой точки зрения теория передачи информации является только узкой специфичной областью, к которой относят все проблемы и задачи, в формулировку которых входит понятие информации. Ее предметом считают изучение процессов, связанных с получением, передачей, хранением, обработкой и использованием информации. В такой постановке она затрагивает проблемы многих наук (в частности кибернетики, биологии, психологии, лингвистики, педагогики) на всех трех уровнях (синтактическом, семантическом и прагматическом).

Попытки широкого использования идей теории передачи информации в различных областях науки связаны с тем, что в основе своей эта теория математическая. Основные ее понятия (энтропия, количество информации, пропускная способность) определяются только через вероятности событий, которым может быть приписано самое различное физическое содержание. Подход к исследованиям в других областях науки с позиций использования основных идей теории передачи информации получил название теоретико-информационного подхода. Его применение в ряде случаев позволило получить новые теоретические результаты и ценные практические рекомендации. Однако нередко такой подход приводит к созданию моделей процессов, далеко не адекватных реальной действительности. Поэтому в любых исследованиях, выходящих за рамки чисто

технических проблем передачи и хранения сообщений, теорией передачи информации следует пользоваться с большой осторожностью. Особенно это касается моделирования умственной деятельности человека, процессов восприятия и обработки им информации.

Содержание данной лекции ограничивается теорией информации в узкой трактовке, то есть теорией передачи информации, а именно вопросами теории и практики кодирования и некоторыми примерами применения теории передачи информации в областях, смежных с техникой связи.

Прикладная теория передачи информации является одним из фундаментальных курсов при подготовке инженеров-системотехников, специализирующихся в области автоматизированных систем управления. Функционирование таких систем существенным образом связано с получением, подготовкой, передачей, хранением и обработкой информации, поскольку без осуществления этих этапов невозможно принять правильное решение, а следовательно, и осуществить требуемое управляющее воздействие, которое является конечной целью функционирования системы.

Рассмотрим подробнее понятие «сигнал». Оно имеет неоднозначное толкование. В широком смысле слова под сигналом понимают материальный носитель информации, передаваемый на расстояние. При этом к сигналам относят как естественные сигналы, так и сигналы, специально создаваемые с определенной целью. Естественными являются, например, световые сигналы, позволяющие видеть окружающий мир, космические сигналы. Примером специально создаваемых могут служить сигналы, генерируемые с целью извлечения информации об изменениях в объекте или процессе (эталонные сигналы).

В дальнейшем понятие «сигнал», если это не оговорено специально, будет использоваться в узком смысле как сигнал, специально создаваемый для передачи сообщения в информационной системе. Материальную основу сигнала составляет какой-либо физический объект или процесс, называемый носи-

телем (переносчиком) информации (сообщения). Носитель становится сигналом в процессе модуляции. Параметры носителя, изменяемые во времени в соответствии с передаваемым сообщением, называют *информативными*.

В качестве носителей информации используются колебания различной природы, чаще всего *гармонические*, включая частный случай – постоянное состояние (ω = 0). В технических информационных системах наиболее широкое распространение получили носители в виде электрического напряжения или тока. Поэтому, рассматривая в дальнейшем модели сигналов, для конкретности будем соотносить их с электрическими сигналами.

В носителе u(t) = const имеется только один информативный параметр – *уровень* (например, уровень напряжения). При использовании гармонических электрических колебаний информативными могут стать такие параметры, как амплитуда, частота, фаза. Колебания принято подразделять на детерминированные и случайные.

Детерминированными называют колебания, которые точно определены в любые моменты времени.

Случайные колебания отличаются тем, что значения их некоторых параметров предсказать невозможно. Они могут рассматриваться как сигналы, когда несут интересующую нас информацию (случайные сигналы), или как помехи, когда мешают наблюдению интересующих нас сигналов.

При изучении общих свойств каналов связи, сигналов и помех мы отвлекаемся от их конкретной физической природы, содержания и назначения, заменяя моделями. *Модель* – это выбранный способ описания объекта, процесса или явления, отражающий существенные с точки зрения решаемой задачи факторы.

Задачи повышения эффективности функционирования информационных систем связаны с установлением количественных соотношений между основными параметрами, характеризующими источник информации и канал связи. Поэтому при исследовании используют *математические модели*. Матема-

тическое моделирование может быть реализовано различными методами в зависимости от способа, которым определяются интересующие нас показатели.

Фундаментальные исследования базируются на методе *аналитического моделирования*, заключающемся в создании совокупности математических соотношений, позволяющих выявить зависимости между параметрами модели в общем виде. При этом широко используются модели, параметры которых противоречат физическим свойствам реальных объектов. Например, модель сигнала часто представляется суммой бесконечного числа функций (синусоид), имеющих неограниченную продолжительность. Поэтому важно обращать внимание на условия, при которых это не мешает получать результаты, соответствующие наблюдаемым в действительности.

Так как источник сообщений выдает каждое сообщение с некоторой вероятностью, то предсказать точно изменения значения информативного параметра невозможно. Следовательно, сигнал принципиально представляет собой *случайное колебание* и его аналитической моделью может быть только случайный процесс, определяемый вероятностными характеристиками.

Тем не менее, в случае детерминированного колебания условно также говорят о *детерминированном сигнале*. Такой сигнал отображает известное сообщение, которое нет смысла передавать. Ему соответствует модель в виде функции, полностью определенной во времени.

Изучение моделей детерминированных сигналов необходимо по многим причинам. Важнейшая из них заключается в том, что результаты анализа детерминированных сигналов являются основой для изучения более сложных случайных сигналов. Это обусловлено тем, что детерминированный сигнал может рассматриваться как элемент множества детерминированных функций, составляющих в совокупности случайный процесс. *Детерминированное колебание*, таким образом, представляет собой вырожденную форму случайного процесса со значениями параметров, известными в любой момент времени с вероят-

ностью, равной единице. Детерминированные сигналы имеют и самостоятельное значение. Они специально создаются для целей измерения, наладки и регулирования объектов информационной техники, играя роль эталонов.

Тема 17. Представление информации

Большинство кодов, используемых при кодировании информации без учета статистических свойств источника и помех в канале связи, основано на системах счисления (двоичной, десятичной, восьмеричной, шестнадцатеричной).

Общепризнанным в настоящее время является *позиционный принцип образования системы счисления*. Значение каждого символа (цифры) зависит от его положения – позиции в ряду символов, представляющих число. Единица каждого следующего разряда больше единицы предыдущего в m раз, где m – основание системы счисления. Полное число получаем, суммируя значения по разрядам (пример: в десятичном коде 111_{10} m =10, младший разряд – 1, второй – 10, третий – 100, то есть единица старшего разряда в десять раз больше единицы предыдущего разряда – единицы, десятки, сотни; также и в других системах счисления).

Чем больше основание системы счисления, тем меньшее число разрядов требуется для представления данного числа, а следовательно, и меньшее время для его передачи. Однако с ростом основания усложняются устройства передачи и приема сигналов, так как логические элементы в этом случае должны иметь большее число устойчивых состояний. Если учитывать оба эти обстоятельства, то целесообразно выбрать систему, обеспечивающую минимум произведения основания кода m на количество разрядов n для выражения любого числа. Найдем этот минимум по графику для большого числа 60000_{10}.

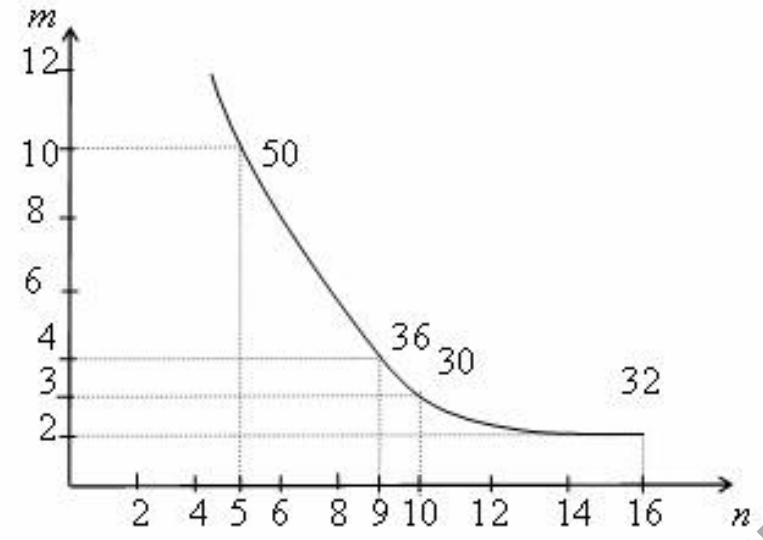


Рис. 2.3. График зависимости числа разрядов *n* от основания кода *m* для числа 60000_{10}

Из графика (рис. 2.3.) следует, что наиболее эффективной системой является троичная. Незначительно уступают ей двоичная и четверичная. Системы с основанием десять и более значительно хуже.

С точки зрения удобства физической реализации логических элементов и простоты выполнения в них арифметических и логических действий, предпочтение необходимо отдать двоичной системе.

Действительно, арифметические операции в двоичной системе достаточно просты:

Сложение	Вычитание	Умножение
0+0=0;	0 - 0=0;	0·0=0;
0+1=1;	1 - 0=1;	0·1=1;
1+0=1;	1 - 1=0;	1·0=1;
1+1=10	10 - 1=1	1·1=1

Сложение по модулю в двоичной системе также просто:

$0 \oplus 0=0;$

$0 \oplus 1=1;$

$1 \oplus 1=0;$

$1 \oplus 0=1$

Итак, для передачи и проведения логических и арифметических операций наиболее целесообразен двоичный код. Однако он неудобен при вводе и выводе информации, так как человеку трудно оперировать с непривычными двоичными числами. Кроме того, запись таких чисел на бумаге оказывается слишком громоздкой. Поэтому, помимо двоичной, получили распространение системы, которые, с одной стороны, легко сводятся как к двоичной, так и к десятичной системе, а с другой – дают более компактную запись. К таким системам относятся восьмеричная, шестнадцатеричная и двоично-десятичная.

В восьмеричной системе для записи всех возможных чисел используется восемь цифр – от нуля до семи включительно. Перевод чисел из восьмеричной системы в двоичную крайне прост и сводится к замене каждой восьмеричной цифры равным ей трехразрядным двоичным числом. Например, для восьмеричного числа 461получим:

4_8	6_8	1_8		
100	110	001	⟵	триады

Поскольку в восьмеричной системе числа выражаются короче, чем в двоичной, она широко используется как вспомогательная система при программировании (особенно для микро- и мини-ЭВМ в машинных кодах).

Чтобы сохранить преимущества двоичной системы, используют *двоично-десятичные коды*. В таком коде каждая цифра десятичного числа записывается в виде четырехразрядного двоичного числа. С помощью четырех разрядов можно образовать шестнадцать различных комбинаций, из которых любые десять могут составить двоично-десятичный код. Наиболее распространен код 8-4-2-1. Этот код относится к *взвешенным кодам*. Цифры в названии кода означают вес единиц в соответствующих двоичных разрядах. Он соответствует первым десяти комбинациям натурального двоичного кода (табл. 2.1).

Таблица 2.1

Число в десятичном коде	Двоично-десятичный код 8-4-2-1	Двоично-десятичный код 5-1-2-1
0	0000	0000
1	0001	0001
2	0010	0010
3	0011	0011
4	0100	0111
5	0101	1000
6	0110	1001
7	0111	1010
8	1000	1011
9	1001	1111

Код 8-4-2-1 обычно используется как промежуточный при введении в вычислительную машину данных, представленных в десятичном коде.

Перевод чисел из десятичного в двоично-десятичный код осуществляется перфоратором в процессе переноса информации на перфоленту или перфокарту. Последующее преобразование в двоичный код осуществляется по специальной программе в самой машине. Двоично-десятичные коды с весами 5-1-2-1 и 2-4-2-1 используются при поразрядном уравновешивании в цифровых измерительных приборах (цифровые вольтметры и т. п.).

Недостаток взвешенных кодов заключается в том, что при передаче информации по каналам связи под действием помех отдельные элементы кода могут так исказиться, что будут приняты неверно. Например, вместо «0» будет принят элемент «1» или наоборот. Если будет искажен старший разряд, то ошибка будет значительно больше, чем при искажении младшего разряда. С этой точки зрения лучше применять *невзвешенный код*, у которого ошибки, вызванные помехами, были бы одинаковыми для любого разряда.

В невзвешенных кодах позициям (разрядам) кодовой комбинации не приписывают определенных весов. Вес имеет лишь вся кодовая комбинация в совокупности. Рассмотрим невзвешенный двоичный рефлексный код Грея (табл. 2.2).

Таблица 2.2

Десятичное число	Двоичный код вес 8-4-2-1	Код Грея
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
...	...	...
15	1111	1000

Правило получения кодовой комбинации полукода сложения по модулю 2 с такой же комбинацией, сдвинутой на один разряд вправо, при этом младший разряд сдвинутой комбинации отбрасывается.

Примеры перевода двоичного кода в код Грея:

1001 – исходный текст

⊕ 100 – сдвинутый код без младшего разряда

1101 – код Грея

1111 – исходный текст

⊕ 111 – сдвинутый код без младшего разряда

1000 – код Грея

Характерные особенности кода Грея:

1) каждая последующая комбинация всегда отличается от предыдущей только в одной позиции (в одном разряде);

2) смена значений элементов в каждом разряде (1 на 0 или 0 на 1) при переходе от комбинации к комбинации в коде Грея происходит вдвое реже, чем в натуральном двоичном коде. Это свойство кода Грея позволяет получить точность кодирования выше по сравнению с натуральным двоичным кодом при том же быстродействии схемы кодирования;

3) при сложении двух соседних комбинаций кода Грея по модулю 2 (mod2) число единиц равно числу разрядов минус три (n-3). Это свойство кода Грея можно использовать для проверки правильности принятых комбинаций.

В коде Грея можно выделить оси симметрии (оси отражения), относительно которых наблюдается идентичность элементов в некоторых разрядах. Так, например, имеет место симметрия относительно оси, проведенной между числами 7 и 8 (идентичны три символа младших разрядов). Эта особенность и послужила основанием для введения термина «рефлексный», то есть отраженный код.

Рассмотренные свойства кода Грея показывают, что он удобен для аналого-цифрового преобразования различных непрерывных сообщений и их передачи по каналам связи.

Недостатком кода Грея и других рефлексных кодов является то, что эти коды невзвешенные, их трудно обрабатывать с помощью ЭВМ, так как сложнее выполнять декодирование.

Преобразование кода Грея в натуральный двоичный код выполняется по правилу: старший разряд записывается без изменения, каждый следующий символ кода Грея нужно инвертировать, если перед ним количество единиц нечетное, в противном случае оставить без изменения.

Пример: $9_{10} = 1101_{ГР} = 1001_2$.

Код Грея, как и другие отраженные коды, относится к системам счисления с неестественным распределением весов разрядов, что затрудняет обработку информации, представленной этими кодами, в ЭВМ и дешифраторах. В силу этого отражен-

ные коды перед обработкой преобразуются в простой двоичный код. Вес разрядов кода Грея определяется выражением: $q_i = 2^i - 1$, где $i = 1, 2, 3, \ldots, n$.

То есть, начиная с младшего разряда веса разрядов, запишутся следующим образом: 1, 3, 7, 15, 31… . Чтобы прочесть число в коде Грея, под каждым разрядом записывают его десятичный эквивалент, старший значащий разряд берется со знаком плюс, перед остальными значащими разрядами знаки чередуются. Например, перевод комбинации кода Грея $101111_{ГР}$ в десятичный код производится следующим образом:

1	0	1	1	1	1	= 63–15+7–3+1=53
63	31	15	7	3	1	

Проверим полученный результат. Для этого число 53 переведем в двоичный код, получим 110101_2, а затем описанным ранее способом переведем двоичный код в код Грея: $101111_{ГР}$. Таким образом, мы получили исходный код Грея и убедились в правильности перевода кода Грея в десятичный код.

Тема 18. Форматы данных в Интернете

В Интернете используется множество различных форматов данных. Некоторые из них используются довольно часто, некоторые реже. Как же связать это бесчисленное множество различных форматов с теорией информации? Данная лекция дает ответы на эти и другие вопросы. Дается понятие сущности компьютерного шрифта, текстов с разметкой и их применение, язык логической разметки HTML и TeX как язык программирования в академических кругах. Также рассматривается формат PDF как самый популярный формат создания, хранения и передачи электронных книг.

Самый распространенный тип данных в компьютерном мире – это *текстовые* файлы, которые непосредственно в той или иной мере понятны для человека, в отличие от *бинарных* файлов, ориентированных исключительно на компьютерные

методы обработки. С использованием текстовых файлов связаны две проблемы.

Первая заключается в сложности единообразного представления символов текста. Для представления английских текстов достаточно ASCII. Для работы с другими языками на основе латинского алфавита, языками на основе кириллицы и некоторыми другими нужно уже несколько десятков наборов расширенного ASCII. Это означает, что одному и тому же коду, большему 127, в каждом наборе соответствует свой символ. Ситуацию усложняет и то, что для некоторых языков, в частности, русского существует несколько наборов ASCII+. Кроме того, необходимо, чтобы все символы каждого языка помещались в один набор, что невозможно для таких языков, как китайский или японский. Таблица кодировки Unicode, предназначенная для постепенной замены ASCII, 16-разрядная, что позволяет представить 65536 кодов. Она широко используется в Linux и Microsoft Windows. Варианты Unicode позволяют использовать 31-разрядное кодирование. Использование Unicode требует переделки всех программ, рассчитанных для работы с текстами ASCII.

Для того чтобы увидеть символы, соответствующие кодам из текстового файла, каждому коду нужно сопоставить визуальное представление символа из выбранного шрифта.

Компьютерный шрифт – это набор именованных кодами рисунков знаков.

Таким образом, чтобы интерактивно работать с текстовым файлом, необходимо знать его кодировку (из текстовых файлов, как правило, прямой информации о кодировке получить нельзя – ее надо знать или угадать!) и иметь в системе шрифт, соответствующий этой кодировке.

Вторая проблема связана с тем, что такие средства, как курсивный, полужирный или подчеркнутый текст, а также графики, диаграммы, примечания, звук, видео и т. п. элементы электронных документов, выходят за рамки естественных, интуитивных элементов текста и требуют соглашений по их исполь-

зованию, что приводит к возникновению различных форматов текстовых данных. Последние иногда даже не ориентированы на непосредственную работу с ними человека, фактически не отличаясь по назначению в таких случаях от бинарных данных.

Внесение в простой текст (plain text) дополнительной информации об его оформлении или структуре осуществляется при помощи разметки текста (markup). Различают физическую, или процедурную, разметку и логическую, или обобщенную, разметку.

При физической разметке точно указывается, что нужно сделать с выбранным фрагментом текста: показать курсивным, приподнять, центрировать, сжать, подчеркнуть и т. п. При логической разметке указывается структурный смысл выбранного фрагмента: примечание, начало раздела, конец подраздела, ссылка на другой фрагмент и т. п.

Для печати документа на принтере или показе на экране используется физическая разметка. Исторически она появилась первой, но имеет очевидные недостатки. Например, в Америке и Европе существуют разные стандарты на размер писчей бумаги, наборы шрифтов и размер экрана меняются от системы к системе, – подобные обстоятельства требуют трудоемкого изменения физической разметки текста при использовании одного и того же документа на разных компьютерах. Кроме того, физическая разметка, как правило, привязана к конкретным программным средствам, время жизни которых ограничено, что не позволяет вести архивы документации без риска через несколько десятков лет остаться без средств для работы с ними.

Логическую разметку всегда можно преобразовать в физическую, используя таблицу стилей, которая представляет собой перечисление способов отображения каждого логического элемента. Таким образом, имея наборы документов в логической разметке, можно всегда при печати придавать им наиболее привлекательный вид, своевременно получая от специалистов-дизайнеров новейшие таблицы стилей. Преобразование

физической разметки в логическую формальными средствами практически невозможно.

Основные форматы текста с разметкой:

1) HTML – Hyper Text Markup Language, язык разметки гипертекста;

2) XML – eXtensible Markup Language, расширяемый язык разметки;

3) SGML – Standard Generalized Markup Language, стандартный язык обобщенной разметки;

4) TeX;

5) PostScript;

6) PDF – Portable Document Format, формат для переносимых документов, или Acrobat (частично бинарный).

Документы в Internet часто публикуются в виде, обработанном программами сжатия данных. Наиболее используемые форматы сжатия – это zip и tgz (tar.gz). Формат tgz – это результат конвейерного применения команд: сначала tar (собирает файлы и каталоги в один файл с сохранением структуры каталогов) и затем gzip.

Часто в Internet нужно преобразовывать бинарные данные в текстовые (для отправки по электронной почте, например) и затем наоборот. Для этого, в частности, служат программы uuencode (перевести в текст) и uudecode (перевести из текста). В текстовом файле закодированный текстом бинарный файл помещается между строками, начинающимися со слов begin и end. Строка begin должна содержать атрибуты и имя бинарного файла.

World Wide Web (WWW, всемирная паутина) базируется на трех стандартах: URI (Universal Resource Identifier, универсальный идентификатор ресурса, раньше назывался URL) – предоставляет стандартный способ задания местоположения любого ресурса Internet, HTTP (Hyper Text Transfer Protocol, протокол передачи гипертекста), HTML – язык страниц WWW.

HTML – язык логической разметки, хотя и допускающий возможность рекомендовать ту или иную физическую размет-

ку выбранного фрагмента текста. Конкретная физическая разметка документа зависит от программы-браузера (browser), используемой для его просмотра. Документы HTML из-за содержащихся в них, как правило, большого количества ссылок на другие документы HTML, с которыми они образуют единое целое, мало приспособлены для распечатки на принтере.

Имя файла с документом HTML имеет обычно расширение html или htm. Существует ряд программ, позволяющих создавать документы HTML в визуальном режиме и не требующих от их пользователя знания HTML. Но создать сложный интерактивный документ без такого знания непросто.

Элементы разметки HTML состоят из тегов (tag). Теги заключаются в угловые скобки, у них, как правило, есть имя и они могут иметь дополнительные атрибуты. Например, тег <A HREF=«http://www.linux.org»> имеет имя A (anchor, якорь), атрибут HREF со значением «http://www.linux.org».

Некоторые теги самодостаточны, например, тег разрыва строки
 (break), но большинство тегов – это пары из открывающего (start tag) и закрывающего (end tag) тегов. Имя закрывающего тега отличается от имени открывающего только тем, что перед ним ставится наклонная черта (slash). Например, если имя открывающего тега A, то имя закрывающего – /A. Открывающий и закрывающий теги обрамляют некоторый фрагмент текста, вместе с которым они образуют элемент текста. Элементы текста могут быть вложенными.

Парные теги EM (emphasis, выделение), STRONG (особо выделить), CITE (цитата или ссылка), CODE (компьютерная программа), SAMP (sample, текст примера), STRIKE (зачеркнуть) и некоторые другие позволяют логически выделить фрагменты текста, а парные теги B (bold, полужирный), I (italic, курсив), U (undelined, подчеркнутый), TT (typewriter, пишущая машинка), SUB (subscript, нижний индекс), SUP (superscript, верхний индекс) и другие – рекомендовать физически выделить фрагмент текста указанным образом.

Полный документ представляет собой один элемент текста HTML. Заголовки – это элементы H1, H2, H3 и т. д. Число по-

сле H (header) – это уровень вложенности заголовка, т. е. H1 – это заголовок всего документа, H2 – заголовок раздела документа, H3 – подраздела и т. д. Абзацы – это элементы P (paragraph). Элементы PRE (preformatted) должны отображаться браузером с таким же разбиением на строки как и в исходном документе.

Специальные символы можно ввести в документ, используя их имена (entity), заключенные между знаками & и точка с запятой. Например, сам знак & можно ввести как &, а знак кавычка – ".

Ссылки и маркеры объявляются при помощи атрибутов HREF и NAME соответственно. Например, элемент <A NAME=«chapter3»></A> – это метка, на которую можно ссылаться по имени chapter3, используя, например, ссылку <A HREF=«\#chapter3»>Глава 3</A>.

Тег IMG (image, образ) позволяет вставить графическую картинку в документ, используя два основных атрибута: SRC (source, источник) для указания URI файла с графикой и ALT (alternative, альтернатива) для указания альтернативного текста, показываемого вместо картинки, в случае, когда файл с графикой недоступен или его тип неизвестен браузеру.

Документы HTML могут быть использованы для интерактивной работы. Например, элемент FORM позволяет пользователю web-страницы передать введенную в страницу информацию на HTTP-сервер. Элемент FORM может содержать разнообразные кнопки, списки, всплывающие меню, однострочные и многострочные текстовые поля и другие компоненты. Обработкой введенных, переданных на сервер данных и созданием динамических HTML-документов в ответ на них занимаются специальные программы, CGI-скрипты (common gate interface), установленные на сервере.

Комментарии вводятся между символами <!-{}- и -{}->.

HTML содержит средства для описания данных в виде таблиц и использования таблиц стилей. HTML использует стандартные системные шрифты, т. е. не существует шрифтов специально для www-страниц.

Имена файлов-документов SGML, как правило, имеют расширение sgml. SGML с начала 1970-х гг. разрабатывался фирмой IBM, а с 1986 г. принят в качестве международного стандарта (ISO 8879) для формата документов с логической разметкой. Сначала документ SGML содержит описание вида кодирования и разметки текста и затем сам размеченный текст. HTML – это SGML с фиксированной разметкой. Создатели технологии WWW отказались от полной поддержки SGML только потому, что в начале 1990-х гг. системы, которые могли работать с SGML в реальном времени были очень дороги.

Элементы SGML делятся на четыре категории:

1) описательные маркеры – определяют структуру документа – им соответствуют элементы разметки HTML типа H1, P, A, IMG и т. п.;

2) ссылки на данные – им соответствуют элементы разметки HTML типа &

3) описательные конструкции компонент документа в их структурной взаимосвязи – не входят в HTML, но определяют его. Их рекомендуется начинать с комбинации знаков <! и заканчивать знаком >>. Примером конструкции, определяющей ссылку &ref; на словосочетание «The Reference» будет <!ENTITY ref «The Reference»>;

4) инструкции по обработке текста – их рекомендуется заключать между знаками <? и > – вводят элементы текста, ориентированного на конкретную, зависящую от системы обработку (физическую разметку). В HTML с их помощью, например, вставляют код для обработки на сервере WWW страниц.

Документы SGML можно конвертировать как в гипертекст, так и в любой формат, ориентированный на распечатку, например, TeX или Microsoft Word. Ведение документации в формате SGML во многих отношениях оптимально.

С 1996 г. официально идет разработка формата XML – подмножества SGML, которое предполагается использовать в Internet наряду с HTML. Преимущество XML перед HTML в его четкой связи с SGML, что позволяет стандартным образом

вводить в документ новые конструкции, избегая тем самым неконтролируемого введения в язык новых возможностей, как это происходит с HTML.

Известный американский математик и теоретик программирования Дональд Кнут (D. E. Knuth) более 10 лет с конца 1970-х гг. разрабатывал систему верстки книг TeX (произносится «тех»). Существует множество расширений возможностей базового (plain) TeX. TeX популярен, прежде всего, в академических кругах, т. к. в целом он весьма сложен для изучения. В отличие от систем, ориентированных на интерпретацию разметки, подобных Microsoft Word или Sun Star Writer, TeX – компилирующая система. Результат компиляции документа TeX – это файл в бинарном формате dvi (device independent), который можно, используя драйверы конкретных устройств (принтеров, экрана), распечатать. TeX применяет собственную систему масштабируемых шрифтов, которые масштабируются не в реальном времени интерпретацией как шрифты True Type или PostScript, а компиляцией при помощи программы METAFONT. В Internet доступны тексты программ TeX и METAFONT – они написаны на Паскале. Шрифты METAFONT написаны на специальном языке, с декларативным синтаксисом. TeX позволяет также использовать шрифты True Type и Adobe Type 1 и Type 3. Прочитать и понять содержимое документа TeX несложно, но скомпилировать и распечатать, а тем более создать новый документ без помощи специалиста или основательной подготовки непросто. Однако TeX до сих пор является почти единственной доступной бесплатно системой, позволяющей получать документы типографского качества. В plain TeX используется физическая разметка, а в наиболее популярном его расширении LaTeX также и логическая. TeX – это язык макросов, большинство из которых начинаются с символа обратная косая черта и состоят затем из букв. Например, запись в документе plain TeX \centerline{Это {\ it мой} заголовок} означает центрировать строку-абзац «Это

мой заголовок», напечатав слово «мой» в нем курсивом, а запись $$\int_1^{}x\{dt\ over t}=\ln x$$ – формулу

$$\int_1^x \frac{dt}{t} = \ln x$$

TeX – это особый язык программирования. Энтузиасты TeX написали на нем интерпретатор языка Бэйсик. Документы TeX могут иметь очень сложную структуру и поэтому их в общем случае нельзя конвертировать в другие форматы. Документы HTML или Microsoft Word теоретически можно всегда конвертировать в формат TeX.

Система GNU texinfo основана на TeX, но использует совершенно другой набор макросов. Макросы в этой системе должны начинаться со знака @. Документы texinfo можно преобразовать как в документ HTML, так и в качественную распечатку. В отличие от SGML, средства для такого преобразования – это часть системы texinfo. Возможности texinfo для верстки документов несколько ограниченней по сравнению с другими развитыми TeX-системами.

Расширения имен файлов документов TeX – tex; LaTeX – tex, latex, ltx, sty (стили) и др.; METAFONT – mf (исходные программы шрифтов), tfm (метрики шрифтов, нужны на этапе компиляции документа TeX), pk (матрицы шрифтов, нужны при печати dvi-файла); texinfo – texi, texinfo.

PostScript – это универсальный язык программирования (имеет много общего с языками Форт и Лисп), предоставляющий большой набор команд для работы с графикой и шрифтами. Он является фактическим международным стандартом издательских систем. Разрабатывается фирмой Adobe Systems с первой половины 1980-х гг. Используется как встроенный язык принтеров для высококачественной печати, а также некоторыми системами X Window при выводе данных на экран дисплея. Существуют и программы-интерпретаторы языка PostScript. Лучшая из них – это Ghostscript. Программа GhostView пре-

доставляет удобный оконный интерфейс для Ghostscript и существует для большинства ОС.

PostScript-программы можно писать вручную, но обычно текст PostScript генерируется автоматически программами вывода данных. Расширения имен файлов с PostScript-программой – это, как правило, ps, eps (Encapsulated PostScript, файл-картинка с заданными размерами), pfa (шрифт), pfb (бинарное представление pfa), afm (метрики шрифта, могут быть частично получены из соответствующего pfa-файла), pfm (бинарное представление afm).

Преимущество формата PostScript в том, что он, как и формат DVI, независим от физических устройств воспроизведения. Один и тот же PostScript-файл можно выводить как на экран с разрешением 72 dpi (dot per inch, точек на дюйм) или лазерный принтер с разрешением 600 dpi, так и на типографскую аппаратуру с разрешением 2400 dpi, имея гарантии, что изображение будет наилучшего качества, возможного на выбранной аппаратуре. Возможности PostScript перекрывают возможности DVI, поэтому некоторые TeX-системы при компиляции документов производят сразу файлы в формате PostScript или PDF.

Файлы PostScript можно вручную корректировать, но из-за сложности языка – это очень непросто, особенно если используются символы, не входящие в ASCII. Фактически эти файлы можно рассматривать как «только для чтения» и использовать для распространения информации, не подлежащей изменению. Комментарии в PostScript, как и в TeX, начинаются знаком % и заканчиваются концом строки. Первая строчка PostScript-программы обычно содержит точное название формата файла. Собственно программа начинается в файле с символов %! и заканчивается символами %%EOF. PostScript-программы кроме собственной системы шрифтов могут использовать шрифты True Type фирм Apple и Microsoft.

Различают уровни (levels) языка PostScript. Уровень 1 может поддерживать только черно-белую графику. Уровень 2 может работать с цветом. Уровень 3 – это современное состояние языка.

Данные из файла PostScript можно показывать по мере их поступления, что удобно для использования в Internet. Однако есть две причины, по которым документы PostScript сравнительно редко включаются в web-страницы:

1) они весьма велики по размерам (этот недостаток снимается программами сжатия, работающими в реальном времени);

2) они могут содержать в себе шрифты, защищенные авторскими правами (шрифты их владелец может использовать при печати, но не распространять).

Файлы в формате PDF лишены двух означенных недостатков: они сжаты и из них сложно извлечь отдельные шрифты, – поэтому они стали фактическим стандартом Internet для обмена документами, не подлежащими изменению. Программы для просмотра PDF-файлов доступны бесплатно. Наиболее используемая из них – это Adobe Acrobat Reader. Первая строчка файла в формате PDF начинается со знака %, за которым следует идентификационная запись версии формата PDF, используемой в этом файле. Далее, как правило, идут бинарные данные. Расширение имени PDF-файла – pdf.

Между документами PostScript и PDF можно осуществлять взаимно-однозначное преобразование, хотя PDF в отличие от PostScript – это не язык программирования, а скорее язык описания документа.

Тема 19. Сжатие информации

Сжатие данных – алгоритмическое преобразование данных, производимое с целью уменьшения их объема. Применяется для более рационального использования устройств хранения и передачи данных. Синонимы – упаковка данных, компрессия, сжимающее кодирование, кодирование источника. Обратная процедура называется восстановлением данных (распаковкой, декомпрессией).

Сжатие основано на устранении избыточности, содержащейся в исходных данных. Простейшим примером избыточности является повторение в тексте фрагментов (например, слов

естественного или машинного языка). Подобная избыточность обычно устраняется заменой повторяющейся последовательности ссылкой на уже закодированный фрагмент с указанием его длины. Другой вид избыточности связан с тем, что некоторые значения в сжимаемых данных встречаются чаще других. Сокращение объема данных достигается за счет замены часто встречающихся данных короткими кодовыми словами, а редких – длинными (энтропийное кодирование). Сжатие данных, не обладающих свойством избыточности (например, случайный сигнал или шум, зашифрованные сообщения), принципиально невозможно без потерь.

В основе любого способа сжатия лежит модель источника данных, или точнее, модель избыточности. Иными словами, для сжатия данных используются некоторые априорные сведения о том, какого рода данные сжимаются. Не обладая такими сведениями об источнике, невозможно сделать никаких предположений о преобразовании, которое позволило бы уменьшить объем сообщения. Модель избыточности может быть статической, неизменной для всего сжимаемого сообщения, либо строиться или параметризоваться на этапе сжатия (и восстановления). Методы, позволяющие на основе входных данных изменять модель избыточности информации, называются адаптивными. Неадаптивными являются обычно узкоспециализированные алгоритмы, применяемые для работы с данными, обладающими хорошо определенными и неизменными характеристиками. Подавляющая часть достаточно универсальных алгоритмов – в той или иной мере адаптивные.

Все методы сжатия данных делятся на два основных класса:

– сжатие без потерь,

– сжатие с потерями.

При использовании сжатия без потерь возможно полное восстановление исходных данных, сжатие с потерями позволяет восстановить данные с искажениями, обычно несущественными с точки зрения дальнейшего использования восстановленных данных. Сжатие без потерь обычно используется для

передачи и хранения текстовых данных, компьютерных программ, реже – для сокращения объема аудио- и видеоданных, цифровых фотографий и т. п., в случаях, когда искажения недопустимы или нежелательны. Сжатие с потерями, обладающее значительно большей, чем сжатие без потерь, эффективностью, также применяется для сокращения объема аудио- и видеоданных и цифровых фотографий в тех случаях, когда такое сокращение является приоритетным, а полное соответствие исходных и восстановленных данных не требуется.

Коэффициент сжатия – основная характеристика алгоритма сжатия. Она определяется как отношение объема исходных несжатых данных к объему сжатых, то есть:

$$k = S_o/S_c,$$

где k – коэффициент сжатия, S_o – объем исходных данных, а S_c – объем сжатых. Таким образом, чем выше коэффициент сжатия, тем алгоритм эффективнее. Следует отметить:

– если $k = 1$, то алгоритм не производит сжатия, то есть выходное сообщение оказывается по объему равным входному;

– если $k < 1$, то алгоритм порождает сообщение большего размера, нежели несжатое, то есть, совершает «вредную» работу.

Ситуация с $k < 1$ вполне возможна при сжатии. Принципиально невозможно получить алгоритм сжатия без потерь, который при любых данных образовывал бы на выходе данные меньшей или равной длины. Обоснование этого факта заключается в том, что поскольку число различных сообщений длиной n бит составляет ровно 2^n, число различных сообщений с длиной меньшей или равной n (при наличии хотя бы одного сообщения меньшей длины) будет меньше 2^n. Это значит, что невозможно однозначно сопоставить все исходные сообщения сжатым: либо некоторые исходные сообщения не будут иметь сжатого представления, либо нескольким исходным сообщениям будет соответствовать одно и то же сжатое, а значит их нельзя отличить.

Коэффициент сжатия может быть как постоянным (некоторые алгоритмы сжатия звука, изображения и т. п., например

A-закон, μ-закон, ADPCM, усеченное блочное кодирование), так и переменным. Во втором случае он может быть определен либо для каждого конкретного сообщения, либо оценен по некоторым критериям:

– средний (обычно по некоторому тестовому набору данных);

– максимальный (случай наилучшего сжатия);

– минимальный (случай наихудшего сжатия);

– или каким-либо другим.

Коэффициент сжатия с потерями при этом сильно зависит от допустимой погрешности сжатия, или *качества*, которое обычно выступает как параметр алгоритма. В общем случае постоянный коэффициент сжатия способны обеспечить только методы сжатия данных с потерями.

Основным критерием различия между алгоритмами сжатия является описанное выше наличие или отсутствие потерь. В общем случае алгоритмы сжатия без потерь универсальны в том смысле, что их применение безусловно возможно для данных любого типа, в то время как возможность применения сжатия с потерями должна быть обоснована. Для некоторых типов данных искажения не допустимы в принципе. В их числе:

– символические данные, изменение которых неминуемо приводит к изменению их семантики: программы и их исходные тексты, двоичные массивы и т. п.;

– жизненно важные данные, изменения в которых могут привести к критическим ошибкам: например, получаемые с медицинской измерительной аппаратуры или контрольных приборов летательных, космических аппаратов и т. п.;

– многократно подвергаемые сжатию и восстановлению промежуточные данные при многоэтапной обработке графических, звуковых и видеоданных.

Различные алгоритмы могут требовать различного количества ресурсов вычислительной системы, на которых они реализованы:

– оперативной памяти (под промежуточные данные);

– постоянной памяти (под код программы и константы);

– процессорного времени.

В целом, эти требования зависят от сложности и «интеллектуальности» алгоритма. Общая тенденция такова: чем эффективнее и универсальнее алгоритм, тем большие требования к вычислительным ресурсам он предъявляет. Тем не менее, в специфических случаях простые и компактные алгоритмы могут работать не хуже сложных и универсальных. Системные требования определяют их потребительские качества: чем менее требователен алгоритм, тем на более простой, а следовательно, компактной, надежной и дешевой системе он может быть реализован.

Так как алгоритмы сжатия и восстановления работают в паре, имеет значение соотношение системных требований к ним. Нередко можно усложнив один алгоритм значительно упростить другой. Таким образом, возможны три варианта:

Алгоритм сжатия требует больших вычислительных ресурсов, нежели алгоритм восстановления.

Это наиболее распространенное соотношение, характерное для случаев, когда однократно сжатые данные будут использоваться многократно. В качестве примера можно привести цифровые аудио- и видеопроигрыватели.

Алгоритмы сжатия и восстановления требуют приблизительно равных вычислительных ресурсов.

Наиболее приемлемый вариант для линий связи, когда сжатие и восстановление происходит однократно на двух ее концах (например, в цифровой телефонии).

Алгоритм сжатия существенно менее требователен, чем алгоритм восстановления.

Такая ситуация характерна для случаев, когда процедура сжатия реализуется простым, часто портативным устройством, для которого объем доступных ресурсов весьма критичен, например, космический аппарат или большая распределенная сеть датчиков. Это могут быть также данные, распаковка которых требуется в очень малом проценте случаев, например запись камер видеонаблюдения.

Имеется два основных подхода к сжатию данных неизвестного формата:

– на каждом шаге алгоритма сжатия очередной сжимаемый символ либо помещается в выходной буфер сжимающего кодера как есть (со специальным флагом, помечающим, что он не был сжат), либо группа из нескольких сжимаемых символов заменяется ссылкой на совпадающую с ней группу из уже закодированных символов. Поскольку восстановление сжатых таким образом данных выполняется очень быстро, такой подход часто используется для создания самораспаковывающихся программ;

– для каждой сжимаемой последовательности символов однократно либо в каждый момент времени собирается статистика ее встречаемости в кодируемых данных. На основе этой статистики вычисляется вероятность значения очередного кодируемого символа (либо последовательности символов). После этого применяется та или иная разновидность энтропийного кодирования, например, арифметическое кодирование или кодирование Хаффмана, для представления часто встречающихся последовательностей – короткими кодовыми словами, а редко встречающихся – более длинными.

Тема 20. Энтропия дискретного источника

Рассмотрим источник информации, который может в каждый момент времени случайным образом принять одно из конечного множества возможных состояний. Такой источник называют дискретным источником информации. При этом принято говорить, что различные состояния реализуются вследствие выбора их источником. Каждому состоянию источника u ставится в соответствие условное обозначение в виде знака (в частности, буквы) из алфавита данного источника: $u_1, u_2, \ldots, u_N$.

Для получения результата выбора источником u конкретного состояния можно высказать ряд предположений, базирующихся на априорных сведениях об источнике информации. Поскольку одни состояния выбираются источником чаще, а дру-

гие реже, то в общем случае он характеризуется ансамблем U, т. е. полной совокупностью состояний с вероятностями их появления, составляющими в сумме единицу:

$$U = \begin{pmatrix} u_1 & u_2 & \dots u_i \dots & u_N \\ p(u_1) & p(u_2) \dots & p(u_i) \dots & p(u_N) \end{pmatrix}, \quad \sum_{i=1}^{N} p(u_i) = 1$$

или

$$U = \begin{pmatrix} u_1 & u_2 & \dots u_i \dots & u_N \\ p_1 & p_2 & \dots p_i \dots & p_N \end{pmatrix}, \quad \sum_{i=1}^{N} p_i = 1.$$

Обе формы записи используются на равных основаниях.

Опираясь на эти сведения, введем сначала меру неопределенности выбора состояния источника. Ее можно рассматривать и как меру количества информации, получаемой при полном устранении неопределенности относительно состояния источника. Мера должна удовлетворять ряду естественных условий. Одним из них является необходимость монотонного возрастания с увеличением возможностей выбора, т. е. числа возможных состояний источника N, причем недопустимые состояния (состояния с вероятностями, равными нулю) не должны учитываться, так как они не меняют неопределенности.

Ограничиваясь только этим условием, за меру неопределенности можно было бы взять число состояний, предположив, что они равновероятны. Однако такая мера противоречит некоторым интуитивным представлениям. Например, при N=1, когда неопределенность отсутствует, она давала бы значение, равное единице. Кроме того, такая мера не отвечает требованию аддитивности, состоящему в следующем.

Если два независимых источника с числом равновероятных состояний NM рассматривать как один источник, одновременно реализующий пары состояний $n_i m_j$, то естественно предположить, что неопределенность объединенного источника должна равняться сумме неопределенностей исходных источников. Поскольку общее число состояний объединенного ис-

точника равно NM, то искомая функция должна удовлетворять условию

$$f(NM) = f(N) + f(M).$$

Это соотношение выполняется, если в качестве меры неопределенности источника с равновероятными состояниями и характеризующего его ансамбля U принять логарифм состояний:

$$H(U) = \log N.$$

Тогда при $N = 1$ $H(U) = 0$ и требование аддитивности выполняется.

Указанная мера была предложена американским ученым Р. Хартли в 1928 г. Основание логарифма не имеет принципиального значения и определяет только масштаб или единицу неопределенности. Так как современная информационная техника базируется на элементах, имеющих два устойчивых состояния, то обычно выбирают основание логарифма равным двум. При этом единица неопределенности называется двоичной единицей или битом и представляет собой неопределенность выбора из двух равновероятных событий (*bit* – сокращение от англ. *Binary digit* – двоичная единица). Если основание логарифма выбрать равным десяти, то неопределенность получим в десятичных единицах на одно состояние (дитах).

Пример 1. Определить минимальное число взвешиваний, которое необходимо произвести на равноплечих весах, чтобы среди 27 внешне неотличимых монет найти одну фальшивую, более легкую.

Общая неопределенность ансамбля U составляет

$$H(U) = \log_2 27 \text{ дв. ед.}$$

Одно взвешивание способно прояснить неопределенность ансамбля U', насчитывающего три возможных исхода (левая чаша весов легче, правая чаша весов легче, весы находятся в равновесии). Эта неопределенность равна

$$H(U') = \log_2 3 \text{ дв. ед.}$$

Так как

$$H(U) = 3\log_2 3 = 3\,H(U'),$$

то для определения фальшивой монеты достаточно произвести три взвешивания.

Алгоритм определения фальшивой монеты следующий. При первом взвешивании на каждую чашу весов кладется по девять монет. Фальшивая монета будет либо среди тех девяти монет, которые оказались легче, либо среди тех, которые не взвешивались, если имело место равновесие. Аналогично, после второго взвешивания число монет, среди которых находится фальшивая, сократится до трех. Последнее, третье взвешивание дает возможность точно указать фальшивую.

Предложенная мера, как мы убедились, позволяет решать определенные практические задачи. Однако она не получила широкого применения, поскольку была рассчитана на слишком грубую модель источника информации, приписывающую всем его возможным состояниям одинаковую вероятность.

Таким образом, степень неопределенности реализации состояния источника информации зависит не только от числа состояний, но и от вероятностей этих состояний. При неравновероятных состояниях свобода выбора источника ограничивается, что должно приводить к уменьшению неопределенности. Если источник информации имеет, например, два возможных состояния с вероятностями 0,99 и 0,01, то неопределенность выбора у него значительно меньше, чем у источника, имеющего два равновероятных состояния. Действительно, в первом случае результат практически предрешен (реализация состояния, вероятность которого равна 0,99), а во втором случае неопределенность максимальна, поскольку никакого обоснованного предположения о результате выбора сделать нельзя. Ясно также, что весьма малое изменение вероятностей состояний вызывает соответственно незначительное изменение неопределенности выбора.

Это позволяет сформулировать следующее требование к искомой мере неопределенности $H(p_1 \ \ldots \ p_i \ \ldots \ p_N)$: она должна

быть непрерывной функцией вероятностей состояний источника $p_1 \ldots p_i \ldots p_N$ с соблюдением условия $\sum_{i=1}^{N} p_i = 1$. Наибольшее ее значение должно достигаться при равенстве вероятностей всех состояний.

Кроме того, так как мера неопределенности связывается нами только с фактом выбора, а не с множеством конкретных значений наблюдаемых явлений, то $H(p_1 \ldots p_N)$ должна быть функцией от функции распределения случайной величины и не должна зависеть от ее конкретных значений. Иначе говоря, $H(p_1 \ldots p_N)$ должна являться функционалом распределения вероятностей.

Еще одно условие состоит в том, что мера неопределенности не должна зависеть от пути выбора состояния в ансамбле. Выбор может быть как непосредственным, так и многоступенчатым. В последнем случае неопределенность выбора состояния складывается из неопределенности выбора группы состояний и неопределенностей выбора состояния в каждой группе, рассчитанных с учетом вероятности выбора данной группы.

Мера неопределенности выбора дискретным источником состояния из ансамбля U, удовлетворяющая указанным условиям, была предложена американским ученым К. Шенноном. Ее называют энтропией дискретного источника информации или энтропией конечного ансамбля:

$$H(U) = -C\sum_{i=1}^{N} p_i \log p_i \ ,$$

где C – произвольное положительное число.

К. Шенноном высказано утверждение, а советским ученым Л. Я. Хинчиным математически строго доказано, что это единственный функционал, удовлетворяющий сформулированным условиям.

Если снова ориентироваться на измерение неопределенности в двоичных единицах, то основание логарифма следует при-

нять равным двум. Примем также C=1. Тогда формула энтропии дискретного источника будет иметь следующий вид

$$N(U) = -\sum_{i=1}^{N} p_i \log_2 p_i .$$

Предложенная мера неопределенности выбора дискретным источником состояния из ансамбля U была названа энтропией не случайно. Дело в том, что формальная структура ее выражения совпадает с энтропией физической системы, определенной ранее Больцманом.

Совпадение имеет глубокий физический смысл, так в обоих случаях величина H характеризует степень разнообразия системы.

Рассмотрим взаимосвязь меры К. Шеннона с мерой Хартли. Если в источнике может быть реализовано N равновероятных состояний, то вероятность каждого из них равна p_i=(1/N) (1≤ i ≤ N) и неопределенность, по Хартли, приходящаяся на каждое состояние, выражается числом

$$H_i = \log N = -\log(1/N) = -\log p_i .$$

Будем теперь считать вероятности событий различными, а неопределенность, приходящуюся на одно конкретное состояние источника, характеризовать по аналогии величиной

$$H_i = -\log p_i .$$

Эта частная неопределенность представляет собой случайную величину, зависящую от того, какое состояние источника в действительности реализуется. Усреднив по всему ансамблю U состояний источника, найдем неопределенность, приходящуюся в среднем на одно состояние:

$$H(U) = -\sum_{i=1}^{N} p_i \log p_i .$$

Следовательно, мера К. Шеннона является естественным обобщением меры Хартли на случай ансамбля с неравновероят-

ными состояниями. Она позволяет учесть статистические свойства источника информации.

Пример 2. Сравнить неопределенность, приходящуюся на букву источника информации *и* (алфавита русского языка), характеризуемого ансамблем, представленным в таблице, с неопределенностью, которая была бы у того же источника при равновероятном использовании букв.

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
а	0,064	й	0,010	т	0,056	ъ, ь	0,015
б	0,015	к	0,029	у	0,021	ы	0,016
в	0,039	л	0,036	ф	0,02	э	0,003
г	0,014	м	0,026	х	0,09	ю	0,007
д	0,026	н	0,056	ц	0,04	я	0,019
е, е	0,074	о	0,096	ч	0,013	–	0,143
ж	0,008	п	0,024	ш	0,006		
з	0,015	р	0,041	щ	0,003		
и	0,064	с	0,047				

При одинаковых вероятностях появления всех 32 букв алфавита неопределенность, приходящаяся на одну букву, составляет

$$H(U) = \log_2 32 = 5 \text{ дв. ед.}$$

Энтропию источника, характеризуемого заданным ансамблем (см. таблицу), находим, используя формулу (5):

$H(U) = -\ 0{,}064\ \log_2\ 0{,}064 - 0{,}015\log_2\ 0{,}015 - \ldots - 0{,}143\ \log_2\ 0{,}143 \approx 4{,}42$ дв. ед.

Таким образом, неравномерность распределения вероятностей использования букв снижает энтропию источника с 5 до 4,42 дв. ед.

Рассмотрим основные *свойства энтропии*.

1. Энтропия является вещественной и неотрицательной величиной, так как для любого $i(1 \le i \le N)$ p_i изменяется в интервале от 0 до 1, $\log p_i$ отрицателен и, следовательно, $-p_i \log p_i$ положительна.

2. Энтропия – величина ограниченная. Для слагаемых $-p_i \log p_i$ в диапазоне $0<p_i \le 1$ ограниченность очевидна. Остается определить предел, к которому стремится слагаемое $-p_i \log p_i$ при $p_i \to 0$, поскольку $-\log p_i$ при этом неограниченно возрастает:

$$\lim_{p_i \to 0}(-p_i \log p_i) = \lim_{p_i \to 0} \frac{\log(1/p_i)}{1/p_i}.$$

Сделаем замену $\alpha = 1/p_i$ и, воспользовавшись правилом Лопиталя, получим

$$\lim_{p_i \to 0}(-p_i \log p_i) = \lim_{\alpha \to \infty} \frac{\log \alpha}{\alpha} = \lim_{\alpha \to \infty} \frac{(1/\alpha)\log e}{1} = 0.$$

3. Энтропия обращается в нуль лишь в том случае, если вероятность одного из состояний равна единице. Тогда вероятности всех остальных состояний, естественно, равны нулю. В этом случае состояние источника полностью определено.

4. Энтропия максимальна, когда все состояния источника равновероятны:

$$H_{\max}(U) = -\sum_{i=1}^{N} \frac{1}{N} \log_2 \frac{1}{N} = \log_2 N.$$

5. Энтропия источника u с двумя состояниями u_1 и u_2 изменяется от нуля до единицы, достигая максимума при равенстве их вероятностей:

$$p(u_1)=p=p(u_2)=1-p=0{,}5.$$

6. Энтропия объединения нескольких статистически независимых источников информации равна сумме энтропий исходных источников. Рассмотрим объединение, включающее два

источника информации *u* и *v*. Под объединением двух источников *u* и *v* понимают обобщенный источник информации (*u, v*), характеризующийся вероятностями $p(u_i v_j)$ всех возможных комбинаций состояний u_i источника *u* и v_j источника *v*. Аналогично трактуется и объединение ансамблей.

В соответствии с определением энтропия объединения

$$H(UV) = -\sum_{i=1}^{N}\sum_{j=1}^{k} p(u_i v_j)\log p(u_i v_j),$$

здесь $p(u_i v_j)$ – вероятности совместной реализации состояний

$$u_i(1 \le i \le \mathrm{N}) \text{ и } v_j(1 \le j \le k).$$

В случае статистической независимости источников информации *u* и *v* имеем

$$p(u_i v_j) = p(u_i)\, p(v_j),$$

отсюда

$$H(UV) = -\sum_{i=1}^{N}\sum_{j=1}^{k} p(u_i)p(v_j)\log p(u_i)p(v_j) =$$

$$= -\sum_{i=1}^{N} p(u_i)\log p(u_i)\sum_{j=1}^{k} p(v_i) - \sum_{j=1}^{k} p(v_j)\log p(v_j)\sum_{i=1}^{N} p(u_i).$$

Учитывая, что

$$\sum_{i=1}^{N} p(u_i) = 1 \text{ и } \sum_{j=1}^{k} p(v_j) = 1,$$

получим

$$H(UV)=H(U)+H(V)=H(VU).$$

Эта же формула может быть распространена на несколько независимых источников информации *u*, *v*, …, *z*

$$H(UV\ldots Z)=H(U)+H(V)+\ldots+H(Z).$$

Пример 3. Заданы ансамбли U и V двух дискретных случайных величин U' и V':

$$U = \begin{vmatrix} 0{,}2 & 0{,}7 & 0{,}4 & 0{,}6 \\ 0{,}25 & 0{,}25 & 0{,}25 & 0{,}25 \end{vmatrix}, \; V = \begin{vmatrix} 31 & 10 & 15 & 28 \\ 0{,}25 & 0{,}25 & 0{,}25 & 0{,}25 \end{vmatrix}.$$

Сравнить их энтропии.

Так как энтропия не зависит от конкретных значений случайной величины, а вероятности их появления у обеих величин одинаковы, то

$$H(U) = H(V) = \log 4 = 2 \text{ дв. ед.}$$

Между состояниями двух или нескольких источников, объединенных в рамках одной системы, а также между состояниями, последовательно выбираемыми одним источником, часто бывают *статистические связи*. Эти связи надо учитывать при оценке неопределенности выбора.

Пусть даны два статистически связанных ансамбля U и V. *Объединение ансамблей* характеризуется матрицей $p(UV)$ вероятностей $p(u_i v_j)$ всех возможных комбинаций состояний u_i ($1 \le i \le N$) ансамбля U и состояний v_j ($1 \le j \le k$) ансамбля V:

$$p(U,V) = \begin{Vmatrix} p(u_1 v_1) \ldots p(u_i v_1) \ldots p(u_N v_1) \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ p(u_1 v_j) \ldots p(u_i v_j) \ldots p(u_N v_j) \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ p(u_1 v_k) \ldots p(u_i v_k) \ldots p(u_N v_k) \end{Vmatrix}.$$

Суммируя столбцы матрицы $p(UV)$, получим информацию об ансамбле U исходного источника u:

$$U = \begin{vmatrix} u_1 \quad \ldots \quad u_i \quad \ldots \quad u_N \\ p(u_1) \ldots p(u_i) \ldots p(u_N) \end{vmatrix}.$$

Аналогично, просуммировав строки матрицы $p(UV)$, получим информацию об ансамбле V исходного источника v:

$$V = \begin{vmatrix} v_1 & \dots & v_i & \dots & v_k \\ p(v_1) \dots p(v_i) \dots p(v_k) \end{vmatrix}.$$

Вероятности $p(u_i v_j)$ совместной реализации взаимозависимых состояний u_i и v_j можно выразить через *условные вероятности* $p(u_i/v_j)$ или $p(v_j/u_i)$ в соответствии с тем, какие состояния принять за причину, а какие – за следствие:

$$p(u_i v_j) = p(u_i) p(v_j/u_i) = p(v_j)\, p(u_i/v_j),$$

где $p(u_i/v_j)$ – вероятность реализации состояний u_i ансамбля U при условии, что реализовалось состояние v_j ансамбля V; $p(v_j/u_i)$ – вероятность реализации состояний v_j ансамбля V при условии, что реализовалось состояние u_i ансамбля U.

В этом случае энтропия объединения принимает вид

$$H(U,V) = -\sum_{i=1}^{N}\sum_{j=1}^{k} p(u_i)\, p(v_j/u_i) \log p(u_i)\, p(v_j/u_i) =$$

$$= -\sum_{i=1}^{N} p(u_i) \log p(u_i) - \sum_{i=1}^{N} p(u_i) \sum_{j=1}^{k} p(v_j/u_i) \log(v_j/u_i).$$

Сумма

$$-\sum_{j=1}^{k} p(v_j/u_i) \log(v_j/u_i)$$

представляет собой случайную величину, характеризующую неопределенность, приходящуюся на одно состояние ансамбля V при условии, что реализовалось конкретное состояние u_i ансамбля U.

Эту сумму называют *частной условной энтропией ансамбля* V и обозначают $H_{u_i}(V)$:

$$H_{u_i}(V) = -\sum_{j=1}^{k} p(v_j/u_i) \log(v_j/u_i).$$

При усреднении по всем состояниям ансамбля U получаем среднюю неопределенность, приходящуюся на одно состояние ансамбля V при известных состояниях ансамбля U:

$$H_U(V) = \sum_{i=1}^{N} p(u_i) H_{u_i}(V) = -\sum_{i=1}^{N} p(u_i) \sum_{j=1}^{k} p(v_j / u_i) \log p(v_j / u_i).$$

Величину $H_U(V)$ называют полной условной или просто *условной энтропией ансамбля V* по отношению к ансамблю U.

Подставляя это выражение в формулу для энтропии объединения, получаем

$$H(UV) = H(U) + H_U(V).$$

Поменяв местами состояния u_i и v_j, получаем

$$H(UV) = H(V) + H_V(U),$$

где

$$H_V(U) = \sum_{j=1}^{k} p(v_j) H_{v_j}(U)$$

$$H_{v_j}(U) = -\sum_{i=1}^{N} p(u_i / v_j) \log p(u_i / v_j)$$

Из полученных формул видно, что энтропия объединения двух статистически связанных ансамблей U и V равна безусловной энтропии одного ансамбля плюс условная энтропия другого относительно первого.

Это утверждение можно распространить на объединение любого числа зависимых ансамблей следующим образом

$$H(UVZ...W)=H(U)+H_U(V)+H_{UV}(Z)+\ldots+H_{UVZ...}(W).$$

Наличие сведений о результатах реализации состояний одного ансамбля никак не может увеличить неопределенность выбора состояния из другого ансамбля. Эта неопределенность может только уменьшиться, если существует взаимосвязь в реализациях состояний из обоих ансамблей. Поэтому справедливы следующие неравенства:

$$H_U(V) \le H(V),\ H_V(U) \le H(U).$$

Из этих неравенств и формулы $H(UV) = H(U) + H_U(V)$ следует, что объединение двух произвольных ансамблей удовлетворяет соотношению

$$H(UV) \le H(U) + H(V).$$

Для объединения нескольких произвольных ансамблей справедливо утверждение

$$H(UVZ...W) \le H(U)+H(V)+H(Z)+...+H(W).$$

В случае отсутствия статистической связи в реализациях состояний u_i из ансамбля U и v_j из ансамбля V сведения о результатах выбора состояний из одного ансамбля не снижает неопределенности выбора состояний из другого ансамбля, что находит отражение в следующих равенствах

$$H_U(V) = H(V),\ H_V(U) = H(U).$$

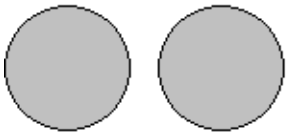
Если имеет место однозначная связь в реализациях состояний u_i ($1 \le i \le N$) из ансамбля U и v_j ($1 \le j \le N$) из ансамбля V, то условная энтропия любого из ансамблей равна нулю:

$$H_U(V) = 0,\ H_V(U) = 0.$$

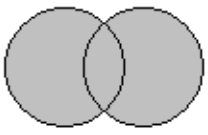
Действительно, условные вероятности $p(u_i/v_j)$ и $p(v_j/u_i)$ в этом случае принимают значения, равные нулю или единице. Поэтому все слагаемые для частных условных энтропий равны нулю. Тогда условные энтропии также равны нулю.

Полученные равенства отражают факт отсутствия дополнительной неопределенности при выборе событий из второго ансамбля.

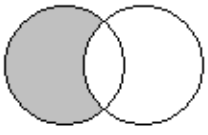
Графически соотношения между энтропиями дискретных источников информации можно представить следующим образом:



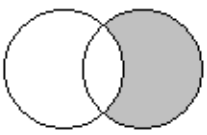
$H(U)\ H(V)$



$H(U,V)$



$H_U(V)$



$H_V(U)$

Пример 4. Дана матрица вероятностей состояний системы, объединяющей источники *u* и *v*:

$$p(v,u) = \begin{Vmatrix} 0{,}4 & 0{,}1 & 0 \\ 0 & 0{,}2 & 0{,}1 \\ 0 & 0 & 0{,}2 \end{Vmatrix}$$

Требуется определить энтропии $H(U)$, $H(V)$, $H_V(U)$ и $H(U,V)$.

Решение. Вычислим безусловные вероятности состояний систем U и V. Для этого просуммируем совместные вероятности по строкам и столбцам заданной матрицы:

$$\begin{array}{cc} & p(u_i) \\ p(v,u) = \left\| \begin{array}{ccc} 0{,}4 & 0{,}1 & 0 \\ 0 & 0{,}2 & 0{,}1 \\ 0 & 0 & 0{,}2 \end{array} \right\| & \begin{array}{c} 0{,}5 \\ 0{,}3 \\ 0{,}2 \end{array} \\ p(v_j) \quad 0{,}4 \quad 0{,}3 \quad 0{,}3 & \end{array}$$

Определим энтропии источников *u* и *v*:

$$H(U) = -\sum_i p(u_i)\log p(u_i) = -(0{,}5\log_2 0{,}5 + 0{,}3\log_2 0{,}3 + 0{,}2\log_2 0{,}2) = 1{,}485 \text{ дв.ед.}$$

$$H(V) = -\sum_j p(v_j)\log p(v_j) = -(0{,}4\log_2 0{,}4 + 0{,}3\log_2 0{,}3 + 0{,}3\log_2 0{,}3) = 1{,}57 \text{ дв.ед.}$$

Определим условные вероятности по формуле

$$p(u_i / v_j) = \frac{p(u_i v_j)}{p(v_j)} :$$

$p(u_1/v_1) = 0{,}4 / 0{,}4 = 1;$

$p(u_1/v_2) = p(u_2/v_3) = 0{,}1 / 0{,}3 = 0{,}33;$

$p(u_2/v_2) = p(u_3/v_3) = 0{,}2 / 0{,}3 = 0{,}67;$

$p(u_1/v_3) = p(u_2/v_1) = p(u_3/v_1) = p(u_3/v_2) = 0.$

Вычислим условную энтропию ансамбля U по отношению к ансамблю V:

$$H_V(U) = -\sum_i \sum_j p(v_j)p(u_i/v_j)\log p(u_i/v_j) = -[0{,}4(1\cdot\log_2 1) + 0{,}3(0{,}33\log_2 0{,}33 +$$

$$+ 0{,}67\log_2 0{,}67) + 0{,}3(0{,}33\log_2 0{,}33 + 0{,}67\log_2 0{,}67)] \approx 0{,}55 \text{ дв.ед.}$$

Вычислим энтропию объединения:

$$H(U,V) = -\sum_i \sum_j p(u_i v_j) \log p(u_i v_j) = -(0{,}4 \log_2 0{,}4 + 0{,}1 \log_2 0{,}1 + 0{,}2 \log_2 0{,}2 +$$

$$+ 0{,}1 \log_2 0{,}1 + 0{,}2 \log_2 0{,}2) = 0{,}529 + 0{,}332 + 0{,}464 + 0{,}332 + 0464 = 2{,}12 \text{ дв.ед.}$$

Проверим полученные результаты:

$H(U,V) = H(V) + H_V(U) = 1{,}57 + 0{,}55 = 2{,}12$ дв. ед.

Тема 21. Введение в криптологию

Криптология – наука о создании и анализе систем безопасной связи. Долгое время, говоря о криптологии, имели в виду не безопасную, а секретную связь, не смотря на то, что секретность является только одним аспектом безопасности. В настоящее время криптология занимается аспектами целостности, подлинности (аутентичности), неотказуемости, анонимности, а также вопросами, возникающими при работе с документальными записями.

Криптологию принято делить в соответствии с аспектами синтеза и анализа на две части: криптографию и криптоанализ. Криптография – наука о методах обеспечения безопасности, то есть она занимается вопросами синтеза систем. Криптоанализ – наука о методах атак на безопасность данных. Существует и другая терминология, по которой термин «криптография» используется для названия всей науки, а криптоанализ называется дешифрованием.

Цели криптографии менялись на протяжении всей ее истории. Сначала она служила больше для обеспечения секретности, чтобы препятствовать несанкционированному раскрытию информации, передаваемой по открытой связи. С началом информационного века обнаружилась потребность применения криптографии и в частном секторе. Количество конфиденциальной информации огромно – истории болезней, юридические, финансовые документы и т. д. Последние достижения криптографии позволили использовать ее не только для защи-

ты информации от несанкционированного раскрытия, но и для обеспечения подлинности и целостности информации.

Условно историю криптологии можно разделить на два периода – период «ручной криптологии», когда основные операции по шифрованию и дешифрованию осуществлялись человеком вручную или с использованием простейших средств механизации, и современный этап, для которого характерно широкое применение ЭВМ как при разработке новых систем шифрования и проверке их на устойчивость, так и в криптоаналитических целях. Этой периодизации придерживается большинство исследователей, четко разграничивающих «ручную криптографию» и современный период, хронологические рамки которого охватывают всю вторую половину XX в. и наши дни.

Однако такая классификация весьма неполна и условна, что обуславливает более сложную систему периодизации развития криптологии. И если о периодизации современного этапа говорить достаточно сложно, то в отношении «ручной» криптологии ситуация вполне определена. Каждый исследователь придерживается своей классификации, однако в целом можно выделить 4 основных периода развития данной науки:

– древнейший (с момента появления письменности до IV в.);

– средневековый (IV–XIII вв.);

– позднего средневековья и раннего нового времени (XIV–XVII вв.);

– нового времени (XVIII – начало XX в.).

Заслуживает внимание периодизация криптологии в книгах белорусских математиков: Ю. С. Харина, В. И. Берника, Г. В. Матвеева, С. В. Агиевича и других. В этой периодизации выделяют три этапа. Первый этап (с самых древних времен до 1949 г.) характеризовался весьма частными, узкоспециальными и вычислительно простыми алгоритмами криптографии и криптоанализа без использования компьютеров. Этот этап часто называют этапом докомпьютерной криптографии. Второй этап (1949–1976 гг.) принято отсчитывать с момента публика-

ции работы американского математика-прикладника К. Шеннона «Теория связи в секретных системах». В этот период активно проводились систематические исследования по криптологии с использованием ЭВМ. Криптология становится математической наукой. Однако потребителями результатов криптологии являлись службы связи и информации в дипломатических и военных организациях, поэтому криптология была «закрытой» наукой. Третий этап (1976 г. – настоящее время), который можно назвать этапом открытой криптологии, принято отсчитывать с момента публикации работы американских математиков У. Диффи, М. Хеллмана «Новые направления в криптографии». В этой работе показано, что «секретная» передача информации возможна (в отличие от результатов К. Шеннона) без предварительной передачи «секретного ключа». Главной особенностью этого этапа становится массовое применение криптографии в банковском деле, компьютерных сетях и других приложениях.

Большинство современных исследователей связывают появление криптографии с появлением письменности, указывая, что эти процессы произошли почти одновременно. Один из самых древних зашифрованных текстов (XX в. до н. э.) был найден при раскопках в Месопотамии. Он был написан клинописью на глиняной табличке и содержал рецепт глазури для покрытия гончарных изделий, что, по-видимому, в то время было коммерческой тайной.

Рассмотрим примеры из истории развития криптологии. В середине IX в. до н. э., как сообщает Плутарх, использовалось устройство для шифрования – скитала, представляющее собой цилиндрический предмет определенной длины и диаметра. При шифровании на цилиндр наматывалась узкая пергаментная лента, на ней вдоль цилиндра писались слова. После написания слов лента разматывалась, буквы слов открытого текста на ней оказывались переставленными. Скитала реализует метод шифрования, названный перестановкой. Ключом для расшифровки полученного текста являлся диаметр скиталы.

Для дешифрования такого шифра текста Аристотель предложил метод, который состоит в следующем. Лента с зашифрованным сообщением наматывалась на конус, а затем определялось место, где появлялось читаемое слово или его часть. Это место указывает на искомый диаметр цилиндра.

В 56 г. н. э. во время войны с галлами Ю. Цезарь использует другую разновидность шифра – шифр замены. Под алфавитом открытого текста писался тот же алфавит со сдвигом (у Цезаря на три позиции) по циклу. При шифровании буквы открытого текста из верхнего алфавита заменялись буквами нижнего алфавита. Хотя этот шифр был известен до Ю. Цезаря, тем не менее, шифр был назван его именем.

Другим более сложным шифром замены является греческий шифр – квадрат Полибия. Алфавит записывается в виде квадратной таблицы 5x5. При шифровании буквы открытого текста заменялись на пару чисел – номера столбца и строки этой буквы в таблице. При произвольном расписывании алфавита по таблице и шифровании такой таблицей короткого сообщения, этот шифр является стойким даже по современным понятиям. Идея была реализована в более сложных шифрах, применявшихся во время Первой мировой войны.

Крах Римской империи в V в. сопровождался закатом искусства и наук, в том числе и криптографии. Церковь в те времена преследовала тайнопись, которую она считала чернокнижием и колдовством. Сокрытие мыслей за шифрами не позволяло церкви контролировать информацию.

В XIII в. францисканский монах и философ Р. Бэкон (1214–1294 гг.) описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

В середине XV в. И. Гутенберг изобрел книгопечатание. Это привело к росту грамотности и увеличению числа людей, которые могли вести переписку. Развиваются межгосударственные отношения, тайнопись становится крайне необходимой.

Во второй половине XV в. архитектор и математик Леон Баттиста Альберти в своей книге описал шифр замены. Этот

шифр использовал два концентрических круга, по периферии которых были нанесены на одном круге – алфавит открытого текста, а на другом алфавит шифрованного текста. Важно, что алфавит для шифрования был не последовательным и мог быть смещен на любое количество шагов. Именно Альберти впервые применил для дешифрования свойство неравномерности встречаемости различных букв в языке. Также он впервые предложил для повышения стойкости применять повторное шифрование с помощью разных систем шифрования. К перешифрованию надо относиться критически, так как в некоторых случаях оно не приводит к повышению стойкости.

Интересен факт, что король Франции Франциск I в 1546 г. издал указ, запрещающий подданным использование шифров. Хотя шифры того времени были исключительно простыми, они считались нераскрываемыми. В настоящее время в разных странах существуют ограничения на использование шифров.

Один из первых учебников по криптографии написал живший в Германии монах-бенедиктинец Иоганн Тритемий (1462–1516 гг.). Он предложил оригинальный шифр многозначной замены под названием «Ave Maria». Каждая буква открытого текста имела не одну замену, а несколько, по выбору шифровальщика. Причем буквы заменялись буквами или словами так, что получался некоторый псевдооткрытый текст, тем самым скрывался сам факт передачи секретного сообщения, то есть применялась стенография вместе с криптографической защитой. Этот термин Иоганн Тритемий ввел в 1499 г. в своем трактате «Стеганография», зашифрованном под магическую книгу. Разновидность шифра многозначной замены применяется до сих пор.

Джироламо Кардано – итальянский математик, механик, врач, изобрел систему шифрования, так называемую решетку Кардано. В куске картона с размеченной решеткой определенным образцом прорезались отверстия, нумерованные в произвольном порядке. Чтобы получить зашифрованный текст, нужно положить этот кусок картона на бумагу и начинать вписы-

вать в отверстия буквы в выбранном порядке. После снятия картона промежутки бессмысленного набора букв дописывались до псевдосмысловых фраз, так что можно было скрыть факт передачи секретного сообщения. Скрытие легко достигается, если промежутки эти большие, и если слова открытого текста имеют небольшую длину. Неудобство шифра в том, что кусок картона надо хранить в тайне.

В XVI в. получили развитие шифры замены в работах итальянца Джованни Батиста Порты и француза Блеза де Вижинера.

В XVII в. кардинал Ришелье (министр при короле Франции Людовике XIII) создал первую в мире службу шифрования. Эту службу возглавлял Антуан Россиньоль (1590–1673 гг.).

Лорд Френсис Бэкон (1562–1626 гг.) был первым, кто обозначил буквы 5значным двоичным кодом: A = 00001, B = 00010 ... и т. д. Правда, Бэкон никак не обрабатывал этот код, поэтому такое закрытие было совсем нестойким. Тут уместно вспомнить коды Морзе, Бодо, международный телеграфный код № 2, код ASCII, также представляющие собой простую замену.

В этом же веке были изобретены так называемые словарные шифры. При шифровании буквы открытого текста обозначались двумя числами – номером строки и номером буквы в строке на определенной странице какой-нибудь выбранной распространенной книги. Эта система является довольно стойкой, но книга может попасть в руки противника.

В конце XVIII в. в переписке французской метрополии с колониями стали применяться в основном трехзначные коды на несколько сот величин кода. Обычно при шифровании пользуются книгой кодирования, где для удобства все величины кодов стоят в алфавитном порядке. Если при кодировании нужного слова не окажется среди величин кода, то оно кодируется побуквенно. Главный недостаток такого шифрования – ограниченная стойкость, особенно при длительной и интенсивной переписке. Криптоаналитики противника обычно предполагают состав величин кода, а обозначения кодов они могут

узнать из перехвата шифровой переписки. Остается только правильно привязать их друг к другу. Чтобы строить гипотезы о соответствии анализируются действия применяющего коды, сопоставляются даты, названия населенных пунктов, имен и т. п.

К. Гаусс (1777–1858 гг.) – великий математик, тоже не обошел своим вниманием криптологию. Он создал шифр, который ошибочно считал нераскрываемым. При его создании использовался интересный прием – рандомизация (random – случайный) открытого текста. Открытый текст можно преобразовать в другой текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В получающемся тексте все символы большего алфавита встречаются с примерно одинаковой частотой. Шифрование такого текста противостоит методам дешифрования на основе анализа частот отдельных символов. После расшифрования законный получатель легко снимает рандомизацию. Такие шифры называют «шифрами с многократной подстановкой» или «равночастотными шифрами».

Итог многовекового противостояния разработчика шифра – криптографа и его оппонента – криптоаналитика, дешифровальщика подвел голландец Керкхоффс (Kerckhoffs, 1835–1903 гг.), который сформулировал правила этого противостояния. Основное правило Керкхоффса состоит в том, что при разработке и применении шифра надо исходить из того, что весь механизм шифрования, множество правил или алгоритмов, рано или поздно становится известным оппоненту, а стойкость шифра должна определяться только секретностью ключа.

Изобретение телеграфа и других технических видов связи в середине XIX в. дало новый толчок развитию криптологии. Информация передается в виде токовых и бестоковых посылок, т. е. представляется в двоичном виде. Поэтому возникла проблема сжатия информации, которая решалась опять же с помощью кодов, чтобы одно слово или даже целую фразу можно было передать двумя-тремя знаками.

В начале XX в. были созданы механические машины для шифрования, вырабатывающие шифр с помощью набора колес, которые, находясь на одной оси, дискретно перемещались одно относительно другого, создавая на каждом такте уникальное сочетание из всех возможных сочетаний угловых положений. Первые такие машины были сконструированы на основе принципов, заложенных в кассовые аппараты, арифмометры, торговые автоматы и т. п. Все эти машины реализовывали шифр замены. Такой же принцип сохранился в электрических машинах, получивших название дисковых (роторных). Колеса этих машин (диски) изготавливались из электроизолирующего материала и имели вид узкого цилиндра, в оба основания которого были запрессованы латунные контакты, соответствующие буквам алфавита.

Принцип работы дисков был почти одновременно открыт четырьмя изобретателями из разных стран. Это американец Эдвард Хеберн (1918 г.), голландец Хуго Кох (1919 г.), швед Арвид Дамм (1919 г.), немец Артур Шербиус (1927 г.).

Тема 22. Методы шифрования информации

Одним из самых старых шифров является шифр Юлия Цезаря. При шифровании с его помощью каждая буква латинского алфавита сдвигается циклически вправо на $k = 3$ позиций. Таким образом, имеем подстановку (замену):

A	B	C	D	E	F	G	H	…	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	…	W	X	Y	Z	B	B	C

Шифрование осуществляется в соответствии с этой подстановкой. Например, E_3(SUN) = VXQ. Понятно, что выбор $k = 3$ не является единственно возможным. При других ключах k имеем

$$E_{25}(\text{IBM}) = \text{HAL},\ E_6(\text{IDMUP}) = \text{OJSAV}.$$

Нетрудно показать, что $D_k = E_{26-k}$, $D_k E_k = E_0 = D_0$, а ключ k определен по модулю 26.

Шифр Цезаря является примером *шифра подстановки,* или *замены.* Его еще называют *шифром простой подстановки.* Криптоанализ такого шифра очень прост. Дело в том, что для любого современного языка вычислены частотные характеристики букв, т. е. относительные частоты их появления в «нормальных» текстах. Приведем эти частоты в процентах (с упорядочением) для английского языка:

Высокий		Средний		Низкий	
E	12,31	L	4,03	B	1,62
T	9,59	D	3,65	G	1,61
A	8,05	C	3,20	V	0,93
O	7,94	U	3,10	K	0,52
N	7,19	P	2,29	Q	0,20
1	7,18	F	2,28	X	0,20
S	6,59	M	2,25	J	0,10
R	6,03	W	2,03	Z	0,09
H	5,14	У	1,88		

Можно сказать, что при шифровании простой заменой буквы текста заменяются буквами этого или другого алфавита в соответствии с некоторой подстановкой.

Еще одним примером шифра простой замены является *модулярный шифр.* Выберем число *a,* взаимно простое с модулем $m = 26$. Пусть p – буква английского алфавита, отождествленная со своим порядковым номером (0, 1, ..., 25). Тогда $E_a(p) = (ap + k)(\mathrm{mod}\ m)$, где k – фиксировано. В этом случае ключом является пара чисел (a, k). Условие взаимной простоты необходимо для обратимости шифра. Конечно, буквы можно заменять и какими-то другими символами. К семейству шифров замены относятся гомофонические, полиграммные и многоалфавитные шифры.

Гомофоническое шифрование – один из способов защиты от частотной криптоатаки. Каждая буква текста шифруется несколькими символами этого или другого алфавита. Число этих символов пропорционально частотной характеристике шиф-

руемой буквы. Ключом в этом случае является таблица с гомофонией, например:

Буква	Гомофония							
H	17	19	34	41	56			
I	08	22	53	65	88	90	83	
M	03	44						
N	02	09	15	27	32	40	59	
O	01	11	23	42	54	70	80	67
P	33	91						
C	05	10	20					

Одним из возможных вариантов зашифровать текст HOMOPHONIC является следующий: 17 01 44 23 91 41 11 15 88 20.

При *полиграммном шифровании* заменяются не буквы текста, а их комбинации. Если заменяются пары букв, то имеем *биграммное шифрование*. Примером биграммного шифрования является шифр ***Плейфера***. Образуем из английского алфавита какой-нибудь квадрат 5 x 5 и будем хранить его, как всякий ключ, в секрете.

Например:

H	A	R	P	S
I	C	O	D	B
E	F	G	K	L
M	N	Q	T	U
V	W	X	Y	Z

Здесь буква J не употребляется или отождествляется с буквой I.

Замена биграмм проводится по правилам:

1) если m_1 и m_2 находятся в одной строке, то биграмма m_1, m_2 шифруется биграммой c_1, c_2, где буквы c_1 и c_2 являются правыми соседями букв m_1 и m_2 соответственно; если правого соседа нет, то берется первая буква строки;

2) если m_1 и m_2 – в одном столбце, то берутся нижние соседи с аналогичной оговоркой;

3) если $m_1 = m_2$, то в незашифрованном тексте между ними вставляется незначащая буква (например X);

4) при нечетном количестве букв в незашифрованном тексте к нему дописывается незначащая буква;

5) в наиболее вероятном случае, когда m_1 и m_2 расположены в разных столбцах и строках, c_1 и c_2 выбираются, как показано на схеме:

$$\begin{array}{cccccccccccc} m_1 & \dots & c_1 & c_2 & \dots & m_2 & c_1 & \dots & m_1 & m_2 & \dots & c_2 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ c_2 & \dots & m_2 & m_1 & \dots & c_1 & m_2 & \dots & c_2 & c_1 & \dots & m_1 \end{array}$$

Покажем это на примере:

$$\begin{array}{cccccccc} \text{m} & = & \text{RE} & \text{NA} & \text{IS} & \text{SA} & \text{NC} & \text{EX} \\ \text{E(m)} & = & \text{HG} & \text{WC} & \text{BH} & \text{HR} & \text{WF} & \text{GV} \end{array}$$

Еще одна биграммная криптосхема, принадлежащая ***Хиллу***, основана на линейной алгебре. Осуществим цифровую кодировку букв английского алфавита: A = 0, B = 1, C = 2, ..., Z = 25. Выберем какую-нибудь обратимую по модулю 26 квадратную матрицу M порядка 2. Это – ключ. Пусть, например,

$$M = \begin{pmatrix} 2 & 5 \\ 3 & 3 \end{pmatrix}, \quad M^{-1} = \begin{pmatrix} 17 & 15 \\ 9 & 20 \end{pmatrix}.$$

Биграммы будем записывать в виде матриц-столбцов. Например:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \quad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

Шифрование биграмм определим формулой $C = MP$. Зашифруем, для примера, слово $m = P_1P_2$: m = HELP, c = IHTA.

К биграммному шифрованию, так же как и к шифру простой подстановки, применима частотная криптоатака. Приведем в связи с этим наиболее распространенные английские биграммы с указанием процентов их встречаемости:

TH	6,3	AK	2,0	HA	1,7
IN	3,1	EN	2,0	OU	1,4
ER	2,7	TI	2,0	IT	1,4
RE	2,5	TE	1,9	ES	1,4
AN	2,2	AT	1,8	ST	1,4
HE	2,2	ON	1,7	OR	1,4

При *многоалфавитном подстановочном шифровании* задается d шифров простой подстановки, определяемых функциями $f_1, f_2, ..., f_d$, а сообщение

$$m = m_1, m_2, ..., m_d, m_{d+1}, ..., m_{2d}, ...$$

шифруется по правилу

$$E_k(m) = f_1(m_1), f_2(m_2), ..., f_d(m_d), f_1(m_{d+1}), ..., f_d(m_{2d}), ...$$

К таким шифрам относится шифр ***Виженера***. Ключ образуется последовательностью букв $k_1, k_2, ..., k_d$, при этом для буквы a i-го алфавита функция выглядит следующим образом: $f_i(a) = (a+k_i)(\mathrm{mod} m)$.

Пример приведен ниже.

m	=	MULT	IALP	HABE	TENC	RYPT	ION
k	=	KEYS	KEYS	KEYS	KEYS	KEYS	KEY
$E_k(m)$	=	WZJL	SEJH	REZW	DILU	BCNL	SSL

Наряду с подстановочными шифрами известны так называемые *перестановочные (транспозиционные)* шифры. При этом буквы сообщения остаются прежними, но меняют свое расположение в тексте. Приведем два примера.

Сообщение можно разбить на группы букв, скажем, по три буквы, а затем в каждой группе сделать одну и ту же перестановку. Например:

TEACHENCRYPTION → EATHECCRNPTYONI.

То же сообщение можно записать в прямоугольнике 3 x 5:

T	E	A	C	H
E	N	C	R	Y
P	T	I	O	N

Затем можно переписать его по столбцам: TEPENTACICROHYN, что и будет криптограммой (зашифрованным текстом).

В заключение отметим еще один шифр, предложенный ***Вернамом***. Сообщение m обычно записывают в виде последовательности нулей и единиц. Длина ключа k равна длине сообщения. Шифрование состоит в применении к m и k *операции* XOR (исключающее ИЛИ, ранее мы ее называли логическим сложением или сложением по модулю 2), $E_k(m) = m \oplus k$. Очевидно, $D_k = E_k$, так как $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$. Шифр Вернама считается практически нераскрываемым, так как данное сообщение с помощью подбора ключа, к сожалению, слишком большого, можно преобразовать в любое другое. Основная проблема состоит в хранении и передаче ключа.

В современной компьютерной криптографии используются многие перечисленные шифры как составные части сложных криптосистем.

Тема 23. Электронная цифровая подпись

Собственноручная подпись на бумажном документе решает следующие задачи:

– убедить читателя в том, что человек, подписавший документ, сделал это сознательно *(подпись достоверна);*

– доказать, что именно этот человек, и никто другой, сознательно подписал документ *(подпись неподдельна);*

– будучи частью документа, защитить ее от мошеннического переноса в другой документ *(подпись невозможно использовать повторно);*

– защитить и сам документ *(подписанный документ невозможно изменить);*

– обеспечить материальность подписи и документа, гарантирующую, что человек, подписавший документ, не сможет утверждать впоследствии, что документ подписан не им *(от подписи нельзя отказаться).*

Однако, как показывает практика, собственноручная подпись на бумажном документе по самой своей природе оставляет лазейки для мошенников. Недаром для затруднения их действий на бланки документов наносят специальные защитные знаки, применяют нумерацию и скрепление листов, а кроме того, наряду с самой подписью используют собственноручное написание фамилии, имени, отчества на документе и т. п. Одним словом, при всех ее достоинствах собственноручная подпись обладает и целым рядом недостатков.

Как результат проникновения компьютерных технологий во все сферы человеческой деятельности возникла потребность реализовать аналог собственноручной подписи человека в электронном виде. Эта задача была успешно решена. В основе решения лежат разработанные в середине 1970-х гг. криптографические алгоритмы с открытым ключом, которые базируются на сложном математическом аппарате.

При этом **электронная цифровая подпись** (ЭЦП) устранила большинство проблем, свойственных подписи на бумажном документе, и обеспечила электронному документу следующие важнейшие характеристики:

– *подлинность* – подтверждение авторства документа;

– *целостность* – документ не может быть изменен после подписания;

– *неотрицание авторства (неотрекаемость)* – автор впоследствии не сможет отказаться от своей подписи.

При обмене информацией в компьютерных сетях для подтверждения авторства были разработаны алгоритмы электронной цифровой подписи. В основе большинства алгоритмов ЭЦП лежит идея шифрования с открытым ключом.

Рассмотрим **обобщенную модель ЭЦП.** В практической деятельности важно не только защищать информацию от незаконного пользователя, но и иметь возможность проверить авторство данного сообщения и отсутствие в нем изменений, внесенных посторонним лицом. Именно для решения этих проблем (аутентификации и целостности) был разработан ряд алгоритмов ЭЦП. В основе большинства из них лежит идея использования односторонней функции с секретом.

Суть этой идеи состоит в использовании некоторой односторонней функции с секретом Fs для создания пары (x,y), где x – сообщение, а y – решение уравнения $Fs\,(y) = x$.

Всякая информация, записанная в некотором алфавите, может быть представлена в виде двоичных слов, т. е. в виде конечных последовательностей из нулей и единиц. Количество двоичных цифр в таком слове будем называть его длиной. Пусть теперь X и Y – некоторые подмножества множества всех двоичных слов.

Односторонней функцией с секретом S называется функция $Fs : Y \to X$, зависящая от параметра S и обладающая следующими тремя свойствами:

1) при любом S существует полиномиальный алгоритм вычисления значений $Fs(y)$;

2) при неизвестном S не существует полиномиального алгоритма для решения уравнения $Fs(y) = x$ относительно y;

3) при известном S существует полиномиальный алгоритм для решения уравнения $Fs(y) = x$ относительно y.

До настоящего времени не известно ни одного примера односторонней функции с секретом, но для практических целей используют некоторые функции, которые могут оказаться односторонними. Для них второе свойство строго не доказано, но известно, что задача инвертирования эквивалентна некоторой трудно решаемой математической задаче.

Пусть A и B – некоторые пользователи, обменивающиеся информацией по открытому каналу связи. Пусть X – совокупность всевозможных сообщений, Y – некоторое множество

«подписей». Пусть $F_k : Y \to X$ – функция, зависящая от параметра $k \in K$, называемого **ключом**. Будем считать, что ключ k состоит из двух частей: k_S и k_O, где k_S – секретная составляющая, известная только A, и k_O – открытая составляющая, известная «всем» (не держится в секрете). Пусть F_k является сюръекцией, т. е. для любого $x \in X$ существует прообраз $y = F_k^{-1}(x)$. Функцию F также считаем общеизвестной.

Предположим, что выполняются следующие свойства:

1) зная k_O, функцию $F_k(y)$ можно вычислить по алгоритму полиномиальной сложности;

2) зная k_S, функцию $F_k(y)$ можно инвертировать по алгоритму полиномиальной сложности;

3) зная k_O, но не зная k_S, функцию $F_k(y)$ сложно инвертировать, то есть не известен или не существует полиномиальный алгоритм нахождения $F_k^{-1}(x)$.

Прообраз $y = F_k^{-1}(x)$ некоторого сообщения x называется ***подписью этого сообщения***. Пара (x, y) называется ***подписанным сообщением.***

В силу первого свойства всегда легко проверить, соответствует ли подпись сообщению, а в силу третьего свойства подделать подпись при достаточно большом ключе практически невозможно. Доказательство этого свойства позволило бы придать подписанным сообщениям юридическую силу.

Секретный и открытый ключи находятся во взаимно однозначном соответствии и в силу третьего требования не существует полиномиального алгоритма вычисления секретной компоненты по открытой компоненте. Таким образом, в общем виде алгоритм ЭЦП выглядит так.

1. Для передаваемого сообщения x отправитель A находит $y = F_k^{-1}(x)$. Знание секретного ключа k_S позволяет ему сделать это за приемлемое время.

2. Далее A передает B по какому-либо каналу связи пару (x, y), где x – сообщение, y – подпись.

3. Получив подписанное сообщение (x, y), B находит $x' = F_k(y)$. Знание открытого ключа k_O позволяет сделать это за приемлемое время.

4. Получатель B сверяет x и x'. Если они совпадают, то полученное сообщение считаем подлинным. В противном случае либо сообщение x изменено (фальшивое), либо подпись y неверная (поддельная).

Указанную модель можно дополнить предварительным шифрованием пересылаемого сообщения и итоговой расшифровкой. Роль функции F_k иногда выполняет некоторая схема шифрования с открытым ключом. В силу этого многие вопросы (стойкость, выбор ключей и др.) равносильны для схем ЭЦП и соответствующих криптосистем.

Тема 26. Алгоритмы хеширования

Многие из алгоритмов электронной цифровой подписи пригодны лишь для подписания сообщений фиксированной или находящейся в заданных пределах длины. На практике сообщение может быть длиннее. Очевидное решение этой проблемы – разбить сообщение на части и подписать каждую в отдельности – неприемлемо из-за увеличения объема сообщения. Еще одно неудобство такого подхода в том, что многие схемы электронной цифровой подписи работают довольно медленно, а многократная подпись лишь усиливает этот недостаток.

В настоящее время для решения этой проблемы используют так называемые хеш-функции. Функция хеширования сопоставляет произвольному набору данных его образ фиксированной небольшой длины, пригодный для алгоритма ЭЦП. Поэтому подписанное сообщение x имеет вид $(x, s(h(x)))$, где h – функция хеширования.

Очевидно, что функция h должна быть односторонней, т. е. не должно существовать алгоритма полиномиальной сложности для вычисления x по известному $y = h(x)$.

Если взломщик найдет сообщение x' такое, что $h(x)=h(x')$, то он сможет выдать его за истинное, поскольку подпись останется прежней. Поэтому при синтезе хеш-функций обычно требуют, чтобы она, как минимум, удовлетворяла следующему определению.

Функция h называется свободной от коллизий, если вычислительно невозможно найти для данного x точное x', что $h(x)=h(x')$.

Функция h называется свободной от коллизий в строгом смысле, если вычислительно невозможно найти два таких сообщения x и x', что $h(x)=h(x')$.

На практике, конечно, любая хеш-функция имеет много коллизий. Тем не менее, для односторонней функции их поиск является трудной задачей.

Большинство известных к настоящему времени хеш-функций можно условно разделить на два класса. К одному из них относятся функции, в основе которых лежат стандарты блочного шифрования, а к другому – функции, основанные на различных преобразованиях из теории чисел, алгебры и других разделов математики.

Функции первого класса удобны тем, что они используют алгоритм, которым одновременно можно шифровать сообщение. Для хеширования само сообщение должно быть разбито на блоки, пригодные для применения стандарта шифрования. При этом в качестве первого блока используется случайный или зависящий от ключа блок, называемый вектором инициализации. Одна из первых функций такого вида была предложена Рабином.

Схема Рабина

Обозначим через $E(к,m)$ образ сообщения m под действием преобразования E с ключом $к$. Если необходимо хешировать сообщение m, то его разбивают на блоки m_1, m_2,…, m_t. Например, если рассматривается стандарт DES, то длина блока равна 64. Выбираем вектор инициализации. Хеш-значение $h(x)$ определяется по формулам:

$h_0 = I$, $h_i=E(m_i,h_{i-1})$, $i = 1,2, ..., t$, $h(m) = h_t$. Впоследствии было предложено усложнение этой схемы:

$h_0 = I$, $h_i = E(m_i \oplus h_{i-1}, h_{i-1})$, $i=1,2, ..., t$, $h(m) = h_t$. Известны варианты, когда используется ключ. Например,

$h_0 = I$, $h_i = E(k, m_i \oplus h_{i-1})$, $i=1,2, ..., t$, $h(m) = h_t$.

К числу схем второго класса относится схема, использующая RSA-преобразование. Выбираем параметры N и e RSA-криптосистемы:

$h_0 = I$, $h_i = (h_{i-1} \oplus m_i)^e \bmod N$, $h(m) = h_t$.

Иногда используют схемы, основанные на возведении в квадрат по модулю:

$$h_i = (h_{i-1} \oplus m_i)^2 \bmod N,$$
$$h_i = h_{i-1} \oplus (m_i^2 \bmod N),$$
$$h_i = h_{i-1} \oplus (m_i \bmod N)^2 \bmod N.$$

Алгоритмы хеширования в базах данных

Алгоритмы хеширования в базах данных используются для преобразования ключа в адрес. Процедура преобразования ключа в адрес выполняется в три этапа:

1. Если ключ не цифровой, он преобразуется в соответствующее цифровое представление таким образом, чтобы исключить потерю информации, содержащуюся в ключе. Например, буквенные знаки должны переводиться в цифровой код; допускается также представление символьного ключа в виде строки битов.

2. Ключи (в цифровом или битовом представлении) затем преобразуются в совокупность произвольно распределенных чисел, значения которых имеют тот же порядок, что и значения адресов основной области памяти. Набор ключей должен быть распределен по возможности равномерно в диапазоне допустимых адресов.

3. Полученные числа умножаются на константу, что позволяет разместить их строго в диапазоне значений адресов основной области. Например, пусть в результате выполнения этапа 2 мы получаем четырехзначные числа, а в основной области имеется 7000 пакетов. Тогда четырехзначные числа следует умножать на 0,7, что позволит распределить получаемые адреса в интервале от 0 до 6999. Этот относительный номер пакета преобразуется в машинный адрес пакета.

Метод средних квадратов. Ключ возводится в квадрат. После этого из полученного результата выделяется число, со-

стоящее из центральных цифр. Например, если ключ записи равен 172 148, то его квадрат 029 634 933 904. Четыре центральные цифры составляют число 3493.

Деление. В основе данного метода лежит обычное деление чисел. Он дает лучшие результаты, чем метод средних квадратов. Ключ делится на число, равное числу пакетов в основной области или близкое к нему. Делитель должен быть простым числом или числом, которое не содержит небольших сомножителей. Остаток от деления и дает относительный адрес пакета.

Например, если число пакетов равно 10 000, то в качестве делителя можно использовать число 9991 (у этого числа один большой делитель 97). Пусть ключ записи равен 172 148. Остаток от деления 172 148 на 9991, равный 2301, будет взят в качестве относительного адреса пакета, в который направляется запись с ключом 172 148.

Сдвиг разрядов. Все разряды числа, являющегося ключом, разбиваются на две части: старшие и младшие разряды. Обе эти части сдвигаются по направлению друг к другу так, чтобы число перекрывающихся разрядов соответствовало длине адреса (рис. 2.4.). Цифры, содержащиеся в перекрывающихся разрядах, суммируются.

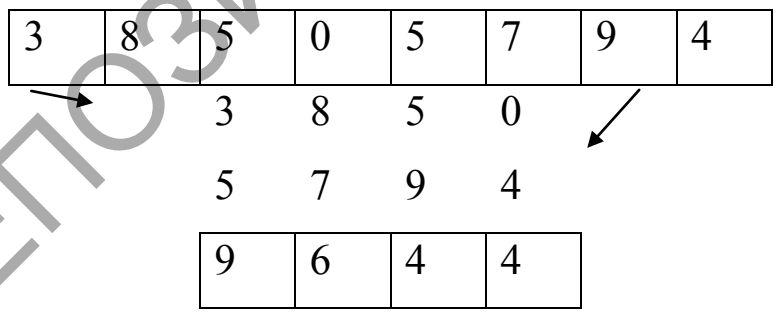


Рис. 2.4. Метод сдвига разрядов

Складывание. Ключ разбивается на части, средняя из которых равна длине адреса (рис. 2.5.). Первая и третья налагаются на вторую подобно тому, как складывается втрое лист бумаги. Цифры затем суммируются. Это метод наиболее удобен для преобразования больших ключей.

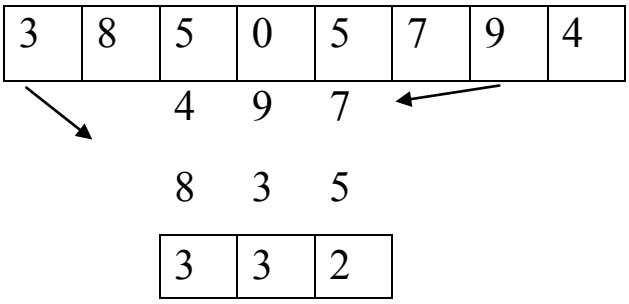


Рис. 2.5. Метод складывания

Анализ отдельных разрядов ключа

Для достижения равномерного распределения адресов пакетов можно использовать анализ распределения значений чисел и символов в каждом ключе. Выбросив из ключа разряды, имеющие распределение, сильно отличающееся от равномерного, мы можем достичь более равномерного распределения адресов.

Преобразование системы счисления

В основе этого алгоритма лежит преобразование основания системы счисления ключа (например, можно использовать основание 11). После преобразования выделяются младшие разряды.

Пример. Пусть ключ равен 172 148. Тогда

$$1 \cdot 11^5 + 7 \cdot 11^4 + 2 \cdot 11^3 + 1 \cdot 11^2 + 4 \cdot 11^1 + 8 = 266\,373.$$

Число 6373, образованное младшими разрядами, будет являться адресом.

При использовании данного метода необходимые расчеты выполняются на компьютере быстрее, чем при использовании методов складывания и сдвига разрядов.

Метод Лина

В данном методе осуществляется представление ключа в системе счисления с основанием p, после чего осуществляется деление результата на q^m. Остаток будет искомым адресом. Здесь p и q – простые числа (или числа, не содержащие небольших множителей), а m – целое положительное число.

Пример. Ключ 172 148 поразрядно преобразуется в двоичную строку: 0001 0111 0010 0001 0100 1000. После этого осуществляется перегруппировка строки по три разряда: 000 101 110 010 000 101 001 000 = 05 620 510.

Затем осуществляется деление числа 05 620 510 на величину $q^m = 97^2$ по правилам деления десятичных чисел. Остаток от деления 3337 есть номер пакета.

Деление полиномов

Цифра каждого разряда ключа рассматривается как коэффициент полинома. Например, ключ 172 148 может быть представлен полиномом $x^5+7x^4+2x^3+x^2+4x+8$. Затем этот полином делится на некоторый выбранный и неизменяемый полином. Выберем для этих целей, например, полином $x^4+x^3+x^2+x+1$. Остатком от деления будет полином $-5x^3-6x^2-3x+8$, а абсолютные значения его коэффициентов образуют число 5638, которое будет относительным адресом пакета.

Выбор алгоритма хеширования

Наиболее приемлемый алгоритм хеширования выбирают следующим образом: берут достаточно представительный набор ключей файла, применяют к нему все возможные алгоритмы хеширования и определяют число записей, направленных в каждый пакет основной области, и число записей, направленных в область переполнения.

Исследования подобного рода выполнялись неоднократно. Они показали, что лучшие результаты получаются, когда применяется метод деления. Метод средних квадратов дает результаты, близкие к теоретическим, полученным с использованием случайного преобразования ключей. Результаты применения сложных методов (метода преобразования основания системы счисления, метода Лина и метода деления полиномов) близки к тем, которые получаются при преобразовании ключей с помощью генератора случайных чисел.

Лучшим является не тот метод, который обеспечивает именно случайное распределение записей, а тот, который обеспечивает равномерное заполнение всего адресного пространства памяти.

III. МЕДИАКУЛЬТУРА СПЕЦИАЛИСТА

Тема 27. Введение. Медиасреда и медиакультура в условиях информационного общества

Краткое содержание

Цель и задачи дисциплины, предмет и объект изучения. Связь с другими дисциплинами специализации. Медиасреда и медиакультура в условиях информационного общества. Медиасреда, медиакультура и их роль в современном обществе. Эволюция медиасреды и медиакультуры. Функции медиакультуры. Этимология понятия «медиа». Особенности его употребление в современном мире. Воздействие медиасреды на человека. Медиатизация как атрибутивный принцип информатизации. Учебно-методическое обеспечение. Формы контроля.

Основные понятия и определения

Информатизация общества и культуры – это внедрение информационных технологий в социокультурную деятельность.

Цифровое искусство – творческая деятельность, основанная на использовании информационных технологий, результатом которой являются художественные произведения в цифровой форме.

Основные характеристики информационного общества: увеличение роли информации, знаний и информационных технологий в жизни общества; возрастание числа людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг; нарастающая информатизация общества с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и

электронных СМИ; создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах.

Принципы информационного общества: электронизация, компьютеризация, информатизация, медиатизация, виртуализация.

Социальная информация – это смыслы, движущиеся в социальном времени и пространстве, т. е. объекты (сообщения) социальной коммуникации.

Медиа (media) – средства массовой коммуникации – технические средства создания, записи, копирования, тиражирования, хранения, распространения, восприятия информации и обмена ее между субъектом (автором медиатекста) и объектом (массовой аудиторией).

Классификация медиа: по **типу основного средства** (печать, радио, кино, телевидение, видео, компьютерные сети и др.); по **каналу восприятия** (аудио, видео, аудиовизуальные, знаковые/текстовые, графические); по **месту использования** (индивидуальные, групповые, массовые, домашние, рабочие, транспортные и др.); по **содержанию** информации, направлению социализации (идеологические, политические, нравственно-воспитательные, познавательно-обучающие, эстетические, экологические, экономические); по **функциям и целям использования** (получение информации, образование, общение, решение проблем, развлечение, социальное управление); по **результату воздействия** на личность (развитие кругозора, самопознание, самовоспитание, самообучение, самоутверждение, самоопределение, регуляция состояния, социализация).

Основные теории медиа:

«Инъекционная» теория медиа (сильное и прямое воздействие медиа, понимание любого медиатекста как эффективного стимула, вызывающего немедленную ответную реакцию аудитории, которая представляет собой пассивную массу отдель-

ных индивидуумов, лишенных способности противостоять всевластному влиянию медиа; восприятие медиа в качестве опасного «агента упадка культуры» и т. д.).

Теория «потребления и удовлетворения» как теория ограниченного влияния медиа (медиа не формирует человеческое мировоззрение; медиа – только одна из частей человеческих потребностей, составляющая интеллектуального развития; аудитория активно отбирает для себя те медиатексты, которые удовлетворяют ее запросам и т. д.).

Идеологическая теория медиа (очень сильное воздействие медиа на аудиторию; медийное распространение идей в соответствии с установками «правящего класса»; деление аудитории на социальные классы; приоритет политических, классовых и моральных ценностей в медиатекстах; медиа как поле «идеологической борьбы» и т. д.).

Семиотическая теория медиа («медиа как система символов»; сильное влияние медиа на аудиторию; семиотический (знаковый) характер медиатекстов; аудитория – пассивная масса потребителей медийной мифологии; стремление медиа завуалировать многозначный знаковый характер своих текстов как угроза свободе потребления медийной информациии т. д.).

Этическая теория медиа (медиа способны формировать определенные духовные, этические/моральные, ценностные принципы аудитории).

Теологическая/религиозная теория медиа (медиа способны формировать определенные религиозные, духовные, этические/моральные, ценностные принципы аудитории).

Культурологическая теория медиа (сильное влияние медиа на аудиторию; медиатекст – сложная структура значений и «кодов», а медиа – поле борьбы различных социальных концепций; аудитория представляет собой сообщество «субкультурных формаций», групп с различными культурными ориентациями, разным уровнем «декодирования» медиатекстов; медиа, скорее, предлагают, чем навязывают интерпретацию медиатекстов; аудитория всегда находится в процессе диалога с

медиатекстами и их оценивания, она не просто «считывает» медийную информацию, а вкладывает различные смыслы в воспринимаемые медиатексты, самостоятельно их анализирует и т. д.).

Характеристики новой аудитории: большая активность по отношению к предлагаемому СМИ продукту; самостоятельное вступление в процесс его создания и распространения; активная аудитория участвует в создании единой коммуникативной виртуальной медиакультуры.

Мем (греч. «подобие») – это идея, образ или любой другой объект нематериального мира, который передается от человека к человеку вербально и невербально.

Медиавирус (англ. media virus) – термин, введенный американским специалистом в области средств массовой информации Дугласом Рашкоффом для обозначения медиасобытий, вызывающих прямо или косвенно определенные изменения в жизни общества. Медиавирусы – распространяющиеся по инфосфере мемы и мемокомплексы, чья информация изменяет восприятие людьми локальных и глобальных событий.

Медиакультура (media culture) – совокупность материальных и интеллектуальных ценностей в области медиа, а также исторически определенная система их воспроизводства и функционирования в социуме; по отношению к аудитории «медиакультура» может выступать системой уровней развития личности человека, способного воспринимать, анализировать, оценивать медиатекст, заниматься медиатворчеством, усваивать новые знания в области медиа.

Тема 28. Место и роль медиасреды и медиаобразования в профессиональной деятельности культуролога

Краткое содержание

Влияние информатизации общества на социокультурную реальность. Точки соприкосновения науки и искусства. Цифровое искусство как пример медиатизации культуры. История развития и теоретические основы цифрового искусства. Основ-

ные направления современного цифрового искусства: компьютерная графика, компьютерная музыка, мобилография, демосцена, интерактивный компьютерный перформанс и другие. Место цифрового искусства в современной художественной жизни и современном обществе. Выставки, проекты, фестивали компьютерного искусства. Видеоарт: отличительные черты, история возникновения, представители.

Интерактивность и проблема коммуникации. Сетевое искусство. Медиакультура как знаковая система. «Язык» и «код» медиакультуры как средство передачи реалий действительности, выполняющее полифункциональную роль в процессе репрезентации.

Мультимедийная информация как профессиональный ресурс культуролога. Общая характеристика медиасреды. Виды медиа (пресса, телевидение, кинематограф, видео, звукозапись, радио, Интернет и др.). Особенности современной социокультурной ситуации в условиях интенсивного развития медиасреды. Специфика общения, контакта аудитории с медиасредой. Психолого-педагогические аспекты восприятия мультимедийной информации. Медиавосприятие и развитие аудитории в области медиакультуры: основные понятия и проблемы. Медиаграмотность как показатель развития медиакультуры аудитории. Медиавосприятие – восприятие «медиареальности», чувств, мыслей и замыслов авторов медиатекста, выраженных в словесном, аудиовизуальном, пространственно-временном образах. Процесс медиавосприятия: образное обобщение, синтез элементов звукового, зрительного и пространственно-временного повествования. Условия восприятия, сопереживание и сотворчество. Уровни и типология медиавосприятия: «первичная идентификация», «вторичная идентификация», «комплексная идентификация». Особенности восприятия медиатекстов.

Медиаобразование как направление в педагогике, связанное с умениями и навыками восприятия, оценки и интерпретации информации, получаемой из медиасреды. Медиаобразование в современном мире и его влияние на развитие личности. Под-

держка медиаобразования со стороны ЮНЕСКО. Основные термины, теории, ключевые концепции, направления медиаобразования. Основные понятия медиасреды и медиаобразования. Классификации показателей развития аудитории в области медиакультуры. Основные исторические этапы развития медиаобразования в различных странах. Роль ЮНЕСКО и Совета Европы в процессе медиаобразования. Международные конференции по медиаобразованию.

Основные понятия и определения

Мультимедиа – это технология, описывающая порядок разработки, функционирования и применения средств обработки информации разных типов;

– это технология, объединяющая информацию (данные), звук, анимацию и графические изображения;

– информационный ресурс, созданный на основе технологий обработки и представления информации разных типов;

– компьютерное программное обеспечение, функционирование которого связано с обработкой и представлением информации разных типов;

– компьютерное аппаратное обеспечение, с помощью которого становится возможной работа с информацией разных типов;

– особый обобщающий вид информации, которая объединяет в себе как традиционную статическую визуальную (текст, графика), так и динамическую информацию разных типов (речь, музыка, видео фрагменты, анимация и т. п.).

Уровни медиавосприятия:

– уровень «первичной идентификации» – способность воспринимать цепь событий в медиатексте;

– уровень «вторичной идентификации» – способность сопереживать, поставить себя на место героя;

– уровень «комплексной идентификации» – способность соотнесения с авторской позицией, что позволяет предугадать ход событий медиатекста.

Медиакультура – целенаправленная общественно значимая деятельность в медиасреде и ее результаты.

Медиаобразование (согласно определению ЮНЕСКО) связано со всеми видами медиа (печатными и графическими, звуковыми, экранными и т. д.) и различными технологиями; дает возможность людям понять, как используется массовая коммуникация, овладеть способностью использовать медиа в коммуникации с другими людьми; *обеспечивает человеку знание* того, как:

– анализировать, критически осмысливать и создавать медиатексты;

– определять источники медиатекстов, их политические, социальные, коммерческие и/или культурные интересы, их контекст;

– интерпретировать медиатексты и ценности, распространяемые медиа;

– отбирать соответствующие медиа для создания и распространения своих собственных медиатекстов и обретения заинтересованной в них аудитории;

– получить возможность свободного доступа к медиа как для восприятия, так и для продукции.

Теории медиаобразования: идеологическая теория; социокультурная теория; культурологическая; теория «потребления и удовлетворения»; практическая теория; теория развития критического мышления/критической автономии; предохранительная/инъекционная/защитная теория; эстетическая/художественная; семиотическая теория; социокультурная теория.

Тема 29. Медиатекст как средство художественно-творческой, воспитательной и организационно-методической деятельности учреждений культуры и искусств

Краткое содержание

Медиатекст – результат медиапроизводства – сообщение, изложенное в любом виде и жанре медиа (сайт, телепередача, чат, форум, блог, статья, клип, баннер, рекламный ролик, компьютерная игра и т. д.). Принципы построения медиатекстов:

формульность, серийность, цитатность, интерактивность (динамичность), коммуникативность, синергичность, дружественность интерфейса (usability, UI) и др. Способы реализации интерактивности.

Жанровая структура медиа. Документальные медиатексты (официальный сайт (форум, блог)), репортаж, интервью, кинотелехроника и т. д.). Научно-популярные медиатексты. Учебные медиатексты: расчет на профессиональную специфику аудитории. Игровые медиатексты (компьютерные игры, фильмы, телепередачи, видеоклипы): специфика, тематическое многообразие. Анимационные медиатексты: роль, задачи, функции, виды (рисованные, объемные, аппликационные, силуэтные и др.). Межвидовые связи и синтез видов медиа. Композиция современного медиатекста. Синтез жанров – характерное явление современной медиакультуры. Условность жанровых делений.

Анализ произведений медиакультуры: ключевые содержательные моменты медиатекста; логика авторского мышления (в развитии конфликтов, характеров, идей, звукопластического ряда и т. д.); концепция автора (агентства) и личное отношение пользователя к данной позиции создателей медиатекста. Медиавоздействие – основная функция медиатекста. Медиаманипуляция как форма медиавоздействия.

Основные понятия и определения

Медиатекст – коммуникационное сообщение, изложенное в любом виде и жанре медиакоммуникации (роман, газетная статья, телепередача, видеоклип, фильм, сайт, поисковый сервис и пр.).

В отличие от линейного толкования текста как объединенной общим смыслом последовательности вербальных знаков, текст в массовой коммуникации приобретает черты *объемности* и *многослойности*. Это происходит за счет совмещения вербальной части текста с медийными свойствами того или иного средства массовой информации.

Медиатексты можно классифицировать по следующим признакам: по форме восприятия (звуковые, зрительные, комбинированные); по форме представления (аудио, видео, графиче-

ские, анимационные, мультимедийные); по содержанию (идеологические, политические, эстетические, культурологические и др.); по функциям и целям использования (информационные, развлекательные, компенсаторные и др.); по результату медиакоммуникации, в частности, по воздействию на личность (познание или введение в заблуждение, воспитание или развращение, самоопределение или декультурация, расширение или сжатие кругозора, развитие личности или медиазомбирование и др.).

Анализ медиатекста – изучение, трактовка медиатекста того или иного вида и жанра.

Виды анализа:

– *идентификационный* (identification analysis of media and media text) – распознание/идентификация скрытых сообщений в медиатекстах, т. к. медийные агентства часто предлагают упрощенные решения сложных проблем.

– *идеологический* (ideological analysis of media and media text) – анализ идеологических аспектов медийной сферы. Теоретической базой является идеологическая теория медиа. Предполагается, что медиа способны целенаправленно воздействовать на общественное мнение, в том числе в интересах того или иного социального класса, расы или нации.

– *иконографический* (iconographic analysis of media text) – ассоциативный анализ изображения в медиатексте (например, вода, огонь – как символы чистоты и разрушения), связанный с семиотическим анализом.

– *семиотический* (semiological analysis of media text) – анализ языка знаков и символов в медиатекстах; семиотический анализ медиатекста в учебных целях опирается на семиотическую теорию медиаобразования.

– *сюжетный/повествовательный* (narrative analysis of media and media text) – анализ сюжетов, фабул медиатекстов. Сюжетный анализ тесно связан со структурным, мифологическим, семиотическим и другими видами анализа медиа и медиатекстов.

– *автобиографический* (личностный) (autobiographical analysis of media text) – сопоставление своего жизненного опыта (событий личной жизни, проявлений своего характера в различных ситуациях) с жизненным опытом персонажей и авторов медиатекстов.

– *философский* (philosophical analysis of media and media text) – анализ философских аспектов медийной сферы и медиатекстов.

– *эстетический* (aesthetical analysis of media text) – анализ художественной концепции произведений медиакультуры разных видов и жанров, тесно связан с эстетической (художественной) теорией медиаобразования.

– *этический* (ethical analysis of media and media text) – анализ моральных аспектов в сфере медиа и в медиатекстах.

– *структурный* (structural analysis of media and media text) – анализ систем, отношений, форм медиакультуры, структуры медиатекстов.

Графический медиатекст – медиатекст, который репрезентует реальность в форме графических изображений.

Электронный медиатекст – медиатекст, созданный для репрезентации реальности в процессе электронной коммуникации.

Ключевые понятия для анализа медиатекста:

Агентство – коммуникант, источник медиатекста (источник воздействия: человек, организация – тот, кто организует коммуникацию).

Категория – жанр и тематика медиатекста (вид: печать, телевидение, кинематограф и др.; форма: рекламная, документная, образовательная и т. д.; жанр: статья, интервью, репортаж, драма, комедия и др.).

Технология – способ создания медиатекстов (графические редакторы, видеооборудование и т. д.).

Язык – комплекс средств и приемов выразительности, используемых при создании медиатекста.

Аудитория – реципиент, человек или группа, на которых воздействует или рассчитан медиатекст (обычно характеризу-

ется как «массовая», «белорусская», «молодежная» и т. п.; «целевая аудитория» – аудитория, на которую медиатекст рассчитан).

Репрезентация – «преподношение», как медиатекст преподносит действительность (медиатекст не отражает ее, а репрезентирует, преподносит в каком–либо виде с какой–либо целью: для убеждения целевой аудитории, формирования ее мнения и т. д.).

Эффективность медиатекста – степень достижения цели медиакоммуникации – заранее запланированного медиавоздействия (побуждение, знание, мнение, эмоция и др.) на целевую аудиторию.

Тема 30. Информационные ресурсы социокультурной сферы: технологии их поиска и передачи

Краткое содержание

Сущность и специфика информационной деятельности в художественно-эстетической и социально-культурной сфере. Основные характеристики и классификация информационных ресурсов. Текстовые, графические, аудио-, фото- и видеоресурсы. Мультимедийные ресурсы. Медиагалереи – базы данных и каталоги медиаресурсов. Интерактивное теле- и радиовещание. Определение и сохранение адреса (ссылки) Интернет-ресурса. Анализ ссылок и критерии анализа. Создание списка аннотированных ссылок профессиональных ресурсов культуролога.

Интернет-каталоги: тематические (предметные), иерархическая структура материала, встроенная система автоматического поиска по ключевым словам, примеры. Поисковые системы: принцип действия, индексация, категоризация (классификация), примеры.

Виды поискового запроса. Синтаксис языков запросов различных поисковых систем. Принцип подбора ключевых слов. Особенности поиска мультимедийной информации. Специфика поиска различных медиаресурсов по ключевым словам. Поиск похожих документов: по подобию, стилю и т. д.

Интернет-сообщества как информационный ресурс. Правила регистрации, участия и доступа к медиаресурсам (музыкальным, графическим, фото-, видео- и др.) Интернет-сообществ. Файлообменные (пиринговые) сети. Принципы построения: кооперативный обмен файлами через Интернет, равноправие участников, отсутствие выделенных серверов, передача файлов частями, сохранение работоспособности сети при любом количестве и любом сочетании доступных узлов. Пиринговые сетевые протоколы для кооперативного обмена файлами через Интернет. Среда для обмена. Статус пользователя: пир, сид, лич. Программы для работы в пиринговых сетях.

Основные понятия и определения

Информационный ресурс (в узком понимании) – это сетевые информационные ресурсы, доступные через компьютерные средства связи; (в широком понимании) – любая зафиксированная на традиционных или электронных носителях информация, пригодная для сохранения и распространения.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных и знаний, другие массивы информации в информационных системах (Закон Республики Беларусь «Об информации, информатизации и защите информации»).

Аннотированное описание (от annotatio замечание) – краткая характеристика информационного ресурса, которая показывает отличительные особенности и достоинства информационного ресурса, помогает пользователю сориентироваться в оценке и выборе.

Аннотированное описание может включать следующие элементы:

1) название и URL–адрес;

2) основное контентное наполнение;

3) организация обратной связи;

4) используемые средства навигации;

5) возможность использования в профессиональной деятельности культуролога.

Интернет-каталог – структурированный набор ссылок на сайты с кратким их описанием. Сайты внутри каталога разбиваются по темам, а внутри тем могут быть ранжированы по индексу цитирования, по дате добавления, алфавиту или другому параметру.

Классификация каталогов:

– закрытые каталоги (добавление сайтов в данный каталог может проводить только одно ответственное лицо);

– белые каталоги (не требуют обратную ссылку и ставят прямую ссылку);

– серые каталоги (требуют обратную ссылку и ставят прямую ссылку);

– черные каталоги (требуют обратную ссылку и не ставят прямую ссылку);

– каталоги сайтов с прямыми ссылками (при регистрации сайта в данном каталоге веб–мастер получает ответную прямую (без перенаправления) ссылку на свой сайт);

– каталоги сайтов с ссылками (регистрация сайта в данном каталоге не дает ссылки на регистрируемый сайт. Ссылки в таких каталогах даны через перенаправление (редирект)).

Поисковая система – программно–аппаратный комплекс с веб–интерфейсом, предоставляющий возможность поиска информации в Интернете. Под поисковой системой обычно подразумевается сайт, на котором размещен интерфейс (фронт–энд) системы.

Поисковые системы состоят из трех компонентов:

– агент (в сети можно встретить – паук) – перемещаясь по сети, собирает информацию;

– база данных – входит вся информация, которую собирают пауки;

– поисковый механизм, который пользователи используют как интерфейс для работы с базой данных.

Интернет-сообщество – группа людей со сходными интересами, которые общаются друг с другом в основном через Интернет. Технологии с помощью которых создаются сообще-

ства (веб–форумы, блоги и блог-платформы, вики, чаты, списки, рассылки, скайпкасты и др.).

Технология peer-to-peer – это схема построения распределенной сети, каждый узел которой может одновременно выступать как в роли клиента, получающего информацию, так и в роли сервера, информацию предоставляющего (сеть равных, в которой возможно взаимодействие между всеми узлами).

Пиринговые сети (peer-to-peer) – это технология построения распределенной сети, где каждый узел может одновременно выступать как в роли клиента (получателя информации), так и в роли сервера (поставщика информации).

Тема 31. Коммуникативное пространство. Сетевые сообщества

Краткое содержание

Коммуникативное пространство и его организация. Информация и коммуникация в обществе. Исследование Маршалла Маклюэна о формирующем воздействии электрических и электронных средств коммуникации на человека. Сетевые сообщества. Формы Интернет-сообществ (социальные сети, веб-форумы, блоги, вики, чаты, списки рассылки и т. д.). Технологии создания и регулирования деятельности сетевых сообществ. Особенности Интернет-общения. Правила этикета в сетевых сообществах.

Форум. Принципы организации. Правила поведения на форуме. Разграничение доступа. Модератор и администратор: обязанности и функции. Тематика форума. Чат. ICQ. Характерные особенности. История организации и развития. Технология организации. Программа-клиент. Коммерческая служба. Управление службой ICQ. Учетная запись. Основные данные учетной записи. Правила организации переписки, поиск пользователей в системе. Возможности использования в профессиональной деятельности культуролога форума и чата. Блог. История возникновения. Характеристики записей блога. Отличия блога от традиционного дневника. Разновидности блогов:

по авторам, тематической направленности, наличию/виду мультимедиа, особенностям контента, технической основе. Мотивация участия и функции блогов. Вики. Википедия. История. Концепции Википедии. Признаки. Возможности применения в профессиональной деятельности культуролога-менеджера. Рассылки как средство маркетинга и рекламы в профессиональной деятельности культуролога. Сервер списков рассылок. Рассылки электронной почты. Виды рассылок. Список рассылки. Групповой адрес. Информационная и/или рекламная рассылка. СПАМ, фишинг. Требования к рассылкам. Телефонные сети, информационный сервис и маркетинг. Интеграция телефонной сети и Интернет на уровне пользовательских сервисов – пример общей тенденции интеграции медиасреды.

Основные понятия и определения

Коммуникация – целесообразное взаимодействие через средство коммуникации субъектов коммуникации с помощью объекта коммуникации (в трансмиссионной модели: через канал коммуникант реципиенту передает сообщение).

Коммуникация – опосредованное и целесообразное взаимодействие двух субъектов (коммуниканта и реципиента) посредством сообщения – передаваемого от коммуниканта к реципиенту объекта, который может иметь, а может и не иметь материальной формы (рис. 3.1).

Основные элементы: отправитель, лицо, собирающее информацию и передающее ее; сообщение, представленное в той или иной форме; канал, или средства передачи; получатель, или лицо, которому предназначена информация и который интерпретирует ее.

Рис. 3.1. Типы коммуникации

Коммуникации свойственна целесообразность или функциональность, которая может проявляться в трех формах:

Материальной: перемещение материального объекта в геометрическом пространстве из одной точки в другую в течение некоторого астрономического времени.

Сигнальной: передача управляющих команд, например закодированной программы воспроизводства (биосинтеза, репликации) определенного организма (в пространстве – времени биологической системы) или команды в технической кибернетической системе (компьютере).

Смысловой: цель заключается не в обмене материальными предметами или сигналами, а в сообщении друг другу смыслов, обладающих идеальной природой. Носителями смыслов являются знаки, символы, тексты, имеющие внешнюю, чувственно воспринимаемую форму и внутреннее, постигаемое умозрительно содержание. При психической автокоммуникации смыслы движутся в психическом пространстве – времени внутри личности, т. е. в области ее духовной жизни. При социальной коммуникации – в социальном пространстве–времени.

Социальное пространство – интуитивно ощущаемая людьми система социальных отношений между ними.

Социальное время – интуитивно ощущаемое людьми течение социальной жизни, зависящее от интенсивности социальных изменений.

Социальная коммуникация есть движение смыслов в социальном времени и пространстве. Она имеет, как правило, материальные, чувственно воспринимаемые проявления и духовную, умопостигаемую сущность.

Смыслы, движущиеся в социальном пространстве – времени, представляют собой знания, умения, стимулы, эмоции.

В качестве коммуникантов и реципиентов социальной коммуникации обычно рассматривают три субъекта, относящихся к разным уровням социальной структуры: индивидуальную личность (И), социальную группу (Г), массовую совокупность (М). Они могут взаимодействовать друг с другом, образуя 9 видов социальных коммуникаций: И ↔ Г, И ↔ И, Г ↔ М и проч.

Формы пространственно – коммуникационного действия имеют лишь три аспекта: подражание, управление, диалог[1]. Диалог есть взаимодействие равноправных партнеров, которое возможно только между субъектами одинакового уровня. Между разноуровневыми субъектами может быть подражание или управление, но не диалог.

Пространственно – коммуникационную деятельность, где в качестве реципиента выступает И, Г либо М относят к индивидуальной, групповой и массовой коммуникации соответственно.

Основные типы коммуникационной деятельности представлены в таблице (табл. 3.1), где п – подражание; д – диалог; у – управление).

Таблица 3.1

Описание основных типов коммуникационной деятельности

№	Уровень	Обозначение	Примеры
1	инд.	И п И	копирование образца
2	инд.	И у И	команда
3	инд.	И д И	беседа
4	групп.	И п Г	референция (референтная группа)
5	групп.	И у Г	руководство коллективом, обучение
6	масс.	И п М	социализация
7	масс.	И у М	авторитаризм, массовый гипноз
8	инд.	Г п И	групповое подражание
9	инд.	Г у И	консилиум, суд
10	групп.	Г п Г	мода, детские коллективные игры
11	групп.	Г у Г	групповая иерархия
12	групп.	Г д Г	групповые переговоры, «обмен опытом»
13	масс.	Г п М	адаптация к среде, медиатизация политики
14	масс.	Г у М	руководство обществом, СМИ
15	инд.	М п И	подражание вождю, кумиру масс
16	инд.	М у И	обратная связь при авторитаризме
17	групп.	М п Г	подражание элите, массовый ажиотаж, толпа
18	групп.	М у Г	обратная связь при демократии
19	масс.	М п М	заимствование достижений
20	масс.	М у М	информационная агрессия
21	масс.	М д М	взаимодействие культур

[1] Диалог – от греческих logos – «слово» и dia – «через», «посредством»

Сетевое сообщество – группа людей, поддерживающих коммуникацию и ведущих совместную деятельность с помощью средств сетевых коммуникаций.

Сетевое сообщество – группа людей, взаимодействие которых протекает преимущественно в глобальных компьютерных сетях.

Предпосылки формирования сообществ в Сети связаны с процессами урбанизации, глобализации всех социальных процессов. В основе формирования социальных групп в Сети, лежит стремление личности к достижению определенных целей, что возможно через создание группы.

Маршалл Маклюэн – первый теоретик масс-медиа, который утверждал, что само средство коммуникации и есть сообщение, то есть важно не конкретное содержание «послания», а то, как средство сообщения меняет наши масштабы восприятия мира, себя.

Сетевое общество – общество, в котором значительная часть информационных взаимодействий производится с помощью информационных сетей.

Социальный сервис Интернета – средство социальной коммуникации в Интернете, объединяющее людей в сетевые сообщества. Включает компьютерную сеть (серверы, хосты и т. п.), коммуникационное программное обеспечение и веб–сервис.

Виды социальных сервисов Интернета:

Блог – сервис, основное назначение которого состоит в выражении и возможной публикации авторского мнения (в форме дневника). Блогом управляет хозяин, он ведет дискурс, определяя его структуру и регламент, статус и права посетителей. В частности, хозяин блога регламентирует порядок доступа посетителей к своим публикациям, возможности их комментирования, публикации ими иных сообщений.

Вики – сервис, наполнение структуры и содержания которого выполняется пользователями с помощью представленных инструментов.

Географический сервис – сервис для совместной работы с картами (размещение информации, создание комментариев и т. д.).

Социальная сеть – сервис построения сообществ из людей со схожими интересами и/или деятельностью на одной аппаратной и программной платформе, может включать другие сервисы.

Социальное хранилище – сервис хранения и совместного использования файлов.

Форум – сервис, основное назначение которого состоит в организации и проведении обсуждений заданных тем. Размещая на форуме свои сообщения, посетители могут вести обсуждение. Управление форумом осуществляют администраторы и модераторы.

Примеры социальных сервисов	
URL–адрес	Описание
http://www.livejournal.com	Блог–система «LiveJournal» – «Живой журнал». Наиболее популярный среди русскоязычных пользователей блог-ресурс, считается одним из первых примеров сервисов социальных сетей
http://www.wikipedia.org	Открытая многоязычная энциклопедия Wikipedia. Эта социальная система ориентирована на подготовку энциклопедических статей о любом понятии. Система предусматривает возможности коррекции и обсуждения статей, сравнения их версий
http://picasa.google.com	Сервис публикации фотографий. На этом сервисе каждый посетитель имеет возможность публиковать, редактировать, отправлять и распечатывать свои фотографии
http://www.delicious.com	Сервис публикации аннотированных ссылок. Публикуются ссылки с описаниями, ведутся личные иерархические каталоги ссылок. В сети рассчитывается рейтинг ссылки на основе частоты переходов и использования в личных закладках
http://www.facebook.com	Социальная сеть, в которой возможно создание профиля с фотографиями, приглашение друзей, обмен сообщениями, оповещение других пользователей, создание групп по интересам

Платформа блогов – ресурс, предоставляющий возможность любому пользователю завести свой персональный блог и организовать работу с ним. Примеры блог-платформ: LiveInternet.ru – http://www.liveinternet.ru; LiveJournal – http://www. livejournal.com; WordPress – http://wordpress.com; Blogger – http://www.blogger.com и др.

Направления использования блогов в профессиональной деятельности культуролога:

– использование блога для организации индивидуального пространства культуролога;

– использование блога для организации и проведения дискуссий;

– использование блога для организации и проведения коллективных дискуссий и совместной работы над проектом.

Блог как индивидуальное пространство культуролога, средство социокультурного просвещения аудитории (двусторонний канал коммуникации, основная форма коммуникации «я» → «все»): создание личного пространства культуролога для размещения просветительного материала; создание электронных медиабиблиотек по определенной тематике (рис. 3.2).

Рис. 3.2. Схема блога как индивидуального пространства культуролога

Блог как инструмент для организации культурно–массовых мероприятий и проведения дискуссий (двусторонний канал коммуникации, основная форма коммуникации «я» ↔ «все»): организация обсуждения высказываний аудитории по предложенному вопросу (оценка медиатекста, анализ культурологической проблемы и т. д.), опросов для определения мнений аудитории по интересующему вопросу (рис. 3.3).

Рис. 3.3. Схема блога как инструмента
для организации и проведения дискуссий

Блог как инструмент для коллективной организации и проведения мероприятий, в том числе дискуссий: коллективное ведение блога культурологом и пользователями (двусторонний канал коммуникации, основная форма коммуникации «все» ↔ «все»): организация открытых и закрытых сообществ для коллективного обсуждения предлагаемой проблемы и проведение совместной работы над проектом; предоставление пользователям возможности обмена сообщениями (рис. 3.4).

Рис. 3.4. Схема блога как инструмента
для коллективной организации и проведения дискуссий

Пиринговые сети (peer-to-peer) – это технология построения распределенной сети, где каждый узел может одновременно выступать как в роли клиента (получателя информации), так и в роли сервера (поставщика информации).

Тема 32. Авторское право и информационная безопасность в Интернете

Краткое содержание

Условия соблюдения авторских прав при использовании информационных ресурсов Интернет. Правовое регулирование деятельности на примере фотобанков. Понятие лицензионного соглашения. Особенности белорусского правового поля. Меры по защите авторских прав на создаваемые электронные ресурсы. Элементы специального знака авторского права. Защита авторских прав на информационное наполнение веб-сайта.

Виды противоправной деятельности в медиасреде: распространение вирусов, фишинг, получение несанкционированного доступа к информационным и иным ресурсам, сетевые атаки, незаконное использование программного обеспечения и т. д. Способы защиты от противоправных действий: конфигурация системного ПО и оборудования, распределение компетенций, политики контроля и ограничения доступа к сетевым ресурсам, ПО для защиты от вирусов и несанкционированного доступа.

*Электронные публикации***.** Правила цитирования электронных источников на физическом носителе (CD-ROM, DVD-ROM, электронный гибкий диск и т. д.) и электронных публикаций в Интернете (статей, телеконференций, электронных словарей и др.). Размещение медиатекстов в Интернет. Специфика размещения различных видов медиаресурсов: графики, музыки, видео, галерей и т. п.

Основные понятия и определения

Авторское право – совокупность норм права, регулирующих отношения по поводу создания и использования произведений науки, литературы, искусства.

Лицензионный договор – соглашение, по которому одна сторона патентообладатель (лицензиар) передает право на использование изобретения (полезной модели, промышленного образца) другому лицу (лицензиату), а последний принимает на себя обязанность вносить лицензиару обусловленные договором платежи и осуществлять другие действия, предусмотренные договором об исключительной или неисключительной лицензии.

Электронная публикация – способ публикации материалов в виде электронных медиатекстов, при котором их восприятие происходит с помощью электронных средств медиа.

При цитировании материала из Интернета можно придерживаться следующего формата ссылки: название произведения; имя автора (псевдоним), имена соавторов; дата публикации (если возможно обнаружить); название сайта; адрес страницы сайта, содержащей произведение.

Тема 33. Компьютерные среды для работы с медиаприложениями

Краткое содержание

Браузеры. Программное обеспечение для навигации и просмотра веб-ресурсов. История развития. Распространенные браузеры (Internet Explorer, Mozilla Firefox, Google Chrome, Opera и другие): сравнительные характеристики и возможности. Текстовые браузеры. Браузеры для портативных устройств. Назначение и специфика использования. Статистика использования браузеров в Интернете.

Стандартные платформы и интегрированные медиапродукты для работы с мультимедийной информацией: Microsoft, Apple. Операционные системы Windows, комплекты серверных программ, мультимедийная продукция, средства разработки программ и др. Операционная система Apple – первая в области персональных компьютеров и современных многозадачных операционных систем с графическим интерфейсом.

Специализированные платформы. Adobe Integrated Runtime (AIR) как эмуляция интернет-среды в качестве рабочей платформы компьютера. Платформенно независимая среда для запуска приложений, позволяющая использовать HTML/CSS, Ajax, Adobe Flash и Adobe Flex для переноса веб-программ на настольные персональные компьютеры. Преимущества: доступ к файловой системе, буферу обмена, поддержка нескольких окон, технологии drag and drop; возможность переноса готового HTML или Adobe Flex приложения на компьютер пользователя; работа в off-line режиме, передача накопленных в процессе работы данных в момент появления соединения. Недостатки: ограниченный доступ к SQLite и веб-сервисам, зависимость от среды выполнения Adobe. Приложения, разработанные с использованием Abobe AIR.

Основные понятия и определения

Браузер – программа, с помощью которой пользователь организует взаимодействие с WWW-серверами и другими сервисами и ресурсами Интернета.

Средства коммуникации – средства, обеспечивающие взаимодействие между людьми, совместно работающими над решением общих задач. К электронным средствам коммуникации относятся электронная почта, календари, чаты, вики, корпоративные закладки, блоги, социальные сети и т. д. Электронные средства коммуникации обеспечивают поддержку как индивидуальной, так и групповой работы людей, которые могут работать совместно вне зависимости от их географического расположения.

По уровню обеспечиваемого взаимодействия электронные средства коммуникации условно можно разделить на индивидуальные средства (электронная почта, факс, голосовая почта и др.), коллективные средства (видео- и аудиоконференции, интернет-форумы, чаты и др.) и средства управления (электронные календари, системы управления проектами, совместное управление документами, совместная видеозапись и др.).

Организацию совместной работы в Интернете рассмотрим на примере сервиса Google: приложения для обмена сообщениями (Gmail, Google Talk, Google Calendar), приложения для взаимодействия (Google Docs, Google Sites, Google Reader, Blogger, Picasa Web Albums, Google Video, и др.).

Для того, чтобы воспользоваться этими сервисами, необходимо войти на *Google* и выбрать ссылку *Еще* (рис. 3.5).

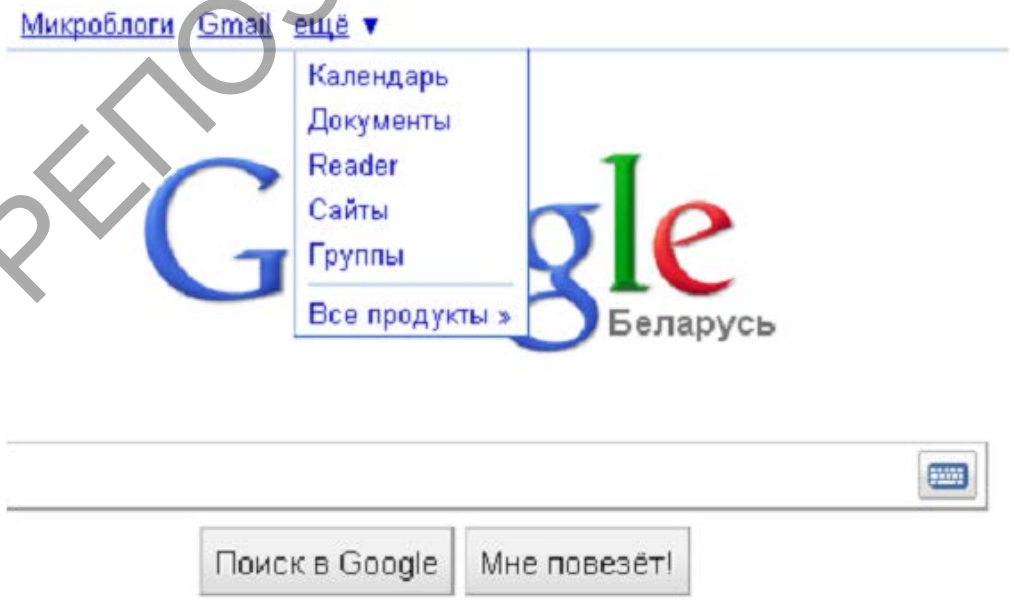


Рис. 3.5. Доступ к сервисам Google

Рассмотрим технологию работы с Google Docs.

Google Docs – это веб-редакторы текста, презентаций, таблиц, форм и картинок, которые позволяют пользователю:

– создавать новые документы в Интернете;

– загружать в Интернет существующие документы с вашего компьютера;

– хранить документы в Интернете и обмениваться ими с другими пользователями;

– совместно работать над документами в онлайн–режиме;

– экспортировать документы из Интернета к себе на компьютер.

Adobe Adobe Integrated Runtime – кроссплатформенная среда выполнения, позволяющая разработчикам использовать стандарты HTML/CSS, Ajax, JavaScript, программное обеспечение Adobe Flash Professional и Adobe Flex и язык ActionScript для развертывания веб-приложений, которые реализуются в виде автономных клиентских приложений и на которые не распространяются ограничения, связанные с применением браузера.

Тема 34. Программные средства создания, редактирования и управления медиатекстами

Краткое содержание

Компьютерная графика и анимация. Виды и особенности применения в профессиональной деятельности культуролога. Обзор и анализ программных средств. Основные технологии создания анимации. GIF-анимация. FLASH-анимация.

Создание и обработка видео. Особенности применения в профессиональной деятельности культуролога. Основные характеристики видео. Обзор и анализ программных средств.

Компоновка (англ. compositing) – создание целостного изображения путем совмещения двух и более слоев (видео, анимации, изображений, текста и др.). Программы для создания спецэффектов и компоновки. Интерфейс и функциональные возможности программ. Настройка рабочего пространства программ. Создание нового проекта. Импортирование файлов. Ос-

новы работы с импортированными файлами. Управление импортированными файлами. Основные настройки окон. Управление проектом и просмотром видеоматериала. Основные элементы управления проектом. Понятие видеокомпозиции. Способы создания новых композиций. Многослойные композиции. Работа со слоями. Основные свойства слоя. Базовые операции над слоями: редактирование параметров, выравнивание, распределение, трансформация и др. Временная шкала и ее основные настройки. Создание простой анимации. Инструменты цветокоррекции. Эффекты размывания и резкости, особенности их применения при работе с видеоматериалом. Применение альфа-канала для сложной компоновки. Типы альфа-каналов. Специальные эффекты. Совместное использование эффектов. Текст. Текстовые эффекты. Звук. Основы работы. Создание переходов. Микширование звука. Отображение звуковой информации. Настройка общей громкости звука клипа. Просмотр композиции, управление просмотром. Свойства композиции. Готовый продукт. Настройки экспорта. Экспорт клипа в различные форматы.

Основные понятия и определения

Компьютерная графика – область деятельности, связанная с созданием и обработкой цифровых изображений.

Компьютерная графика – область информатики, занимающаяся проблемами получения, представления, обработки и отображения различных изображений (рисунков, чертежей, мультипликации) при помощи компьютера.

Компьютерная графика – процесс создания, обработки и вывода изображений разного рода с помощью компьютера.

Компьютерная графика – вид искусства.

Растровая графика – компьютерная графика, в которой изображение представляется двумерным массивом точек (элементов растра), цвет и яркость каждой из которых задается независимо. Программные средства: Adobe Photoshop, Corel Photo-Paint, Microsoft Paint, GNU Image Manipulation Program и др.

Векторная графика – компьютерная графика, в которой изображения описываются в виде математических объектов – «контуров». Каждый контур представляет собой независимый объект, который можно перемещать, масштабировать и изменять. Векторную графику часто называют также объектно-ориентированной графикой. Программные средства: Corel DRAW, Adobe Illustrator и Xara Designer и др.

Фрактальная графика – компьютерная графика, в которой изображения описываются в виде математических процедур построения «фракталов». Фрактал – это бесконечно самоподобная геометрическая фигура. Бесконечное самоподобие означает, что в любом фрагменте фигуры найдется часть, подобная всей фигуре. Структура фрактала не меняется при изменении масштаба. Поэтому в памяти компьютера хранится информация только об этой структуре и алгоритм ее масштабирования. Программные средства: Fractint, Fractal Explorer, Apophysis и др.

Формат – способ организации цифровых данных в файле. Графические форматы служат для цифрового кодирования изображений.

По типу «хранимой» графики различают следующие форматы:

– растровые (PNG, TIFF, GIF, BMP, JPEG и др.);

– векторные (AI, CDR, DXF и др.);

– смешанные (EPS, PDF и др.).

Название формата обычно совпадает с расширением файла.

Видео – технология записи, обработки, передачи, хранения и воспроизведения визуального или аудиовизуального материала.

Анимация – видеотехнология создания и воспроизведения последовательности рисунков с частотой, при которой обеспечивается целостное и непрерывное зрительное восприятие их изменений.

Компьютерная анимация – динамичная компьютерная графика, основанная на применении различных динамических визуальных эффектов (движущиеся картинки, выделение цветом, шрифтом отдельных элементов и т. п.); синтез динамических изображений, создающий иллюзию движения на экране дисплея.

Анимационный медиатекст – медиатекст, который репрезентирует реальность в форме анимации.

Видеомедиатекст – медиатекст, который репрезентирует реальность в форме видео.

Основные технологии создания анимации:

– Классическая (традиционная) анимация представляет собой поочередную смену рисунков, каждый из которых нарисован отдельно.

– Спрайтовая анимация реализуется при помощи языка программирования.

– Морфинг – преобразование одного объекта в другой за счет генерации заданного количества промежуточных кадров.

– 3D-анимация создается при помощи специальных программ трехмерного моделирования. Медиатексты получаются путем визуализации сцены, а каждая сцена представляет собой набор объектов, источников света и текстур.

– «Захват движения» – технология анимации, которая дает возможность передавать естественные, реалистичные движения в реальном времени. Датчики прикрепляются на живого актера в местах, соответствующих контрольным точкам компьютерной модели для ввода и оцифровки движения. Координаты актера и его ориентация в пространстве передаются графической системе, и анимационные модели оживают.

Основные характеристики видео и анимационного медиатекста:

– Битрейт или ширина видеопотока (для цифрового видео) – это количество обрабатываемых бит видеоинформации за секунду времени (измеряется «бит/с» – бит в секунду или, чаще, «Мбит/с» – мегабит в секунду). Чем шире видеопоток, тем лучше качество видео.

– Глубина цвета – количество бит, приходящихся на кодирование цвета в одном пикселе. Для цветовой модели RGB обычно характерны следующие режимы глубины цвета: 24 бит/пиксель, 48 бит/пиксель.

– Разрешение – ширина и высота кадра в пикселях. Стандартное разрешение (SD, Standard Definition) – формат DVD с

разрешением 720 x 576 (PAL), 720 x 480 (NTSC). Высокое разрешение (HD, High Definition) – HD720 (1280 x 720 точек) и HD1080 (1920 x 1080 точек).

– Частота кадра – это число неподвижных изображений, сменяющих друг друга за 1 секунду показа видео или анимационного материала и создающих эффект движения объектов на экране. Чем больше частота кадра, тем более плавным и естественным будет казаться движение (24 кадра в секунду – скорость записи и воспроизведения кинофильмов, 25 и 30 кадров в секунду в телевизионных стандартах PAL/SECAM и в NTSC; 4–15 кадров в секунду – для анимационного GIF или SWF, например, баннера на web-странице).

Создание и обработка видео и анимационных медиатекстов:

GIF-анимация – растровая компьютерная анимация, сохраненная в формате GIF, который поддерживает возможность использования режима индексированных цветов (не более 256), режим постепенного проявления изображения (interleaved), прозрачность и использует алгоритм сжатия без потерь качества LZW. Средства – Adobe Photoshop, GIF Animator и др.

FLASH-анимация – векторная компьютерная анимация, способная объединить в одном формате текст, графику, звук, анимацию, интерактивные компоненты. Средства – Adobe Flash, Adobe Animate.

Создание и обработка видео. Средства – Adobe Premiere, Adobe After Effects и др.

Тема 35. Медиапроект социально-культурной тематики: технологии создания и размещения

Краткое содержание

Проектирование творческой работы культуролога на основе материалов, полученных из медиасреды. Медиапроект социально-культурной тематики как способ организации профессиональной деятельности культуролога. Значение проектной

деятельности в работе культуролога. Типология Интернет-проектов. Использование медиасреды на различных этапах выполнения медиапроекта. Методика использования медиаресурсов при работе над медиапроектом. Способы реализации медиапроекта: блог, видеоролик, форум, медиагалерея и др.

Оформление материалов для размещения в Интернете. Работа над композицией текста. Принципы построения композиции. Основные требования к верстке: расположению фотографий, текста, заголовка, используемые шрифты, наличие дополнительных элементов. Работа с заголовками. Изменение принципов создания заголовков. Значение содержимого элемента «заголовок» для успешного поиска ресурса. SEO-копирайтинг: адаптация текстов для поисковых систем, оптимизация страниц сайта (включение ключевых слов): мета-тэги title, description, keywords; название страниц и заголовков в тексте.

Методика включения в медиапроекты элементов медиаобразования. Формы медиаобразования: медиагалереи, фотовыставки, дискуссионные медиаклубы, любительские медиастудии и др. Критерии развития аудитории в области электронной медиаграмотности. Методика проведения социологического исследования предпочтений аудитории в области медиакультуры.

Основные понятия и определения

Интернет-проект – совокупность гипертекстовых документов, отражающих общий замысел (план) или предварительные схемы создания какой-либо информационной инфраструктуры; под Интернет-проектом можно подразумевать любую технически реализуемую концепцию информационного массива, масштаб, программная поддержка и сетевая стратегия которого зависят от ряда важнейших факторов, влияющих на уровень популяризации проекта, его надежности и рентабельности.

Интернет-проекты можно условно разделить на три большие группы: торговые, контентные (содержательные) и Интернет-сервисы.

Функции интернет-проектов: информационная; рекламная; организация товародвижения; платежная; создание дохода; производство товаров.

SEO (Search Engines Optimization, продвижение сайтов, раскрутка сайтов) – оптимизация сайтов для поисковых систем. SEO обозначает продвижение сайтов в поисковых системах по нужным ключевым словам, а термин «оптимизация» используется для обозначения работы с внутренними факторами, влияющими на ранжирование.

Медиаграмотность – приобретенная способностью человека к восприятию, созданию, анализу, оценке медиатекстов, к пониманию социокультурного и политического контекста функционирования медиа в современном мире, кодовых и репрезентационных систем, используемых медиа; результат медиаобразования, изучения медиа.

Медиаграмотность – умение осваивать, интерпретировать, анализировать и создавать медиатексты с целью медиакоммуникации.

Таблица 3.2.

Система показателей развития медиаграмотности аудитории

Показатели развития аудитории в области медиакультуры	Расшифровка уровня данного показателя
«понятийный»	Знание истории, теории и терминологии медиакультуры
«сенсорный» («контактный»)	Систематическое общение с медиа, умение выбирать любимые жанры, темы и пр.
«мотивационный»	Мотивы контакта с медиа: эмоциональные, гносеологические, нравственные, эстетические, терапевтические и др.
«оценочный»	Уровень медиавосприятия, способность к анализу и синтезу медиатекстов
«креативный»	Уровень творческого начала в различных аспектах деятельности (игровой, художественной, исследовательской и др.), связанной с медиа

ПРАКТИЧЕСКИЙ РАЗДЕЛ

МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ СЕМИНАРОВ

к разделу II
«Основы теории информации и криптологии»

Тема 16. Система передачи информации

Цель: изучить этапы обращения и передачи информации.

Вопросы:

1. Этапы обращения информации: восприятие, подготовка, обработка, отображение, воздействие, передача и хранение.
2. Структурная схема системы передачи информации.
3. Дискретные и непрерывные сообщения. Алфавит источника сообщений.
4. Кодирование и декодирование информации. Модуляция и демодуляция.
5. Понятие линии связи. Помехи. Верность передачи.
6. Уровни проблем передачи информации: синтаксический, семантический и прагматический.

Литература

1. Кудряшов, Б. Д. Теория информации: учеб. пособие / Б. Д. Кудряшов. – СПб. : СПбГУ ИТМО, 2010. – 188 с.

2. Тарасенко, Ф. П. Введение в курс теории информации / Ф. П. Тарасенко. – Томск : ТГУ, 1963. – 240 с.

3. Фурсов, В. А. Лекции по теории информации: учеб. пособие / В. А. Фурсов / под ред. Н. А. Кузнецова. – Самара : Самар. гос. аэрокосм. ун-т, 2006. – 148 с.

Тема 18. Форматы данных в Интернете

Цель: углубить и систематизировать знания об основных форматах данных в Интернете.

Вопросы:

1. Система верстки книг TeX.
2. Универсальный язык программирования PostScript.
3. Программа-интерпретатор Ghostscript.
4. Расширения имен ps, eps, pfa, pfb, afm, pfm.
5. Формат PDF.
6. Формат DjVu.
7. Форматы JPEG, GIF, PNG.
8. Форматы psd, ico, svg, swf, tif.

Литература

1. Открытый формат – Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Открытый_формат. – Дата доступа: 12.11.2015.

2. Список форматов файлов – Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Список_ форматов_файлов. – Дата доступа: 12.11.2015.

3. Формат графического файла на Web-странице // КомпьютерПресс [Электронный ресурс]. – Режим доступа: compress. ru/article. aspx?id= 10542. – Дата доступа: 12.11.2015.

4. Форматы текстовых и графических файлов – My-comp.by [Электронный ресурс]. – Режим доступа: www.my-comp.by/ index.../73-format-failov.html. – Дата доступа: 12.11.2015.

Тема 19. Сжатие информации

Цель: углубить и систематизировать знания об основных методах сжатия информации.

Вопросы:

1. Преобразование Барроуза–Уилера.
2. Классы приложений с алгоритмами сжатия.
3. Требования приложений к алгоритмам сжатия.
4. Методы сжатия видеоданных.
5. Словарные методы сжатия.

6. Классификация методов сжатия информации.

7. Алгоритмы сжатия аудиосигналов.

8. Цифровое кодирование звуковых сигналов.

Литература

1. Алгоритмы: построение и анализ = Introduction to Algorithms / Х. Томас. – 2-е изд. – М. : Вильямс, 2006. – 1296 с.

2. Блаттер, К. Вейвлет-анализ. Основы теории / К. Блаттер – М. : Техносфера, 2006. – 279 с.

3. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс / пер. с англ. – М. : Техносфера, 2006. – 1072 с.

4. Ковалгин, Ю. А. Цифровое кодирование звуковых сигналов / Ю. А. Ковалгин, Э. И. Вологодин. – СПб. : КОРОНА-принт, 2004. – 240 с.

5. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин [и др.]. – М. : Диалог-МИФИ, 2002. – С. 384.

6. Ричардсон, Я. Видеокодирование. H.264 и MPEG-4 – стандарты нового поколения / Я. Ричардсон. – М. : Техносфера, 2005. – 368 с.

7. Сэломон, Д. Сжатие данных, изображений и звука / Д. Сэломон. – М. : Техносфера, 2004. – 368 с.

8. Тропченко, А. Ю. Методы сжатия изображений, аудиосигналов и видео: учеб. пособие / А. Ю. Тропченко, А. А. Тропченко. – СПб. : СПбГУ ИТМО, 2009. – 108 с.

9. Фурсов, В. А. Лекции по теории информации : учеб. пособие / В. А. Фурсов / под ред. Н. А. Кузнецова. – Самара : Самар. гос. аэрокосм. ун-т, 2006. – 148 с.

Тема 20. Энтропия дискретного источника

Цель: изучить понятия условной и дифференциальной энтропии.

Вопросы:

1. Объединение ансамблей.
2. Понятие условной энтропии.
3. Свойства условной энтропии.
4. Дифференциальная энтропия.
5. Количество информации.
6. Свойства дифференциальной энтропии.
7. Количество информации как мера снятой неопределенности.
8. Передача информации от дискретного источника.

Литература

1. Кудряшов, Б. Д. Теория информации : учеб. пособие / Б. Д. Кудряшов. – СПб. : СПбГУ ИТМО, 2010. – 188 с.

2. Фурсов, В. А. Лекции по теории информации : учеб. пособие / В. А. Фурсов / под ред. Н. А. Кузнецова. – Самара : Самар. гос. аэрокосм. ун-т, 2006. – 148 с.

3. Тарасенко, Ф. П. Введение в курс теории информации / Ф. П. Тарасенко. – Томск : ТГУ, 1963. – 240 с.

Тема 24. Стандарты и правовые акты электронной цифровой подписи

Цель: изучить основные стандарты и законы об электронной цифровой подписи.

Вопросы:

1. Формирование подписи в стандарте DSS. Проверка подписи в стандарте DSS. Проблемы стойкости алгоритма DSA.

2. Механизм цифровой подписи в стандарте RSA. Алгоритмы генерации и проверки подписи в стандарте RSA.

3. Протоколы генерации ключей. Главные ключи. Ключи шифрования ключей файлов. Сеансовые ключи.

4. Протоколы взаимной аутентификации. Протоколы прямого обмена ключами. Протоколы распределения сеансовых ключей с использованием центра распределения ключей.

5. Закон Республики Беларусь об электронном документе и электронной цифровой подписи. Назначение и применение электронной цифровой подписи. Юридическая сила электронного документа.

6. Государственная система управления открытыми ключами. Карточка и сертификат открытого ключа.

Литература

1. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

2. Об информации, информатизации и защите информации: Закон Респ. Беларусь 10 нояб. 2008 г. № 455-З: принят Палатой представителей 9 окт. 2008 г.: одобр. Советом Респ. 22 окт. 2008 г. [Электронный

ресурс]. – Режим доступа: http://www. pravo.by/webnpa/text.asp?start=-1&RN=H10800455. – Дата доступа: 10.09.2010.

3. Об электронном документе и электронной цифровой подписи: Закон Респ. Беларусь 28 дек. 2009 г. № 113-З: принят Палатой представителей 4 дек. 2009 г.: одобр. Советом Респ. 11 дек. 2009 г. [Электронный ресурс]. – Режим доступа: http://www.pravo.by/webnpa/text.asp?RN=H10900113. – Дата доступа: 10.09.2010.

к разделу III
«Медиакультура специалиста»

Тема 27. Введение. Медиасреда и медиакультура в условиях информационного общества. Влияние информатизации общества на социокультурную реальность

Цель: изучить основные направления информатизации культуры.

Вопросы:

1. Точки соприкосновения науки и искусства. Цифровое искусство как пример медиатизации культуры.
2. История развития и теоретические основы цифрового искусства.
3. Основные направления современного цифрового искусства: компьютерная графика, компьютерная музыка, мобилография, демосцена, интерактивный компьютерный перформанс и другие.
4. Место цифрового искусства в современной художественной жизни и современном обществе. Выставки, проекты, фестивали компьютерного искусства. Примеры.
5. Видеоарт: отличительные черты, история возникновения, представители.

Литература

1. Гасумова, С. Е. Информационные технологии в социальной сфере / С. Е. Гасумова. – М. : Дашков и Ко, 2011. – 248 с.

2. Ерохин, С. В. Цифровое компьютерное искусство / С. В. Ерохин. – СПб. : Алетейя, 2011. – 192 с.

3. Соколова, И. В. Социальная информатика / И. В. Соколова. – 2-е изд., с изм. и доп. – М. : Перспектива, РГСУ, 2008. – 272 с.

4. Шлыкова, О. В. Культура мультимедиа : учеб. пособие для студентов вузов / О. В. Шлыкова. – М. : ГРАНД–ФАИР, 2004. – 416 с.

5. http://www.adobemuseum.com – музей виртуального искусства.

6. http://mediaforum.mediaartlab.ru – представлены авангардные направления творчества художников, перформеров, видеоартистов, аниматоров, экспериментирующих с языком, контекстом и техникой электронных и дигитальных средств массовой информации.

Тема 28. Место и роль медиасреды и медиаобразования в профессиональной деятельности культуролога. Медиаобразование как направление деятельности культуролога

Цель: определить место и роль электронной медиасреды и медиаобразования в профессиональной деятельности культуролога.

Вопросы:

1. Психолого-педагогические аспекты восприятия мультимедийной информации. Особенности восприятия медиатекстов.
2. Медиаобразование. Основные термины, теории, ключевые концепции и направления медиаобразования.
3. Классификации показателей развития аудитории в области медиакультуры.
4. Основные исторические этапы развития медиаобразования в различных странах.
5. Роль ЮНЕСКО и Совета Европы в процессе медиаобразования. Международные конференции по медиаобразованию.

Литература

1. Брайант, Дженнингз. Основы воздействия СМИ : пер. с англ. / Дженнингз Брайант, Сузан Томпсон. – М. : Вильямс, 2004. – 432 с.

2. Выгонский, С. И. Обратная сторона Интернета. Психология работы с компьютером и сетью / С. И. Выгонский. – М. : Феникс, 2010. – 320 с.

3. Разлогов, К. Искусство экрана. От синематографа до Интернета / К. Разлогов. – М. : Российская политическая энциклопедия, 2010. – 304 с.

4. Федоров, А. В. Медиаобразование и медиаграмотность : учеб. пособие для вузов / А. В. Федоров. – Таганрог : Кучма, 2004. – 340 с.

5. Федоров, А. В. Медиаобразование: история, теория и методика / А. В. Федоров. – Ростов : ЦВВР, 2001. – 708 с.

6. Федоров, А. В. Медиаобразование: социологические опросы / А. В. Федоров. – Таганрог : Кучма, 2007. – 228 с.

7. http://www.ifap.ru – программа ЮНЕСКО «Информация для всех».

8. http://www.mediagram.ru – электронный ресурс по медиаграмотности.

9. http://www.edu.of.ru/mediaeducation – электронный ресурс по медиаобразованию.

10. http://www.psyfactor.org/lybr.htm – материалы психологической и общегуманитарной тематики (медиавоздействие, медиаманипуляции).

Тема 31. Коммуникативное пространство. Сетевые сообщества

Цель: углубить и систематизировать имеющиеся знания о правилах функционирования и средствах организации сетевых сообществ.

Вопросы:

1. Коммуникационное пространство и его организация. Информация и коммуникация в обществе.

2. Исследование Маршалла Маклюэна о формирующем воздействии электрических и электронных средств коммуникации на человека.

3. Особенности интернет-общения. Правила этикета в сетевых сообществах.

4. Форум. Принципы организации. Правила поведения на форуме. Разграничение доступа. Модератор и администратор: обязанности и функции. Тематика форума.

5. Чат. Характерные особенности. История организации и развития. Технология организации. Возможности использования в профессиональной деятельности культуролога форума и чата.

6. Блог. История возникновения. Характеристики записей блога. Отличия блога от традиционного дневника.

7. Вики. Википедия. История. Концепции Википедии. Признаки. Возможности применения в профессиональной деятельности культуролога-менеджера.

8. Рассылки как средство маркетинга и рекламы в профессиональной деятельности культуролога. Сервер списков рассылок.

Литература

1. Брайант, Дженнингз. Основы воздействия СМИ : пер. с англ. / Дженнингз Брайант, Сузан Томпсон. – М. : Вильямс, 2004. – 432 с.

2. Волохонский, В. Л. Психологические механизмы и основания классификации блогов / В. Л. Волохонский // Личность и межличностное взаимодействие в сети Internet : сб. ст. СПбГУ; под ред. В. Л. Волохонского, Ю. Е. Зайцевой, М. М. Соколова. – СПб. : СПбГУ, 2006. – С. 117–131.

3. Жданевич, И. М. Коммуникативное пространство. Личность и межличностное взаимодействие в сети Internet / И. М. Жданевич, Е. И. Кучерявый. – М. : Компак, 2002. – 286 с.

4. Кветна, И. Маркетинг в социальных сетях – ставка на доверие / И. Кветна // Маркетинг и реклама. – 2009. – № 6.

5. Кучников, Т. В. Общение в Интернет / Т. В. Кучников. – М. : Альянс-пресс, 2004. – 128 с.

6. Лазарев, В. Г. Рассылки как средство маркетинга и рекламы / В. Г. Лазарев, Г. Г. Савин. – М. : Эрудит, 2005. – 301 с.

7. Ландэ, Д. В. Поиск знаний в Internet. Профессиональная работа / Д. В. Ландэ. – М. : Вильямс, 2005. – 272 с.

8. Сафонова, Т. В. Порядок интеракции в сетевых дневниках: альтернативная экономика сообщений / Т. В. Сафонова // Личность и межличностное взаимодействие в сети Internet : сб. ст. СПбГУ ; под ред. В. Л. Волохонского, Ю. Е. Зайцевой, М. М. Соколова. – СПб. : СПбГУ, 2006. – С. 55–75.

9. Сметанина, С. И. Медиатекст в системе культуры: динамические процессы в языке и стиле журналистики конца XX века / С. И. Сметанина. – М. : Издательство Михайлова В. А., 2002. – 384 с.

Тема 32. Авторское право и информационная безопасность в Интернете

Цель: изучить основные вопросы авторского права в сети Интернет.

Вопросы:

1. Условия соблюдения авторских прав при использовании информационных ресурсов Интернета.

2. Правовое регулирование деятельности на примере фотобанков. Понятие лицензионного соглашения.

3. Меры по защите авторских прав на создаваемые электронные ресурсы. Элементы специального знака авторского права. Защита авторских прав на информационное наполнение веб-сайта.

4. Виды противоправной деятельности в медиасреде: распространение вирусов, фишинг, получение несанкционированного доступа к информационным и иным ресурсам, сетевые атаки, незаконное использование программного обеспечения и т. д.

5. Способы защиты от противоправных действий: конфигурация системного программного обеспечения и оборудования, распределение компетенций, политики контроля и ограничения доступа к сетевым ресурсам, программное обеспечение для защиты от вирусов и несанкционированного доступа.

6. Электронные публикации. Правила цитирования электронных источников на физическом носителе (CD, DVD, электронный гибкий диск и т. д.) и электронных публикаций в Интернете (статье, телеконференции, электронные словари и др.).

7. Размещение медиатекстов в Интернете. Специфика размещения различных видов медиаресурсов: графики, музыки, видео и т. д.

Литература

1. ГОСТ 7.82–2001 Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления. – Минск, 2001. – 35 с.

2. ГОСТ 7.83–2001 Электронные издания. Основные виды и выходные сведения. – Минск, 2001. – 6 с.

3. Об авторском праве и смежных правах : Закон Респ. Беларусь, 16 мая 1996 г., № 370-XIII : в ред. Закона Респ. Беларусь от 14.07.2008 г. // Нац. реестр правовых актов Респ. Беларусь. – 2001. – № 2/519.

4. Зима, В. М. Безопасность глобальных сетевых технологий / В. М. Зима. – СПб. : БХВ-Петербург, 2003. – 368 с.

5. Чашин, А. Н. Борьба с правонарушениями в сети Интернет / А. Н. Чашин. – М. : Дело и Сервис, 2010. – 80 с.

Тема 34. Программные средства создания, редактирования и управления медиатекстами. Программно-компьютерные среды для работы с медиаприложениями

Цель: изучить основные платформы для работы с медиаприложениями, знать их достоинства и недостатки, возможности использования в зависимости от поставленных профессиональных задач.

Вопросы:

1. Программное обеспечение для навигации и просмотра веб-ресурсов. Браузеры: сравнительные характеристики и возможности.

2. Статистика использования браузеров в Интернете.

3. Стандартные платформы и интегрированные медиапродукты для работы с мультимедийной информацией.

4. Специализированные платформы. Adobe Integrated Runtime (AIR) как эмуляция Интернет-среды в качестве рабочей платформы компьютера.

Литература

1. Дьяконов, В. П. Браузер Opera. Специальный справочник / В. П. Дьяконов. – СПб. : Питер, 2007. – 336 с.

2. Ландэ, Д. В. Поиск знаний в Internet. Профессиональная работа / Д. В. Ландэ. – М. : Вильямс, 2005. – 272 с.

3. Торопков, С. А. Альтернативные браузеры / С. А. Торопков. – М. : Наука, 2006. – 319 с.

4. Adobe AIR. Практическое руководство по среде для настольных приложений Flash и Flex / Дж. Лотт [и др.]. – П. : Символ-Плюс, 2009. – 352 с.

МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

к разделу I
«Прикладная математика»

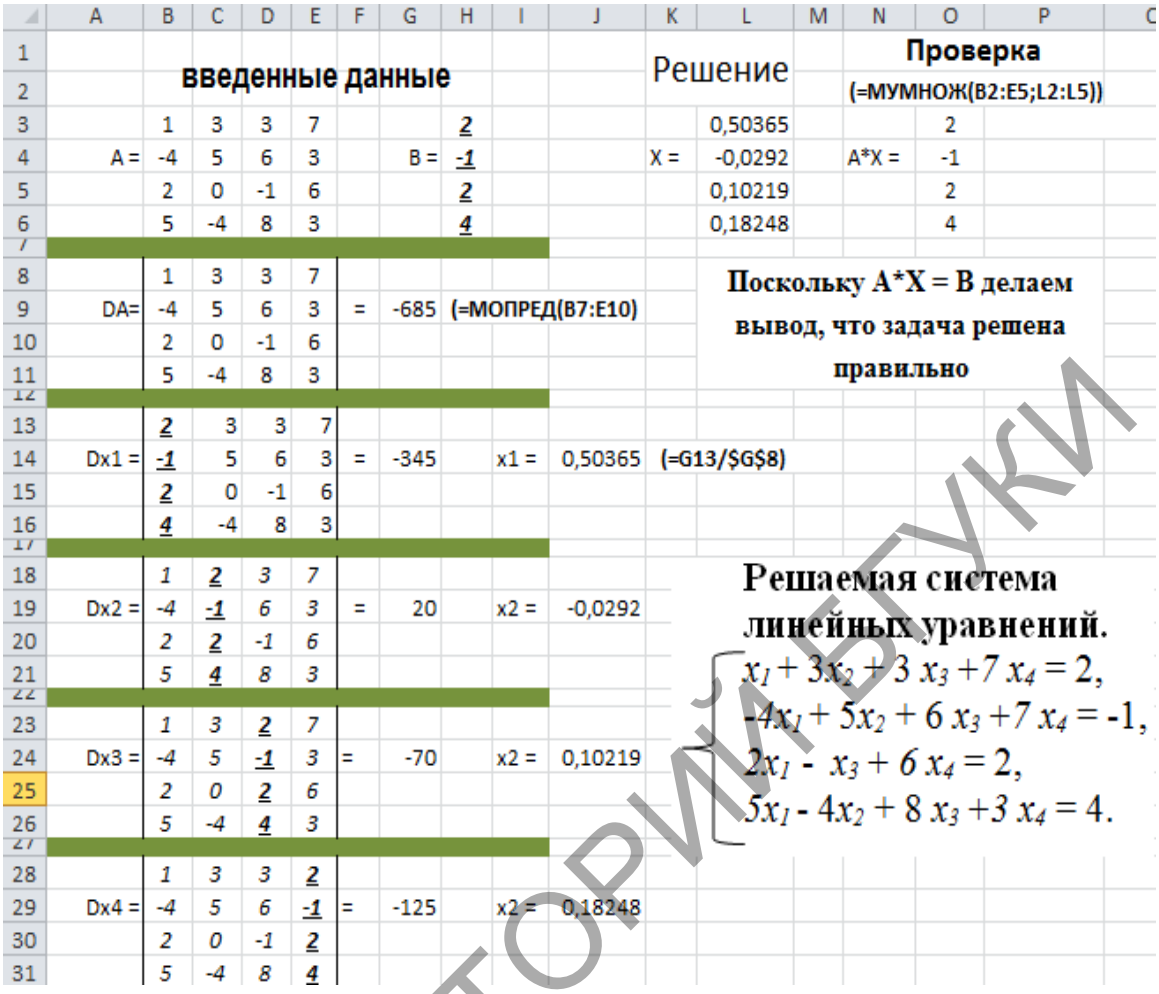
Тема 3. Линейные уравнения

Лабораторная работа 1. **Решение систем линейных уравнений с помощью табличного редактора Microsoft Excel**

Цель: используя встроенные математические функции Microsoft Excel научиться решать системы линейных уравнений методом Крамера и методом обратной матрицы.

Задание 1. Записать матрицу *A* размерности 4x4 и вектор *B* размерности 4x1 произвольно. Составить систему линейных уравнений с матрицей ***A*** и вектором значений ***B***. Решить систему линейных уравнений методом Крамера, используя функцию вычисления определителя матрицы МОПРЕД. Проверить полученное решение, используя функцию умножения матриц МУМНОЖ.

Пример решения



				введенные данные							Решение			**Проверка**			
														(=МУМНОЖ(B2:E5;L2:L5))			
		1	3	3	7			2				0,50365			2		
	A =	-4	5	6	3		B =	-1			X =	-0,0292		A*X =	-1		
		2	0	-1	6			2				0,10219			2		
		5	-4	8	3			4				0,18248			4		
		1	3	3	7												
	DA=	-4	5	6	3	=	-685	(=МОПРЕД(B7:E10)									
		2	0	-1	6												
		5	-4	8	3												
		2	3	3	7												
	Dx1 =	-1	5	6	3	=	-345		x1 =	0,50365	(=G13/G8)						
		2	0	-1	6												
		4	-4	8	3												
		1	2	3	7												
	Dx2 =	-4	-1	6	3	=	20		x2 =	-0,0292							
		2	2	-1	6												
		5	4	8	3												
		1	3	2	7												
	Dx3 =	-4	5	-1	3	=	-70		x2 =	0,10219							
		2	0	2	6												
		5	-4	4	3												
		1	3	3	2												
	Dx4 =	-4	5	6	-1	=	-125		x2 =	0,18248							
		2	0	-1	2												
		5	-4	8	4												

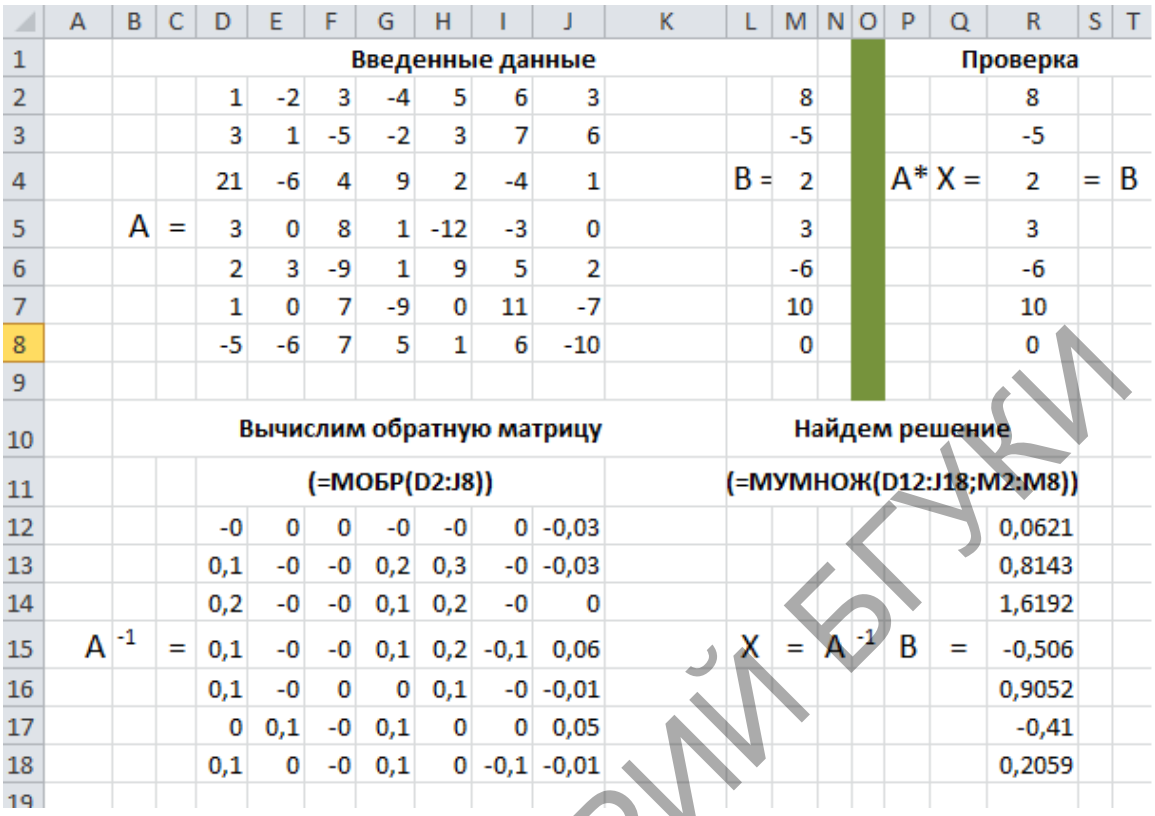
Поскольку A*X = B делаем вывод, что задача решена правильно

Решаемая система линейных уравнений.

$$\begin{cases} x_1 + 3x_2 + 3x_3 + 7x_4 = 2, \\ -4x_1 + 5x_2 + 6x_3 + 7x_4 = -1, \\ 2x_1 - x_3 + 6x_4 = 2, \\ 5x_1 - 4x_2 + 8x_3 + 3x_4 = 4. \end{cases}$$

Задание 2. Записать матрицу *A* размерности 7x7 и вектор *B* размерности 7x1 произвольно. Составить систему линейных уравнений с матрицей ***A*** и вектором значений ***B***. Решить систему линейных уравнений с помощью обратной матрицы, используя функцию вычисления обратной матрицы МОБР и функцию умножения матриц МУМНОЖ. Проверить полученное решение.

Пример решения



1				Введенные данные													Проверка			
2				1	-2	3	-4	5	6	3			8				8			
3				3	1	-5	-2	3	7	6			-5				-5			
4				21	-6	4	9	2	-4	1		B =	2			A* X =	2	=	B	
5		A	=	3	0	8	1	-12	-3	0			3				3			
6				2	3	-9	1	9	5	2			-6				-6			
7				1	0	7	-9	0	11	-7			10				10			
8				-5	-6	7	5	1	6	-10			0				0			
9																				
10				Вычислим обратную матрицу								Найдем решение								
11				(=МОБР(D2:J8))								(=МУМНОЖ(D12:J18;M2:M8))								
12				-0	0	0	-0	-0	0	-0,03							0,0621			
13				0,1	-0	-0	0,2	0,3	-0	-0,03							0,8143			
14				0,2	-0	-0	0,1	0,2	-0	0							1,6192			
15		A^{-1}	=	0,1	-0	-0	0,1	0,2	-0,1	0,06		X	=	A^{-1}	B	=	-0,506			
16				0,1	-0	0	0	0,1	-0	-0,01							0,9052			
17				0	0,1	-0	0,1	0	0	0,05							-0,41			
18				0,1	0	-0	0,1	0	-0,1	-0,01							0,2059			
19																				

Тема 6. Задачи оптимизации на графах

Лабораторная работа 1. Достижимость

Цель: научиться решать задачи на достижимость.

Задача. Фирма-поставщик располагает возможностью осуществлять бесплатные перелеты между 10 городами, перелеты между которыми заданы списком рейсов. Необходимо: 1) построить матрицу смежности графа бесплатных перелетов; 2) построить промежуточные матрицы, отражающие возможности перевозок с одной, двумя, тремя, четырьмя, пятью пересадками и т. д.; 3) построить матрицу достижимости графа; по матрице достижимости найти города в которые фирма-поставщик может осуществлять перелеты *из заданного города* бесплатно; 4) построить путь из одного заданного города в другой с заданным количеством пересадок, если таковой имеется. Ниже приведены варианты задачи:

Вариант 1

1) Список городов: *Бостон, Дрезден, Копенгаген, Нью-Йорк, Берлин, Пекин, Рим, Рейкьявик, Москва, Франкфурт.*

2) *Бостон – Дрезден, Бостон – Копенгаген, Дрезден – Берлин, Дрезден – Рим, Копенгаген – Нью-Йорк, Нью-Йорк – Пекин, Берлин – Копенгаген, Берлин – Франкфурт, Пекин – Берлин, Пекин – Москва, Рим – Бостон, Рим – Пекин, Рейкьявик – Пекин, Москва – Пекин, Франкфурт – Бостон, Франкфурт – Рейкьявик.*

3) *Дрезден.*

4) Из *Берлина* в *Москву* с *тремя* пересадками.

Вариант 2

1) Список городов: *Будапешт, Франкфурт, Киев, Кишинев, Берлин, Стамбул, Рим, Рейкьявик, Москва, Гаага.*

2) *Будапешт – Берлин, Будапешт – Рим, Киев – Москва, Франкфурт – Берлин, Кишинев – Стамбул, Кишинев – Гаага, Берлин – Кишинев, Стамбул – Берлин, Стамбул – Москва, Рим – Будапешт, Рим – Стамбул, Рейкьявик – Москва, Москва - Кишинев, Гаага – Будапешт, Гаага - Рейкьявик.*

3) *Рим.*

4) Из *Рима* в *Стамбул* с *четырьмя* пересадками.

Вариант 3

1) Список городов: *Лондон, Люксембург, Женева, Минск, Берлин, Киев, Москва, Рим, Астана, Пекин.*

2) *Лондон – Берлин, Женева – Астана, Женева –Минск, Люксембург – Пекин, Люксембург – Лондон, Минск – Пекин, Минск – Люксембург, Берлин - Киев, Киев – Астана, Москва – Лондон, Москва – Пекин, Рим – Берлин, Астана – Лондон, Астана – Рим, Пекин – Москва, Пекин – Лондон.*

3) *Москва.*

4) Из *Минска* в *Киев* с *тремя* пересадками.

Вариант 4

1) Список городов: *Дрезден, Люксембург, Франкфурт, Минск, Берлин, Милан, Москва, Рим, Вена, Мадрид*.

2) Минск – Берлин, Минск – Мадрид, Дрезден – Берлин, Дрезден – Люксембург, Люксембург – Дрезден, Вена – Минск, Дрезден – Мадрид, Франкфурт – Вена, Вена – Рим, Франкфурт – Дрезден, Берлин – Франкфурт, Берлин – Рим, Милан – Вена, Москва – Дрезден, Рим – Франкфурт, Мадрид – Рим.

3) *Берлин.*

4) Из *Минска* в *Мадрид* с *четырьмя* пересадками.

Пример решения

Фирма-поставщик располагает возможностью осуществлять бесплатные перелеты между городами:

Минск, Милан, Вильнюс, Мюнхен, Берлин, Киев, Рим, Варшава, Москва, Франкфурт;

перелеты между которыми заданы списком рейсов:

Минск – Милан, Милан – Рим, Вильнюс – Мюнхен, Мюнхен – Берлин, Берлин – Вильнюс, Берлин – Франкфурт, Киев – Берлин, Киев – Москва, Рим – Минск, Варшава – Москва, Москва – Киев, Москва – Франкфурт, Франкфурт – Минск, Франкфурт – Киев, Франкфурт – Варшава.

Необходимо: 1) построить матрицу смежности графа бесплатных перелетов; 2) построить промежуточные матрицы, отражающие возможности перевозок с одной, двумя, тремя, четырьмя, пятью пересадками и т. д.; 3) построить матрицу достижимости графа; по матрице достижимости определить города в которые фирма-поставщик может осуществлять перелеты из *Милана* бесплатно; 4) построить путь из *Мюнхена* в *Вильнюс* с *четырьмя* пересадками, если таковой имеется.

Решение. Решим задачу с помощью Excel.

1. Построим матрицу смежности графа ***A***, и введем две вспомогательные матицы слева.

Матрица смежности А		Минск	Милан	Вильнюс	Мюнхен	Берлин	Киев	Рим	Варшава	Москва	Франкфурт
		1	2	3	4	5	6	7	8	9	10
Минск	1	0	1	0	0	0	0	0	0	0	0
Милан	2	0	0	0	0	0	0	1	0	0	0
Вильню	3	0	0	0	1	0	0	0	0	0	0
Мюнхен	4	0	0	0	0	1	0	0	0	0	0
Берлин	5	0	0	1	0	0	0	0	0	0	1
Киев	6	0	0	0	0	1	0	0	0	1	0
Рим	7	1	0	0	0	0	0	0	0	0	0
Варшав	8	0	0	0	0	0	0	0	0	1	0
Москва	9	0	0	0	0	0	1	0	0	0	1
Франкф	10	1	0	0	0	0	1	0	1	0	0

A_1=A

	1	2	3	4	5	6	7	8	9	10
1	0	1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	0	0	0
3	0	0	0	1	0	0	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0
5	0	0	1	0	0	0	0	0	0	1
6	0	0	0	0	1	0	0	0	1	0
7	1	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	1	0
9	0	0	0	0	0	1	0	0	0	1
10	1	0	0	0	0	1	0	1	0	0

A_1=A

	1	2	3	4	5	6	7	8	9	10
1	0	1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	0	0	0
3	0	0	0	1	0	0	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0
5	0	0	1	0	0	0	0	0	0	1
6	0	0	0	0	1	0	0	0	1	0
7	1	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	1	0
9	0	0	0	0	0	1	0	0	0	1
10	1	0	0	0	0	1	0	1	0	0

2. Построим матрицу *A*x*A*, перемножив вспомогательные матрицы A_1 и A_1 с помощью функции МУМНОЖ. Построим матрицу А2, показывающую наличие перелета с одной пересадкой, заменив в матрице АхА все элементы большие 1 на 1 с помощью функции ЕСЛИ.

Построим матрицу *A*x*A*x*A*, перемножив матрицу *A*x*A* и вспомогательную матрицу A_2 = A.

А2 - наличие пути с одной пересадкой		Минск	Милан	Вильнюс	Мюнхен	Берлин	Киев	Рим	Варшава	Москва	Франкфурт
		1	2	3	4	5	6	7	8	9	10
Минск	1	0	0	0	0	0	0	1	0	0	0
Милан	2	1	0	0	0	0	0	0	0	0	0
Вильнюс	3	0	0	0	0	1	0	0	0	0	0
Мюнхен	4	0	0	1	0	0	0	0	0	0	1
Берлин	5	1	0	0	1	0	1	0	1	0	0
Киев	6	0	0	1	0	0	1	0	0	0	1
Рим	7	0	1	0	0	0	0	0	0	0	0
Варшава	8	0	0	0	0	0	1	0	0	0	1
Москва	9	1	0	0	0	1	1	0	1	1	0
Франкфу	10	0	1	0	0	1	0	0	0	1	0

Матрица АхА. Перемножаем матрицы A_1 и A_1 функцией **МУМНОЖ(O4:X13;AA4:AJ13)**

	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	1	0	0	0
2	1	0	0	0	0	0	0	0	0	0
3	0	0	0	0	1	0	0	0	0	0
4	0	0	1	0	0	0	0	0	0	1
5	1	0	0	1	0	1	0	1	0	0
6	0	0	1	0	0	1	0	0	0	2
7	0	1	0	0	0	0	0	0	0	0
8	0	0	0	0	0	1	0	0	0	1
9	1	0	0	0	1	1	0	1	1	0
10	0	1	0	0	1	0	0	2	0	

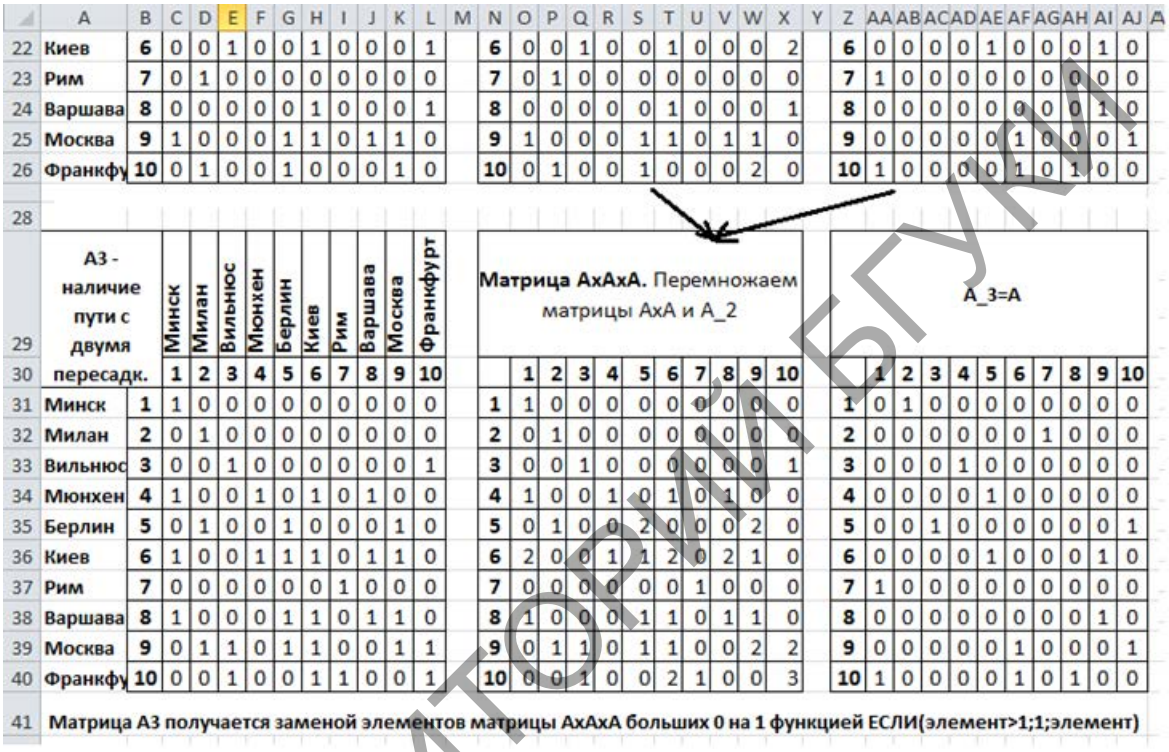
A_2=A

	1	2	3	4	5	6	7	8	9	10
1	0	1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	0	0	0
3	0	0	0	1	0	0	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0
5	0	0	1	0	0	0	0	0	0	1
6	0	0	0	0	1	0	0	0	1	0
7	1	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	1	0
9	0	0	0	0	0	1	0	0	0	1
10	1	0	0	0	0	1	0	1	0	0

Матрица А2 получается заменой элементов матрицы АхА больших 0 на 1 функцией ЕСЛИ(элемет>1;1;элемент)

Затем построим матрицу А3, показывающую наличие перелета с двумя пересадками, заменив в матрице *A*x*A*x*A* все элементы большие 1 на 1.

По аналогии построим матрицы А4, А5, А6, А7, А8, А9, А10, отвечающие соответственно за количество пересадок на единицу меньшее номера матрицы.



		6	0	0	1	0	0	1	0	0	0	1
		7	0	1	0	0	0	0	0	0	0	0
		8	0	0	0	0	0	1	0	0	0	1
		9	1	0	0	0	1	1	0	1	1	0
		10	0	1	0	0	1	0	0	0	1	0

		6	0	0	1	0	0	1	0	0	0	2
		7	0	1	0	0	0	0	0	0	0	0
		8	0	0	0	0	0	1	0	0	0	1
		9	1	0	0	0	1	1	0	1	1	0
		10	0	1	0	0	1	0	0	0	2	0

		6	0	0	0	0	1	0	0	1	0
		7	1	0	0	0	0	0	0	0	0
		8	0	0	0	0	0	0	0	1	0
		9	0	0	0	0	0	1	0	0	1
		10	1	0	0	0	0	1	0	1	0	0

А3 - наличие пути с двумя пересадк.		Минск	Милан	Вильнюс	Мюнхен	Берлин	Киев	Рим	Варшава	Москва	Франкфурт
		1	2	3	4	5	6	7	8	9	10
Минск	1	1	0	0	0	0	0	0	0	0	0
Милан	2	0	1	0	0	0	0	0	0	0	0
Вильнюс	3	0	0	1	0	0	0	0	0	0	1
Мюнхен	4	1	0	0	1	0	1	0	1	0	0
Берлин	5	0	1	0	0	1	0	0	0	1	0
Киев	6	1	0	0	1	1	1	0	1	1	0
Рим	7	0	0	0	0	0	0	1	0	0	0
Варшава	8	1	0	0	0	1	1	0	1	1	0
Москва	9	0	1	1	0	1	1	0	0	1	1
Франкфу	10	0	0	1	0	0	1	1	0	0	1

Матрица АхАхА. Перемножаем матрицы АхА и А_2

1	1	0	0	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0	0	1
4	1	0	0	1	0	1	0	1	0	0
5	0	1	0	0	2	0	0	0	2	0
6	2	0	0	1	1	2	0	2	1	0
7	0	0	0	0	0	0	1	0	0	0
8	1	0	0	0	1	1	0	1	1	0
9	0	1	1	0	1	1	0	0	2	2
10	0	0	1	0	0	2	1	0	0	3

A_3=A

1	0	1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	0	0	0
3	0	0	0	1	0	0	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0
5	0	0	1	0	0	0	0	0	0	1
6	0	0	0	0	1	0	0	0	1	0
7	1	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	1	0
9	0	0	0	0	0	1	0	0	0	1
10	1	0	0	0	0	1	0	1	0	0

Матрица А3 получается заменой элементов матрицы АхАхА больших 0 на 1 функцией ЕСЛИ(элемент>1;1;элемент)

3. Далее построим матрицу достижимости D, найдя сумму матриц $D_s = E+A$+A2+A3+A4+A5+A6+A7+A8+A9+A10 и заменив в полученной матрице D_s элементы большие 1 на 1.

Элемент (*i, j*) матрицы достижимости *D* равный 1, показывает, что из города *i* в город *j* есть путь, равный 0 означает, что таковой отсутствует. Таким образом, из Милана фирма-поставщик может осуществить бесплатные перелеты в города Минск и Рим.

D		Минск	Милан	Вильнюс	Мюнхен	Берлин	Киев	Рим	Варшава	Москва	Франкфурт
		1	2	3	4	5	6	7	8	9	10
Минск	1	1	1	0	0	0	0	1	0	0	0
Милан	2	1	1	0	0	0	0	1	0	0	0
Вильнюс	3	1	1	1	1	1	1	1	1	1	1
Мюнхен	4	1	1	1	1	1	1	1	1	1	1
Берлин	5	1	1	1	1	1	1	1	1	1	1
Киев	6	1	1	1	1	1	1	1	1	1	1
Рим	7	1	1	0	0	0	0	1	0	0	0
Варшава	8	1	1	1	1	1	1	1	1	1	1
Москва	9	1	1	1	1	1	1	1	1	1	1
Франкфу	10	1	1	1	1	1	1	1	1	1	1

Ds										
	1	2	3	4	5	6	7	8	9	10
1	4	4	0	0	0	0	3	0	0	0
2	3	4	0	0	0	0	4	0	0	0
3	4	3	6	5	6	6	2	4	5	5
4	5	4	6	6	7	7	3	5	6	6
5	6	5	7	6	8	8	4	6	7	7
6	7	6	8	7	9	10	5	7	9	8
7	4	3	0	0	0	0	4	0	0	0
8	7	6	7	6	8	9	5	8	9	8
9	8	7	8	7	9	10	6	8	10	9
10	7	6	7	6	8	9	5	7	8	8

E										
	1	2	3	4	5	6	7	8	9	10
1	1	0	0	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0	0	0
4	0	0	0	1	0	0	0	0	0	0
5	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	1	0	0	0	0
7	0	0	0	0	0	0	1	0	0	0
8	0	0	0	0	0	0	0	1	0	0
9	0	0	0	0	0	0	0	0	1	0
10	0	0	0	0	0	0	0	0	0	1

4. За путь с четырьмя пересадками из Мюнхена в Вильнюс отвечает матраца А5. Поскольку на пересечении строки «Мюнхен» и столбца «Вильнюс» стоит 1, такой путь существует. Построим его.

По матрице *A* определяем, что из Мюнхена можно вылететь только в Берлин. Таким образом, осталось проложить маршрут из Берлина в Вильнюс с тремя пересадками. По матрице *A* определим, что из Берлина есть вылеты в Вильнюс и Франкфурт. Поскольку стоит задача добраться из Мюнхена в Вильнюс с четырьмя пересадками, перелет Берлин-Вильнюс рассматривать не будем. С помощью матрицы А3 убедимся что из Франкфурта в Вильнюс существует маршрут с двумя пересадками. Итак имеем:

Мюнхен – Берлин – Франкфурт – … – … – Вильнюс. По матрице *A* определяем, куда можно вылететь из Франкфурта: Минск, Киев, Варшава. По матрице А2 проверяем наличие перелетов до Вильнюса с одной пересадкой для каждого из трех городов. Такой перелет возможен только для города Киева. Имеем: Мюнхен – Берлин – Франкфурт – Киев – … – Вильнюс.

Из Киева существуют перелеты в Берлин и Москву, однако перелет из Москвы в Вильнюс отсутствует. Таким образом получаем маршрут:

Мюнхен – Берлин – Франкфурт – Киев – Берлин – Вильнюс.

Тема 11. Основные распределения случайных величин

Лабораторная работа 1. **Биномиальное распределение**

Цель: научиться решать практические задачи, используя закон биномиального распределения.

Пример. Требуется подсчитать число изделий в партии фармакологического препарата, не соответствующих требованиям. Все причины, влияющие на качество препарата, принимаются одинаково вероятными и независящими друг от друга. Сплошная проверка качества в этой ситуации не возможна, поскольку изделие, прошедшее испытание, не подлежит дальнейшему использованию. Для контроля из партии наудачу выбирают определенное количество образцов изделий n. Эти образцы всесторонне проверяют и регистрируют число бракованных изделий k. Считают, что вероятность брака составляет $p = k / n$. 1) Найти вероятность того, что из m выбранных наудачу единиц препарата l окажутся бракованными; 2) найти вероятность того что из m выбранных наудачу единиц препарата не более l окажутся бракованными; 3) найти вероятность того, что из m выбранных наудачу единиц препарата, количество бракованных изделий будет превышать r, но окажется меньшим l.

Биномиальное распределение применяется для вычисления вероятности в задачах с фиксированным числом тестов или испытаний, когда результатом любого испытания может быть только успех или неудача.

Воспользуемся функцией Excel **БИНОМРАСП (число_успехов; число_испытаний; вероятностъ_успеха; интегральная)**, где

число_успехов – количество успешных испытаний;

число_испытаний – число независимых испытаний;

вероятность_ успеха – это вероятность успеха каждого испытания;

интегральное – это логическое значение, определяющее форму функции.

Если данный параметр имеет значение **ИСТИНА** (=1), то считается интегральная функция распределения (вероятность того, что число успешных испытаний не менее значения *число_успехов*); если этот параметр имеет значение **ЛОЖЬ** (=0), то вычисляется значение функции плотности распределения (вероятность того, что число успешных испытаний в точности равно значению аргумента *число_успехов*).

Для решения в диалоговом окне **Мастер функций** выбираем **Статистическая → БИНОМРАСП**. В поле **число_успехов** вводим количество бракованных препаратов *l*, в поле **число_испытаний** – *m*. В поле **вероятность_успеха** вводим *p*. В поле **интегральная** вводим 0. В результате получаем вероятность того, что из *m* выбранных наудачу единиц препарата *l* окажутся бракованными. Для ответа на второй вопрос задачи в поле **интегральная** необходимо ввести 1. Вероятность того, что из *m* выбранных наудачу единиц препарата количество бракованных изделий будет превышать *r*, но окажется меньшим *l,* будет равно **БИНОМРАСП (*l*; *m*; *p*; 1) – БИНОМРАСП (*r*; *m*; *p*; 1)**

Задание. Провести опрос группы: «Пошли бы вы на фильм _____(название фильма)?». Для опроса выбрать четыре фильма различных жанров. Профком может оплатить студентам вашего факультета поход в кино. Вам нужно принять решение, основываясь на опросе группы, стоит ли в качестве такого фильма предлагать выбранный вами фильм, если ожидается, что на него должно пойти не менее 30 % студентов факультета, но и не более 60 %. Какова вероятность того, что на фильм пойдет 40 % студентов? Построить закон распределения вероятностей для 40 студентов по четырем фильмам. Найти наивероятнейшее количество человек, которые пойдут на каждый из фильмов. Найти математическое ожидание и среднеквадратическое отклонение, указав наивероятнейший интервал значений количества студентов, которые готовы пойти на каждый из фильмов. Для одного из фильмов построить функцию

распределения случайной величины – количества студентов, которые изъявят желание пойти на фильм.

Тема 12. Основные понятия математической статистики

Лабораторная работа 1. Описательная статистика

Цель: сформировать умение решения задач описательной статистики с помощью табличного редактора Microsoft Excel.

Задание. Тестирование прошли 4 526 человек. Произведено выборочное обследование балов 100 тестируемых, результаты которого приведены в таблице:

125+N	125+N	40+2N	90+N	30+2N	140+N	100+N	50+N	25+2N	145-N
135+N	125-N	85+N	125+N	35+2N	180-N	90+N	85+N	35+2N	190-N
125+N	140+N	200-2N	120+N	190-N	150+N	110+N	60+N	45+2N	160-N
135+N	125-N	45+N	125+N	30+2N	180-N	90+N	90+N	25+2N	170-N
150+N	100+N	40+2N	200-2N	125+N	45+2N	50+N	40+2N	60+N	145-N
180-N	90+N	85+N	45+N	135+N	25+2N	85+N	85+N	90+N	160-N
50+2N	125+N	40+2N	90+N	30+2N	140+N	100+N	50+2N	25+2N	185-2N
175-N	125-N	85+N	145+N	35+2N	180-N	90+N	85+N	35+2N	190-N
115+N	145+N	200-2N	20+3N	190-N	150+N	110+N	60+N	45+2N	165-N
105+N	130-N	45+N	25+3N	30+2N	180-2N	115+N	90+N	25+3N	170-N
150+N	170-N	40+2N	200-2N	125+N	45+2N	50+N	40+2N	60+N	155-N
180-N	95+N	85+N	45+N	135+N	25+2N	85+N	85+N	90+N	160-N

N – дополнительное число, указанное преподавателем.

Используя Microsoft Excel выполнить следующие задания:

1. Составить вариационный ряд распределения.
2. Вычислить относительные частоты.
3. Построить полигон частот.
4. Используя формулы математической статистики вычислить статистические характеристики данного ряда: среднее значение, дисперсию, среднее квадратическое отклонение, моду, медиану, асимметрию, эксцесс.
5. Выполнить пункт 4 с помощью модуля **Описательная статистика** (Сервис→Анализ данных→Описательная статистика), имеющегося в пакете «Статистический анализ» MS Excel.
6. Проанализировать полученные данные.

Тема 13. Основы фрактальной геометрии

Лабораторная работа 1. **Алгоритмы построения фракталов**

Цель: Изучить основные геометрические фракталы. Познакомиться с динамическими фракталам – множествами Жюлиа и Мандельброта**.**

Задание. С помощью модуля построения геометрических фракталов ресурса http://elementy.ru/ выполнить следующие задания:

1. Построить снежинку Коха, выбрав понравившиеся настройки изображения. Определить номер итерации, начиная с которой дальнейшее выполнение алгоритма не вносит существенных различий для зрительного восприятия.

2. Построить дерево Пифагора, выбрав произвольный угол наклона элементов. Определить номер итерации, на которой фигура самопересекается. Найти взаимосвязь величины угла и номера итерации, на которой получается первое самопересечение.

3. Изучить алгоритм построения кривой дракона. Выполнить четыре итерации на листе в клетку. Сравнить результат с полученным с помощью модуля построения геометрических фракталов. Определить номер итерации, на которой фигура самопересекается для произвольного угла наклона элементов кривой. Найти взаимосвязь величины угла и номера итерации, на которой получается первое самопересечение. С помощью опции замощения плоскости убедиться, что кривой дракона можно «замостить плоскость».

4. Построить треугольник Серпинского. Найти площадь треугольника Серпинского, обосновать ответ.

5. Изучить алгоритмы построения множеств Жюлиа и Мандельброта. Изменяя настройки в окне построения множества Мандельброта, изучить границу фрактала. Что можно сказать о множестве Жюлиа и границе множества Мандельброта, изучив их наглядные изображения?

к разделу II
«Основы теории информации и криптологии»

Тема 17. Представление информации

Лабораторная работа 1

Цель: сформировать умения выполнять арифметические и логические операции над числами в двоичной системе, переводить двоичное число в код Грея и наоборот.

Задание 1. Выполните операцию сложения над числами в двоичной системе:

а) $1001011101101110_2 + 1100101001000011_2$,

б) $1101011101101110_2 + 1000111010010010_2$,

в) $1001111101101110_2 + 1111101001000011_2$.

Задание 2. Выполните операцию вычитания над числами в двоичной системе:

а) $1101011101101110_2 - 1100101001000011_2$,

б) $1101011101101110_2 - 1001111010010010_2$,

в) $1111101001000011_2 - 1001111101101110_2$.

Задание 3. Выполните операцию поразрядного умножения над числами в двоичной системе:

а) $1101011101101110_2 \times 1100101001000011_2$,

б) $1101011101101110_2 \times 1000111010010010_2$,

в) $1001111101101110_2 \times 1111101001000011_2$.

Задание 4. Выполните операцию сложения по модулю два (исключающее или) над числами в двоичной системе:

а) $1001011101101110_2 \oplus 1100101001000011_2$,

б) $1101011101101110_2 \oplus 1000111010010010_2$,

в) $1001111101101110_2 \oplus 1111101001000011_2$.

Задание 5. Три десятичных числа представлены в каком-то одном двоично-десятичном коде. Известно, что использовались двоично-десятичные коды с весовыми коэффициентами: 8–4–2–1, 5–1–2–1 и 2–4–2–1. Выясните, какие весовые коэф-

фициенты использовались в двоично-десятичном коде указанных десятичных чисел.

а)	б)	в)
3 → 0011	4 → 0111	4 → 0100
6 → 0110	7 → 1010	9 → 1111
8 → 1000	9 → 1111	8 → 1110

Задание 6. Представьте числа, записанные в коде Грея, в двоичной системе счисления:

а) $10110_{ГР}$, б) $11101_{ГР}$, в) $10100_{ГР}$.

Задание 7. Даны числа, представленные кодом Грея:

а) $101101_{ГР}$, б) $110101_{ГР}$, в) $101100_{ГР}$.

Покажите, как можно преобразовать их в десятичные числа.

Задание 8. Переведите следующие двоичные числа в код Грея:

а) 101101_2, б) 110110_2, в) 101100_2.

Лабораторная работа 2

Цель: сформировать умения переводить числа из одной системы счисления в другую и выполнять арифметические операции в восьмеричной и шестнадцатеричной системах.

Задание 1. Переведите числа из двоичной системы счисления в десятеричную:

101101010101_2, б) 111010011101_2 в) 101000001101_2.

Задание 2. Даны числа, представленные кодом Грея, переведите их в двоичную систему:

а) $101101_{ГР}$, б) $110101_{ГР}$, в) $101100_{ГР}$.

Задание 3. Переведите числа из десятичной системы счисления в двоичную: а) 112385, б) 125042, в) 112016.

Проверку полученного результата осуществите обратным переводом.

Задание 4. Переведите числа из десятичной системы счисления в восьмеричную:

а) 19203813, б) 19250823, в) 91501100.

Задание 5. Переведите числа из десятичной системы счисления в шестнадцатеричную:

а) 29203813, б) 22508234, в) 19150112.

Задание 6. Переведите числа из двоичной системы счисления в восьмеричную:

а) 110011001101101_2, б) 100001101011100_2, в) 101010100001001_2.

Задание 7. Переведите числа из двоичной системы счисления в шестнадцатеричную:

а) 1010011001101101_2, б) 1100001101011100_2, в) 1101010100001001_2.

Задание 8. Переведите числа из восьмеричной системы счисления в шестнадцатеричную:

а) 65134575_8, б) 14327644_8, в) 21156267_8.

Задание 9. Переведите числа из восьмеричной системы счисления в двоичную:

а) 65134575_8, б) 14327644_8, в) 21156267_8.

Задание 10. Переведите числа из восьмеричной системы счисления в десятичную:

а) 65134575_8, б) 14327644_8, в) 21156267_8.

Задание 11. Выполните операцию сложения в восьмеричной системе счисления:

а) $6513_8 + 4575_8$, б) $1432_8 + 7644_8$, в) $2115_8 + 6267_8$.

Задание 12. Выполните операцию сложения в шестнадцатеричной системе счисления:

а) $AD13_{16} + 45C5_{16}$, б) $1FA2_{16} + 7A4E_{16}$, в) $D11C_{16} + 62F7_{16}$.

Задание 13. Выполните операцию умножения в восьмеричной системе счисления:

а) $6513_8 \times 4575_8$, б) $1432_8 \times 7644_8$, в) $2115_8 \times 6267_8$.

Задание 14. Выполните операцию умножения в шестнадцатеричной системе счисления:

а) $A1D_{16} \times 4BC_{16}$, б) $D1A_{16} \times 7CD_{16}$, в) $E11_{16} \times 6F2_{16}$.

Тема 19. Сжатие информации

Лабораторная работа 1

Цель: сформировать умения сжимать информацию на основе методов без потерь данных.

Задание 1. Наберите в системе Pascal ABC текст приведенной программы:

```
program chastota;
var a: string;
k: array[1..100] of integer;
i,j,n,m: integer;
begin
writeln('введите текст');
readln(a);
m:=0;
for i:=1 to length(a) do
begin
a[m+1]:=a[i]; j:=1;
while a[j]<>a[i] do
j:=j+1;
if j=m+1
then
begin m:=m+1; k[m]:=1; end
else k[j]:=k[j]+1;
end;
writeln('количество различных символов',m:3);
for i:=1 to m do
writeln('s[',i:2,']=',a[i],' ',k[i]:2);
end.
```

Выполните эту программу на компьютере для следующих текстов:

а) «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ КУЛЬТУРЫ И ИСКУССТВ»;

б) «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КУЛЬТУРЕ».

Выясните, что делает эта программа:

а) подсчитывает количество различных символов в тексте;

б) формирует текст с различными символами исходного текста;

в) вычисляет частоту символов в тексте;

г) формирует текст с различными символами исходного текста, подсчитывает количество различных символов в тексте и вычисляет частоту символов в тексте.

Задание 2. Составьте программу на языке Pascal ABC, которая будет кодировать текст методом **RLE** (Run-Length Encoding). Этот метод кодирует текст путем учета числа повторений символов в тексте. Идею метода поясняет следующий пример. Пусть требуется закодировать следующую последовательность байтов: 11111111 11111111 11111111 11111111 11111111 11110000 00001111 11000011 10101010 10101010 10101010 10101010 10101010 10101010.

В начале последовательности 5 раз повторяется байт 11111111. Чтобы закодировать эти пять байтов, вначале записывается управляющий байт 10000101, а затем сам повторяющийся байт 11111111. Рассмотрим, как получился этот управляющийся байт: к значению 128 мы прибавили число повторений байта 5, получили $133_{10} = 10000101_2$. Далее идут 3 разных байта. Чтобы их закодировать, записывается управляющий байт 00000011 ($11_2 = 3_{10}$), а затем записываются эти неповторяющиеся байты. Закодированный текст будет выглядеть так: 10000101 11111111 00000011 11110000 00001111 11000011 10000111 10101010. Коэффициент сжатия текста получился 14/8=1,75.

Задание 3. Составьте программу на языке Pascal ABC, которая будет распаковывать текст, закодированный методом RLE.

Схема распаковки может выглядеть следующим образом:

1. Если во входной (сжатой) последовательности встречается управляющий байт с единицей в старшем бите, то следующий за ним байт надо записать в выходную последовательность столько раз, сколько указано в оставшихся 7-ми битах управляющего байта.

2. Если во входной (сжатой) последовательности управляющий байт с нулем в старшем бите, то в выходную последовательность нужно поместить столько следующих за управляющим байтов входной последовательности, сколько указано в оставшихся 7-ми битах управляющего байта.

Литература

1. Алгоритмы и методы сжатия данных / Алгоритмы сжатия [Электронный ресурс]. – Режим доступа: www.compression-pointers.ru/compress_116.html. – Дата доступа: 10.09.2015.

2. Алгоритмы сжатия – Классификация методов сжатия [Электронный ресурс]. – Режим доступа: mf.grsu.by/UchProc/livak/po/comprsite/-theory_classification_01.html. – Дата доступа: 10.09.2015.

3. Ковтанюк, Ю. С. Самоучитель работы на персональном компьютере / Ю. С. Ковтанюк, С. В. Соловьян. – К. : Юниор, 2001. – 560 с.

4. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин [др.]. – М. : Диалог-МИФИ, 2002. – 384 с.

5. Микляев, А. П. Настольная книга пользователя IBM PC / А. П. Микляев. – 3-е изд. – М. : Солон-Р, 2000. – 720 с.

6. Сэломон, Д. Сжатие данных, изображения и звука / Д. Сэломон. – М. : Техносфера, 2004. – 368 с.

Тема 20. Энтропия дискретного источника

Лабораторная работа (4 часа)

Цель: сформировать умения вычислять энтропию и количественную оценку информации.

Задание 1. Вычислите энтропию источника сообщений, если распределение вероятностей появления символов на выходе источника сообщений представлено следующим ансамблем:

$$U = \left| \begin{array}{cccccccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & p_9 & p_{10} \\ 0{,}35 & 0{,}035 & 0{,}07 & 0{,}15 & 0{,}07 & 0{,}07 & 0{,}14 & 0{,}035 & 0{,}01 & 0{,}07 \end{array} \right|.$$

Для вычисления используйте электронную таблицу Microsoft Excel.

Задание 2. Дан алфавит, состоящий из 5 символов. Вероятности появления символов в сообщении равны соответственно: p_1=0,7; p_2=0,2; p_3=0,08; p_4=0,015; p_5=0,005. Определите количество информации в сообщении, состоящем из 20 символов. Выясните, каким будет количество информации в данном сообщении, если все символы будут равновероятны.

Задание 3. Определите энтропию экрана мобильного телефона, если его разрешение 320 x 240, а каждый пиксель может отображать один из 4096 цветов.

Задание 4. Исследования показывают, что количество натуральных блондинов и рыжих год от года уменьшается. Так в 1980 г. вероятность встретить рыжего человека на улице составляла 16 %, натурального блондина – 16 %, русоволосого – 36 %. А в 2010 г. рыжие встречаются с вероятностью 4 %, натуральные блондины – с вероятностью 8 %, русоволосые – с вероятностью 64 %, а брюнеты – с вероятностью 24 %.

Известно, что чем больше энтропия некоторой группы событий, тем тяжелее верно угадать наступление следующего события. Определите, в каком году было тяжелее верно угадать цвет волос случайного человека на улице: в 1980 или в 2010 г.

Задание 5. Опытный индивидуальный предприниматель знает, что 25 % всех его документов составляют налоговые декларации. Для неопытного предпринимателя появление любого типа документа является равновероятным. Вычислите количество информации, которое получат опытный и неопытный предприниматели при получении налоговой декларации.

Задание 6. Определите объем и количество информации в тексте «С давних времен Беларусь называют краем озер», если для его передачи каждый символ заменяют 8 битами. Рассмотрите два случая: равновероятный алфавит и неравновероятный алфавит.

Задание 7. Вероятность появления некоторого события равна p, вероятность того, что это событие не произойдет q=1-p.

Укажите, при каком значении q результат опыта будет обладать максимальной неопределенностью.

Задание 8. Вычислите энтропию системы, состоящую из двух подсистем. Первая подсистема состоит из трех элементов, каждый из которых может находиться в двух состояниях с вероятностями p_1=0,6; p_2=0,4. Вторая подсистема может находиться в трех состояниях с вероятностями p_1=0,1; p_2=0,4; p_3=0,5. Для вычисления используйте электронную таблицу Microsoft Excel.

Задание 9. Дан алфавит мощностью 5. Вычислите количество информации на символ сообщения, составленного из этого алфавита:

а) если символы алфавита встречаются с равными вероятностями;

б) если символы алфавита встречаются в сообщении с вероятностями p_1=0,8; p_2=0,15; p_3=0,03; p_4=0,015; p_5=0,005. Для вычисления используйте электронную таблицу Microsoft Excel.

Задание 10. Вычислите, чему равна неопределенность предпочтения одного из четырех государственных языков жителями Сингапура, если китайский предпочитают 30 % жителей, малайский – 20 %, английский – 40 %, тамильский – 10 %.

Задание 11. Найдите энтропию телевизионного изображения, воспроизводимого телевизионным приемником, если у него разрешающая способность линий не менее 500, число градаций яркости 8, а условное число элементов строки – 700.

Литература

1. Вернер, М. Основы кодирования / М. Вернер. – М. : Техносфера, 2004. – 288 с.

2. Кудряшов, Б. Д. Теория информации : учеб. пособие / Б. Д. Кудряшов. – СПб. : СПбГУ ИТМО, 2010. – 188 с.

3. Могилевская, Н. С. Решение задач по количественной оценке информации и вычислению энтропии. Методические указания по курсу «Теория информации» / Н. С. Могилевская. – Ростов-на-Дону : Издательский центр ДГТУ, 2011. – 12 с.

4. Фурсов, В. А. Лекции по теории информации : учеб. пособие / В. А. Фурсов ; под ред. Н. А. Кузнецова. – Самара : Самар. гос. аэрокосм. ун-т, 2006. – 148 с.

5. Цымбал, В. П. Задачник по теории информации и кодированию / В. П. Цымбал. – К. : Высш. шк., 1976. – 276 с.

Тема 22. Методы шифрования информации

Лабораторная работа 1 (4 часа)

Цель: сформировать умения шифровать информацию с помощью простых методов шифрования.

Задание 1. Зашифруйте текст MICROSOFTOFFICE, используя шифр простой подстановки при k=5.

Задание 2. Отождествите каждую букву текста БЕЗОПАСНОСТЬ ИНФОРМАЦИИ с ее порядковым номером в русском алфавите, начиная с нуля. Будем предполагать, что буква «ё» отсутствует, а пробел имеет номер 32. Для шифрования приведенного текста используйте модулярный шифр $E_a(p)=(ap+k)\text{mod}33$. В качестве ключа возьмите a=7, k=11.

Задание 3. Выполните шифрование текста EASYREPLACEMENT с помощью модулярного шифра $E_7(p)=(7\cdot p+k)\text{mod}26$.

Задание 4. Объясните идею гомофонического шифрования. Составьте таблицу с гомофонией для текста FREQUENCYPROTECTION, используя таблицу частот английских букв в процентах, и зашифруйте этот текст.

Задание 5. Используя приведенный ниже квадрат, выполните биграммное шифрование текста INFORMATIONSECURITY.

Z	Y	M	X	W
U	L	D	V	N
F	T	P	E	O
G	S	B	I	H
C	R	Q	K	A

Задание 6. Используя шифр Вернама, зашифруйте текст UNIVERSITY. В качестве ключа возьмите текст CRYPTOLOGY. Преобразование исходного текста и ключа в двоичную строку

выполните следующим образом. Отождествите каждую букву текста и ключа с ее порядковым номером в английском алфавите. Нумерацию букв начните с цифры 0. Каждую букву представьте пятью двоичными разрядами, соответствующими номеру буквы в алфавите (A → 00000, B → 00001, …, Z → 11000).

Задание 7. Зашифруйте текст БЕЛАРУСЬ методом Вернама. В качестве ключа используйте текст СТОЛИЦА. Для превращения текста в двоичную строку используйте подход, описанный в предыдущей лабораторной работе. При представлении букв Ь и Ъ используйте один числовой код. Буквы русского алфавита при формировании двоичной строки представляйте пятью двоичными разрядами следующим образом:

(А → 00000, Б → 00001, …, Я → 11111).

Литература

1. Герасименко, В. А. Основы защиты информации : учеб. пособие / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

2. Жельников, В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1996. – 335 с.

3. Коробейников, А. Г. Математические основы криптологии : учеб. пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПбГУ ИТМО, 2004. – 106 с.

4. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

Лабораторная работа 2 (4 часа)

Цель: сформировать умения шифровать информацию с помощью биграммной криптосхемы и транспозиционных подходов.

Задание 1. Используйте биграммную криптосхему Хилла для шифрования текста DEFINITION. В качестве ключа возьмите квадратную матрицу

$$M = \begin{bmatrix} 2 & 5 \\ 3 & 3 \end{bmatrix}.$$

Покажите, что данная матрица M является обратимой по модулю 26.

Задание 2. Найдите еще одну квадратную матрицу размерности 2 x 2, которая будет обратимой по модулю 26.

Задание 3. Покажите, что квадратные матрицы A и B размерности 2 x 2 являются обратимыми по модулю 26:

$$A = \begin{bmatrix} 1 & 24 \\ 24 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}.$$

Задание 4. Выясните, является ли квадратная матрица размерности 3 x 3

$$M = \begin{bmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

обратимой по модулю 26.

Задание 5. Распространите метод шифрования биграмм Хилла на шифрование триад символов и зашифруйте текст PASCAL. Для шифрования возьмите квадратную матрицу размерности 3 x 3

$$M = \begin{bmatrix} 1 & 24 & 1 \\ 24 & 5 & 22 \\ 1 & 22 & 6 \end{bmatrix},$$

которая является обратимой по модулю 26.

Задание 6. Дан текст ПОДСТАНОВОЧНОЕ ШИФРОВАНИЕ. Для его шифрования используйте шифр Вижинера. С этой целью текст разбейте на блоки по пять символов в каждом. Пусть последовательность букв k_1, k_2, ..., k_5 слова ШРИФТ является ключом. Отождествите каждую букву исходного текста и ключа с номером буквы в алфавите русского языка так, как это сказано в задании 2 лабораторной работы 1. При шифровании используйте следующие функции $f_i(a) = (a+k_i) \bmod 33$, где a есть буква i-го блока.

Задание 7. Зашифруйте текст PERMUTATIONENCRYPTION, используя два подхода транспозиционного шифрования.

Литература

1. Герасименко, В. А. Основы защиты информации: учеб. пособие / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

2. Жельников, В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1996. – 335 с.

3. Коробейников, А. Г. Математические основы криптологии : учеб. пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПбГУ ИТМО, 2004. – 106 с.

4. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

Тема 25. Генерация простых чисел

Лабораторная работа 1

Цель: сформировать умения находить простые числа**.**

Задание 1. Простым числом называется натуральное число, большее единицы, которое имеет только два делителя: единицу и само это число.

Алгоритм нахождения всех простых чисел до некоторого натурального числа n приписывают древнегреческому математику Эратосфену Киренскому. В честь него алгоритм назвали Решетом Эратосфена. Название алгоритма говорит о принципе его работы, то есть решето подразумевает фильтрацию, в данном случае фильтрацию всех чисел за исключением простых. По мере прохождения списка нужные числа остаются, а ненужные, называемые составными, исключаются.

Для нахождения всех простых чисел не больше заданного числа n, следуя методу Эратосфена, нужно выполнить следующие шаги:

1. Выписать подряд все целые числа от двух до n (2, 3, 4, …, n).

2. Пусть переменная p изначально равна двум – первому простому числу.

3. Зачеркнуть в списке числа от 2p до n, считая шагами по p (это будут числа кратные p: 2p, 3p, 4p, …).

4. Найти первое незачеркнутое число в списке, большее чем p, и присвоить значению переменной p это число.

5. Повторять шаги 3 и 4, пока возможно.

Теперь все незачеркнутые числа в списке – это все простые числа от 2 до n.

Выполните данный алгоритм в электронной таблице Microsoft Excel при значении n, равном 100.

Задание 2. Наберите в системе Pascal ABC текст приведенной программы:

```
Program Prime;
var i,n: longint;
f: boolean;
begin
writeln('Введите n>3'); readln(n);
f:=true;
for i := 2 to round(sqrt(n)) do
if n mod i=0 then begin
f := false; break; end;
if f then writeln('простое число')
else writeln('непростое число');
end.
```

Выполните эту программу несколько раз при разных значениях n и выясните, что она делает:

а) находит максимальное простое число, не превосходящее n;

б) проверяет, является ли число n простым;

в) находит наибольший делитель числа n;

г) находит минимальное простое число, превосходящее n.

Задание 3. Наберите в системе Pascal ABC текст приведенной программы:

```
Program Chisla;
Var m,n,i,k: longint;
flag: boolean;
begin
```

```
writeln('Введите m>3'); readln(m);
write(' 2 3');
k := 2; n := 5;
while n <= m do begin
flag := true;
for i := 2 to round(sqrt(n)) do
if n mod i = 0 then begin flag := false;
break;
end;
if flag then begin
write(n:7); k := k+1;
if k mod 10 = 0 then writeln;
end;
n := n+2;
end;
writeln; writeln('Количество = ',k);
end.
```

Выполните эту программу при значениях m, равных 50 и 60, и выясните, что она делает:

а) находит все простые числа, не превосходящие m;

б) подсчитывает количество простых чисел, не превосходящих m;

в) находит все простые числа, не превосходящие m, и подсчитывает количество простых чисел, не превосходящих m;

г) находит максимальное простое число, не превосходящее m.

Задание 4. Измените программу задания 2 так, чтобы она вводила число m и выводила на экран компьютера максимальное простое число n, не превосходящее m.

Литература

1. Дагене, В. А. 100 задач по программированию / В. А. Дагене, Г. К. Григас, А. Ф. Аугутис. – М. : Просвещение, 1993. – 255 с.

2. Фаронов, В. В. Турбо Паскаль 7.0. Начальный курс : учеб. пособие / В. В. Фаронов. – М. : Нолидж, 1999. – 616 с.

Лабораторная работа 2

Цель: сформировать умения находить простые числа**.**

Задание 1. Два нечетных простых числа, разнящихся на два, называются близнецами. Близнецами являются, например, числа 5 и 7, 11 и 13, 17 и 19 и т. д. В начале натурального ряда такие пары чисел встречаются достаточно часто, но, по мере продвижения по натуральному ряду чисел, их становится все меньше и меньше.

Требуется написать программу, которая будет находить все числа – близнецы в интервале [2; 1000] и подсчитывать количество пар чисел близнецов.

Для написания этой программы используйте программу задания 2. В нее добавьте две переменные для хранения двух «последних» простых чисел и проверяйте условие наличия близнецов – их разность должна быть равна двум.

Задание 2. Запишите в электронной таблице Microsoft Excel формулу, которая будет проверять, является ли натуральное число p простым. Для проверки числа используйте следующее утверждение:

Теорема Вильсона. Натуральное число $p > 1$ является простым тогда и только тогда, когда $(p – 1)! + 1$ делится на p.

Определите максимальное натуральное число p, для которого общий числовой формат данных в Microsoft Excel позволит правильно организовать вычисления по записанной формуле.

Задание 3. Составьте программу на языке Pascal ABC, которая будет формировать ряд простых чисел. Воспользуйтесь алгоритмом, который разработал индийский математик С. П. Сундарам в 40-х гг. XX в.

Идея алгоритма состоит в следующем. Из натурального числового ряда исключаются все значения вида

$$z = i + j + 2ij,$$

где $i = 1, 2, 3, \ldots, n$; $j = 1, 2, 3, \ldots, i$, а оставшиеся числа умножаются 2 и к результату прибавляется 1.

Литература

1. Дагене, В. А. 100 задач по программированию / В. А. Дагене, Г. К. Григас, А. Ф. Аугутис. – М. : Просвещение, 1993. – 255 с.

2. Фаронов, В. В. Турбо Паскаль 7.0. Начальный курс : учеб. пособие / В. В. Фаронов. – М. : Нолидж, 1999. – 616 с.

Тема 26. Алгоритмы хеширования

Лабораторная работа (4 часа)

Цель: сформировать умения выполнять операции хеширования, используемые в базах данных.

Задание 1. Преобразуйте следующие ключи записей в четырехзначные относительные адреса пакета методом средних квадратов: а) 611450, б) 437118, в) 961102.

Для вычислений используйте электронную таблицу Microsoft Excel.

Задание 2. В электронной таблице Microsoft Excel найдите все возможные делители для хеширования методом деления в диапазоне 9971÷9999. Делителем в указанном методе может быть либо простое число, либо число, не имеющее небольших сомножителей. Преобразуйте методом деления восьмизначные ключи записей в четырехзначные относительные адреса:

а) 31465105, б) 24371180, в) 56910217.

В качестве делителя возьмите наибольшее простое число из приведенного диапазона.

Задание 3. Методом сдвига разрядов преобразуйте в четырехзначные относительные адреса следующие восьмизначные ключи записей:

а) 53146510, б) 80243711, в) 91021756.

Задание 4. Используя метод складывания, преобразуйте в трехзначные относительные адреса следующие семизначные ключи записей:

а) 4316510, б) 7243118, в) 1569021.

Задание 5. Для получения четырехзначных относительных адресов из шестизначных ключей записей

а) 145610, б) 743118, в) 910261

воспользуйтесь методом преобразования системы счисления. В качестве основания системы счисления возьмите число 13.

Задание 6. Даны семизначные ключи записей:

а) 4316510, б) 7243118, в) 1569021.

Преобразуйте их в трехзначные относительные адреса методом Лина. При преобразовании возьмите следующие параметры: q=313, m=2.

Задание 7. Получите четырехзначные относительные адреса пакетов методом деления полиномов для следующих шестизначных ключей записей:

а) 145610, б) 743118, в) 910261.

Литература

1. Герасименко, В. А. Основы защиты информации : учеб. пособие / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

2. Жельников, В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1996. – 335 с.

3. Коробейников, А. Г. Математические основы криптологии : учеб. пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПбГУ ИТМО, 2004. – 106 с.

4. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

5. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы / Д. Кнут. – М. : Вильямс, 2007. – 832 с.

6. Мартин, Дж. Организация баз данных в вычислительных системах / Дж. Мартин. – М. : Мир, 1978. – 616 с.

к разделу III
«Медиакультура специалиста»

Тема 31. Коммуникационное пространство. Сетевые сообщества

Лабораторная работа 1. **Использование блог-технологий в профессиональной деятельности культуролога**

Цели:

– углубить и систематизировать имеющиеся знания о создании и ведении блога, сформировать умения применения блог-технологий в профессиональной деятельности культуролога;

– сформировать умения использования Интернета для составления аннотированного списка блогов профессиональной тематики.

Задание для выполнения

Создать блог, в котором разместить отчеты о выполнении каждой из приведенных задач

Выполнение работы

Задача 1.

Создать собственный «блог-портфолио» на любой платформе. Обязательные структурные элементы блог-портфолио:

– приветствие (фотография или видеоколлаж, несколько слов от автора блог-портфолио в свободной форме, исполненных в любом жанре);

– резюме (профессиональное резюме для потенциальных работодателей);

– личное (жизненные принципы, автобиография, фотоальбомы);

– достижения (образовательные, профессиональные, личные);

– ресурсы (полезные ссылки);

– контакты (контактная информация, полнота которой определяется самостоятельно пользователем).

Пример алгоритма создания блога на Blogger http://www.blogger.com :

1. Создать собственный аккаунт на Google (или использовать имеющийся).

2. Выбрать название блога и его URL-адрес;

3. Определить и отредактировать шаблон для блога.

Задача 2.

1. В Интернете найдите материалы о классификации блогов по различным критериям. Включите найденные классификации блогов в отчет с указанием URL-адреса источника.

2. Выполните поиск действующих блогов социокультурной направленности.

3. Составьте аннотированное описание каждого из найденных блогов.

4. Проанализируйте блоги социокультурной направленности по возможности их использования в профессиональной деятельности культуролога (результаты представьте в виде таблицы).

Задача 3. Оцените целесообразность использования в профессиональном блоге культуролога виджетов. Установите один из них на созданный блог.

Задача 4. Оформите отчет и разместите его в разделе ресурсы созданного блога.

Задача 5. Оцените ваши личные успехи при выполнении данной работы и предъявите результаты преподавателю.

Литература

1. Волохонский, В. Л. Психологические механизмы и основания классификации блогов. Личность и межличностное взаимодействие в сети Internet. Блоги: новая реальность / В. Л. Волохонский ; под ред. Ю. Е. Зайцевой, М. М. Соколова. – СПб. : СПбГУ, 2006. – 265 с.

2. Кветна, И. Маркетинг в социальных сетях – ставка на доверие / И. Кветна // Маркетинг и реклама. – 2009. – № 6.

3. Сафонова, Т. В. Порядок интеракции в сетевых дневниках: альтернативная экономика сообщений. Личность и межличностное взаимодействие в сети Internet. Блоги: новая реальность : сб. ст. / Т. В. Сафонова; под ред. В. Л. Волохонского, Ю. Е. Зайцевой, М. М. Соколова. – СПб. : СПбГУ, 2006. – С. 55–75.

4. Ющук, Е. Блог. Создать и раскрутить / Е. Ющук. – М. : Вершина, 2007. – 168 с.

Вопросы для самоконтроля

1. По каким критериям можно классифицировать блоги? Приведите пример.
2. Назовите основные направления использования блогов в профессиональной деятельности культуролога.
3. Опишите технологии создания блогов. Какие блог-платформы вы знаете?
4. Каковы функциональные возможности блога? В каких случаях создание блога обоснованнее, чем персонального сайта? Аргументируйте свое мнение.
5. Приведите примеры использования блогов в профессиональной деятельности культуролога.

Тема 33. Компьютерные среды для работы с медиаприложениями

Лабораторная работа 1. Организация совместной коммуникационной деятельности на основе сетевых сервисов

Цели:

– углубить и систематизировать имеющиеся знания, сформировать навыки использования сетевых сервисов для организации совместной коммуникационной деятельности;

– сформировать умения использовать Интернет для составления аннотированного списка информационных ресурсов, позволяющих организовать совместную коммуникационную деятельность в электронной медиасреде.

Задание для выполнения

Изучите прикладное программное обеспечение для организации совместной коммуникационной деятельности. Организуйте работу по выполнению задач 2–6

Выполнение работы

Задача 1.

Изучите и проанализируйте прикладное программное обеспечение для организации совместной работы. Заполните таблицу 3.1.

Таблица 3.1

Прикладное программное обеспечение для организации совместной работы

Пример совместной коммуникационной деятельности культуролога	Название прикладного программного обеспечения	Основные функциональные возможности	Источник (URL-адрес)
Удаленное редактирование и форматирование текстов			
Удаленное редактирование и форматирование изображений			
Удаленное редактирование и форматирование презентаций			
Удаленное интервьюирование			
Ведение заметок			
Ведение календаря			
Удаленное рисование			
Создание блога			
Создание вики			
Создание социальной сети			
Хранение файлов в сети			

Примечание. Для заполнения таблицы используйте http:// cooltoolsforschools.wikispaces.com – ресурс, описывающий прикладное программное обеспечение для организации работы в сети на примере образовательных технологий.

Задача 2.

1. Разбейтесь на группы по 2–3 человека.

2. Создайте сайт проекта с помощью сервиса Google. В параметрах сайта установите возможность просмотра сайта любым пользователем.

3. На страницах сайта разместите следующую информацию:

– выберите «Объект проекта», которому вы хотите посвятить свой проект. «Объект проекта» – событие, человек, произведение белорусской социокультурной среды и т. д.;

– обоснуйте важность объекта проекта;

– на одной из страниц разместите визитную карточку группы, укажите название группы, состав, желательно вашу фотографию в процессе работы.

Помните о ключевых понятиях анализа медиатекста, которые необходимо определить перед его созданием.

Задача 3.

С помощью документов Google создайте Форму. Разработайте с помощью этой Формы анкету для проведения сетевого опроса об информированности аудитории об объекте вашего проекта (насколько популярен ваш объект, что о нем знают окружающие) и т. д. Анкета должна содержать не менее 6 вопросов. Респондентов должно быть не менее 50 человек. Проанализируйте результаты и сделайте выводы. Описание анкеты, ссылка на нее и анализ результатов представьте на отдельной странице вашего сайта Google. Результаты анкеты сделайте доступными для преподавателя (после создания анкеты с помощью кнопки «Открыть доступ» получите электронный адрес преподавателя и внесите его в список доступа).

Задача 4.

Для рекламы «Объект проекта» создайте изображения сувенирной продукции:

– эмблема (изображение, созданное в технике коллажа);

– имитация сувенирной продукции – изображение сувениров с эмблемой.

Все рекламные материалы должны быть сделаны самостоятельно: созданы в графических программах. Все изображения помещайте на отдельную страницу сайта Google. Добавьте описание изображений и краткое описание процесса создания.

Помните об основных категориях медиатекста, которые необходимо определить перед его созданием.

Примечание. На страницу сайта Google через меню «Вставить» можно добавить фотографии из Picasa Google. Использовать этот сервис необязательно.

Задача 5.

Инсценируйте интервью с «объектом проекта» или людьми, которые могут о нем рассказать. Запишите его одним из двух способов:

– используя видеокамеру: выложите ролик в сети Интернет и сделайте доступным для просмотра;

– используя любой социальный сервис.

Текстовое описание интервью, основные его моменты и выводы, ссылка на записанное видеоинтервью должны быть представлены на отдельной странице сайта Google.

Задача 6.

Оформите отчет. Оцените ваши личные успехи при выполнении данной работы и предъявите результаты преподавателю.

Литература

1. Балуев, Д. Секреты приложений Google / Д. Балуев. – М. : Альпина Паблишерз, 2010. – 288 с.

2. Левин, Джон. Интернет для «чайников» / Джон Левин, Маргарет Левин-Янг. – М. : Диалектика : Вильямс, 2010. – 352 с.

3. http://cooltoolsforschools.wikispaces.com – ресурс, описывающий прикладное программное обеспечение для организации работы в сети на примере образовательных технологий.

Вопросы для самоконтроля

1. Что такое коммуникация? Каковы ее основные формы и виды?

2. Какие сетевые сервисы для организации совместной коммуникационной деятельности вы знаете?

3. Для аудитории какой возрастной группы и уровня подготовки культуролог может предложить ведение совместного сетевого проекта (конкурс работ, фотовыставки и т. д.)?

4. Аргументируйте необходимость использования сетевых сервисов для организации совместной коммуникационной деятельности в профессиональной деятельности культуролога.

5. Приведите примеры использования сетевых сервисов в профессиональной деятельности культуролога.

Тема 34. Программные средства создания, редактирования и управления медиатекстами

Лабораторная работа 1. Использование видео и анимации в профессиональной деятельности культуролога

Цели:

– углубить и систематизировать знания, сформировать умения создания и использования видео и анимации в профессиональной деятельности культуролога;

– сформировать умения использования ресурсов доступа к базам данных медиатекстов, содержащих видео, анимацию и материалы по их созданию.

Задание для выполнения

Проанализируйте возможности использования видео и анимационных медиатекстов в профессиональной деятельности культуролога

Выполнение работы

Задача 1.

1. Сравните GIF- и FLASH-анимацию (табл. 3.2). По результатам анализа сделайте вывод о возможности использования различных видов анимации в профессиональной деятельности культуролога.

Таблица 3.2

Анализ GIF- и FLASH-анимации

	GIF-анимация	FLASH-анимация
Применение компьютерной графики (растровая, векторная)		
Аудиовозможности		
Возможности цветопередачи		
Примеры применения в профессиональной деятельности культуролога		

2. Используя программное обеспечение для создания GIF- или FLASH-анимации создайте рекламный баннер любого мероприятия в сфере белорусской культуры.

Создание GIF-анимации с помощью программы Adobe Photoshop

GIF-анимация складывается из набора кадров (в растровом формате), размещенном в одном файле GIF (Graphics Interchange Format). Для создания анимации в программе Adobe Photoshop служит палитра *Animation (Анимация)*. С ее помощью возможно создание анимационного ряда (последовательность кадров) изображений с целью последующего сохранения его в файле формата GIF.

Алгоритм создание GIF-анимации с помощью программы Adobe Photoshop:

1. Подготовьте изображения для анимации. Для создания набора изображений для анимации необходимо создать изображение с несколькими слоями, которые и будут кадрами для будущей анимации. После того как мы создали каждый кадр анимации в отдельном слое, приступим непосредственно к анимированию изображения.

2. Создание GIF-анимации с помощью палитры *Animation*:

2.1. Выберите команду меню *Windows – Animation (Окно – Анимация)*. Единственный кадр, расположенный на палитре *Animation (Анимация)*, отображает видимые части изображения, определяемые состоянием слоев на палитре *Layers (Слои)*

2.2. Для создания нового кадра на палитре *Animation (Анимация)* щелкните на пиктограмме *Duplicate Current Frame (Создание копии выделенных кадров)*.

1, 2, 4 – выбор кадров;

3 – воспроизведение анимации;

5 – создание промежуточных кадров;

6 – создание копии выделенных кадров;

7 – удаление выделенных кадров;

8 – преобразование в анимации по временной шкале.

2.3. На новом созданном кадре сделайте невидимым слой с предыдущим кадром, а видимым тот слой, который будет соответствовать этому кадру.

2.4. Повторите последовательность действий, описанных в п. 2.3 необходимое количество раз.

2.5. Чтобы сгладить переходы между кадрами, можно использовать команду *Tween (Создание промежуточных кадров*), которая находится в раскрывающемся меню палитры *Animation (Анимация)* или щелкнуть на соответствующем значке внизу палитры. Эта функция автоматически добавляет размытие, чтобы сгладить переходы между кадрами.

2.6. Установите число повторов воспроизведения анимации 

.

2.7. Сохранение анимации. После того как вы достигли желаемого результата, сохраните этот анимационный ряд в формате GIF, выбрав *File – Save as (Файл – Сохранить как)*. Для просмотра анимации в web-браузере перед сохранением файла выполните *File – Save for Web (Файл – Сохранить для веб)*. В открывшемся окне щелкните на *Preview in Default Browser (Просмотр)* внизу окна – ваша анимация будет показана в окне браузера, который используется по умолчанию в вашей системе.

Создание FLASH-анимации с помощью программы Adobe Flash

Символ – это своеобразный шаблон объекта с определенным набором свойств, который создается один раз и хранится в библиотеке текущего документа, а затем может использоваться в документах необходимое количество раз.

Экземпляр – копия символа, расположенная в рабочей области или вложенная в другой символ. Экземпляр может отличаться от родительского символа цветом, размером и функ-

циональностью. При редактировании символа обновляются все его экземпляры, но при применении к нему эффектов изменится только используемый экземпляр.

ТИПЫ СИМВОЛОВ

Графические символы предназначены для создания статических изображений и повторно используемых фрагментов анимации, связанных с основной временной шкалой. В последовательности анимации графического символа интерактивные элементы управления и звуки работать не будут.

Кнопки-символы позволяют создавать интерактивные кнопки, которые реагируют на щелчки кнопкой мыши, перемещение указателя или другие действия.

Символы фрагмента ролика позволяют создавать повторно используемые фрагменты анимации. Могут содержать интерактивные элементы управления, звуки и даже другие экземпляры фрагмента ролика.

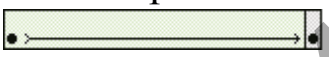
ТИПЫ АНИМАЦИИ

Анимация движения состоит из одного целевого объекта, использующегося во всем диапазоне анимации. Используются ключевые кадры свойств, а не ключевые кадры. Анимация движения преобразует объект во фрагмент ролика. В диапазоне анимации движения не допускается использование кадровых сценариев. При анимации движения к одному переходу между двумя цветами можно применять только один цветовой эффект. Используется для анимации трехмерных объектов. На временной шкале выглядит следующим образом: – черная точка в первом кадре означает, что диапазону анимации присвоен целевой объект. Черные ромбы указывают последний кадр и другие ключевые кадры свойств.

Классическая анимация использует ключевые кадры. Ключевые кадры – это кадры, в которых появляются новые экземпляры объектов. Классическая анимация движения преобразует объект в графический символ. Допускает использование кадровых сценариев. Используется для эффекта перехода, на-

пример тонирования или альфа-прозрачности. На временной шкале выглядит следующим образом:  – черная точка с черной стрелкой на голубом фоне – это классическая анимация движения.  – пунктирная линия означает, что классическая анимация движения прервана или неполна, например пропущен последний ключевой кадр.

Покадровая анимация. Для каждого кадра временной шкалы указываются различные объекты. Применяется при создании комплексной анимации, где графические элементы каждого кадра должны быть различны. На временной шкале выглядят следующим образом:  – черные точки на голубом фоне – ключевые кадры.

Анимация формы создается с помощью включения (вставки) промежуточных кадров между указанными. Одна форма перетекает в другую. На временной шкале это выглядит следующим образом:  – черная точка с черной стрелкой на светло-зеленом фоне на начальном кадре означает анимацию формы.

Позы обратной кинематики позволяют растягивать и поворачивать объекты фигур, а также соединять группы экземпляров символов для их одновременного перемещения. Применяется при передаче естественности движения. На временной шкале выглядит таким образом:  – диапазон кадров с зеленым фоном указывает на использование слоя позы обратной кинематики. Слои позы содержат каркасы и позы. Все позы отмечены на временной шкале черными ромбами.

АЛГОРИТМ СОЗДАНИЯ АНИМАЦИИ ДВИЖЕНИЯ

Примечание. Анимация применяется к экземплярам символов и текстовым полям.

1. Создайте новый файл.
2. Создайте новый символ фрагмента ролика.
3. Отобразите библиотеку фильма.
4. Создайте первый кадр анимации:

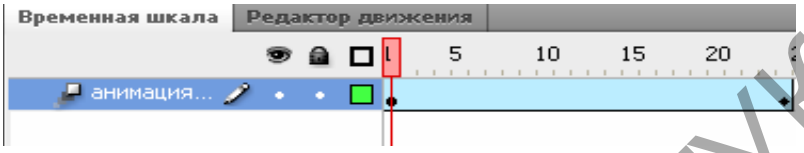
– выделите первый кадр слоя;

– перетащите экземпляр символа из библиотеки в правый верхний угол сцены.

5. Выберите *Insert – Motion Tween (Вставка – Анимация движения)*.

6. Переместите экземпляр символа в левый нижний угол сцены на монтажном столе.

7. Просмотрите анимацию, нажав *Enter*. На рисунке представлена временная шкала анимации движения.



8. Сохраните файл.

АЛГОРИТМ СОЗДАНИЯ КЛАССИЧЕСКОЙ АНИМАЦИИ ДВИЖЕНИЯ

1. Создайте новый файл.

2. Создайте новый графический символ.

3. Отобразите библиотеку фильма.

4. Создайте первый кадр анимации:

– выделите первый кадр слоя;

– перетащите экземпляр символа из библиотеки в правый верхний угол сцены.

5. Создайте последний кадр анимации:

– выделите 20-й кадр (последний кадр будущей анимации);

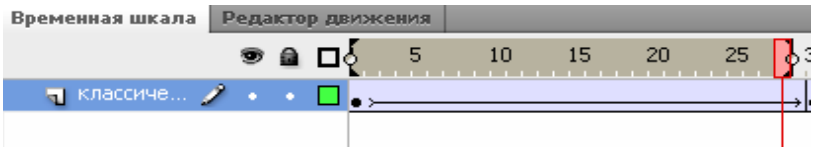
– сделайте его ключевым: *Insert – Timeline – Keyframe (Вставка – Временная шкала – Ключевой кадр)* или клавиша *F6*;

– переместите экземпляр в левый нижний угол сцены.

6. Выделите первый кадр *Insert – Classic Tween (Вставка – Классическая анимация движения)*. Выполните кадрирование

.

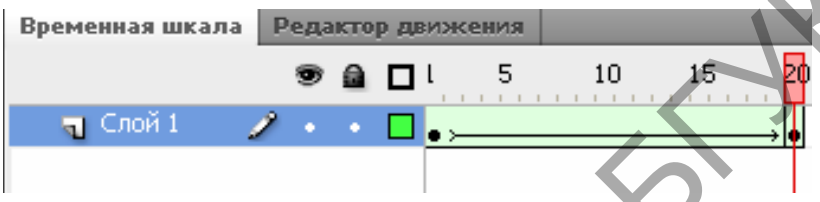
7. Просмотрите анимацию, нажав *Enter*. На рисунке представлена временная шкала классической анимации движения.



8. Сохраните файл.

АЛГОРИТМ СОЗДАНИЯ АНИМАЦИИ ФОРМЫ

Аналогичен алгоритму создания классической анимации в пункте 6 *Insert – Shape Tween (Вставка – Анимация формы)*. На рисунке представлена временная шкала анимации формы.



АЛГОРИТМ СОЗДАНИЯ ПОКАДРОВОЙ АНИМАЦИИ

1. Создайте новый файл.
2. Создайте первый кадр анимации:

– выделите первый кадр слоя;

– создайте в нем объект.

3. Создайте второй кадр анимации:

– выделите второй кадр, сделайте его ключевым: *Insert – Timeline – Keyframe (Вставка – Временная шкала – Ключевой кадр)* или клавиша *F6*;

– переместите объект в центр сцены или вставьте другой объект (на временной шкале появится второй ключевой кадр).

4. Сделайте еще три аналогичных кадра (шаг 5: третий, четвертый и пятый кадр).

5. Просмотрите анимацию, нажав *Enter*. На рисунке представлена временная шкала покадровой анимации.

6. Сохраните файл.

АЛГОРИТМ СОЗДАНИЯ ПОЗ ОБРАТНОЙ КИНЕМАТИКИ (ДОБАВЛЕНИЕ КАРКАСА К ВНУТРЕННИМ СОСТАВЛЯЮЩИМ ОБЪЕКТА ФИГУРЫ)

1. Создайте новый файл.

Примечание. Использование обратной кинематики возможно при использовании ActionScript 3.0.

2. Создайте новую фигуру на монтажном столе.

3. Создайте первый кадр анимации:

– добавьте кости к фигуре при помощи инструмента *Кость (Bone),* фигура и связанный с ней каркас переместятся на новый слой временной шкалы – слой позы.

Примечание. Каждый слой позы может содержать только один каркас и связанные с ним экземпляры или фигуру.

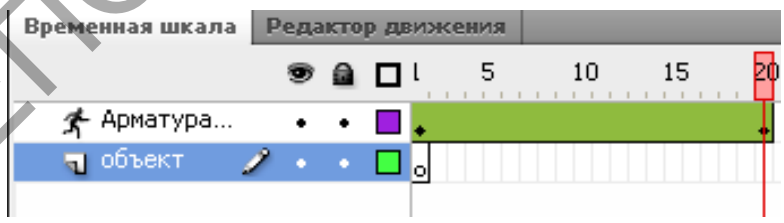
– используя инструмент *Связывание (Link),* откорректируйте взаимосвязи между отдельными костями и точками управления объектов фигуры.

4. Создайте второй кадр анимации:

– на слое позы щелкните на 20 кадре и выберите пункт меню *Добавить позу (Keyframe) (Insert – Timeline – Keyframe (Вставка – Временная шкала – Ключевой кадр))*.

– в 20 кадре измените конфигурацию каркаса с помощью инструмента *Выделение (Arrow Tool).*

5. Просмотрите анимацию, нажав *Enter*. На рисунке представлена временная шкала поз обратной кинематики.



6. Сохраните файл.

Создание видео с помощью программы Adobe After Effects

1. Создайте новый проект (*File – New – New Project*). Настройте свойства проекта в дополнительном меню окна проект (*Project – Project Settings*).

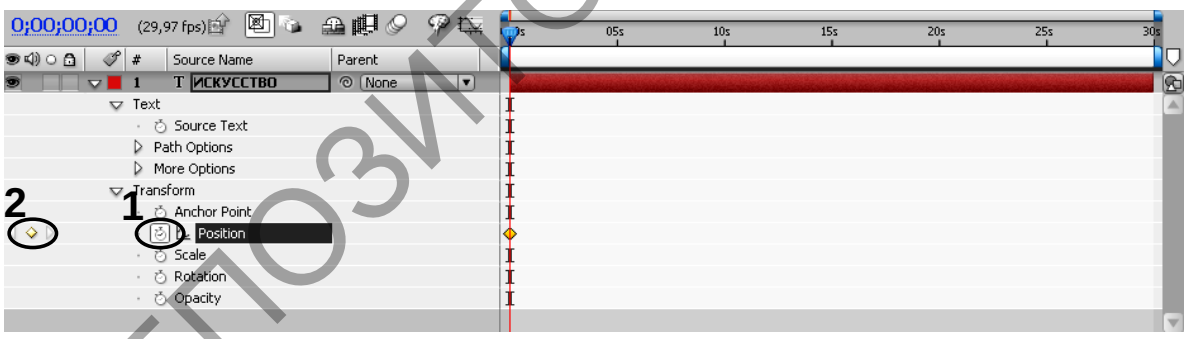
2. Импортируйте два файла: изображение и видео (*File – Import – File*).

3. Создайте новую композицию (*Composition – New Composition*). Настройте длительность композиции в окне свойства композиции (*Composition – Composition Settings*). Установите длительность 30 секунд, как представлено на рисунке.

4. В окне композиции введите текст и разместите его в правом верхнем углу.

5. Анимируйте текст:

– в окне временной шкалы на текстовом слое откройте вкладку *Transform – Position* и включите режим редактирования  , на рисунке обозначенный как кнопка 1.

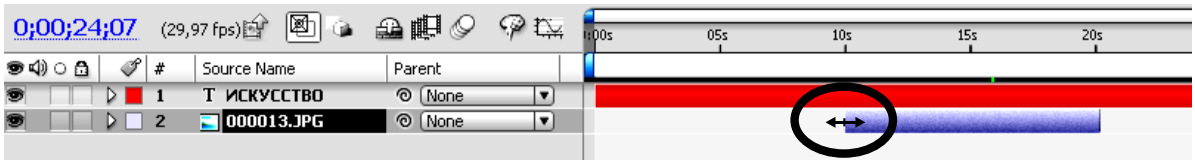


– переместите временной индикатор на 10 секунд и добавьте ключевой кадр  , на рисунке обозначенный как кнопка 2.

– в ключевом кадре переместите текст в левый нижний угол.

6. С помощью окна *Time Controls* просмотрите анимацию движения.

7. Переместите файл с изображением из окна *Проект* на временную шкалу. Разместите его на временной шкале с 10 до 20 секунды, используя преобразование, как показано на рисунке.



8. Переместите видеофайл из окна *Проект* на временную шкалу. Разместите его на временной шкале с 10 до 20 секунды.

9. Аналогично разместите видеофайл с 20 до 30 секунды.

10. Просмотрите весь проект с помощью окна *Time Controls*.

11. Сохраните проект (*File – Save*) и экспортируйте проект в SWF-формат (*File – Export – Adobe Flash (swf)*).

Создание видео с помощью программы Adobe Premier

1. Создайте новый проект (*File – New – Project*). Свойства проекта определите в предлагаемых окнах настроек: предложенные по умолчанию (*Load Preset*), собственные (*Custom Settings*).

Примечание. Для телевизионных программ основные характеристики видео будут следующими:

– разрешение от 720 x 480 пикселей и выше;

– частота кадров в секунду – 25 (в системе PAL) или 30 (в системе NTSC);

– глубина цвета – 32 бит.

Мультимедийные продукты, содержащие видео, имеют обычно такие характеристики:

– разрешение 360 x 240 пикселей;

– частота кадров – 15 (в секунду);

– глубина цвета – 16 бит.

Для размещения видеофайлов в Интернете необходимо, чтобы они были небольшого размера, поэтому часто приходится жертвовать качеством картинки. Обычные параметры видеоизображений в Интернете таковы:

– разрешение 160 x 120 или 180 x 120 пикселей;

– частота кадров – 10 (в секунду);

– глубина цвета – 8 бит.

2. Импортируйте три файла: изображение, звук и видео (*File – Import*).

Примечание. Для разъединения звука и видео выделяют требуемые файлы, выбирают меню *Клип (Clip)* и команду *Разъединить (Unlink)*.

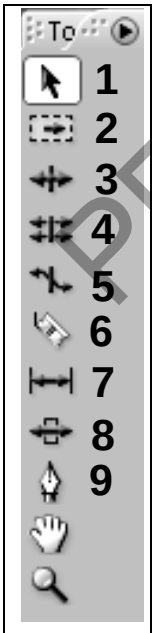
3. Создайте две текстовые надписи (одна – название, вторая – исполнители). Откройте окна для работы с надписями (*Window – Title*).

Текстовые надписи автоматически появятся в окне *Проект (Project)*.

4. Переместите файл с первой надписью из окна *Проект (Project)* на временную шкалу (*Timeline*). Поместите его на временной шкале с 1 до 10 секунды. Вторую надпись разместите с 30 до 40 секунды.

5. Переместите видеофайл из окна *Проект (Project)* на временную шкалу. Поместите его на временной шкале с 10 до 20 секунды.

Примечание. При необходимости используйте панель с инструментами монтажа рисунка.

	**1**	Инструмент выбора (Selection Tool) позволяет выделить один клип, трек, сделать активным какое-либо из окон
	2	Инструмент выбора трека (Track Select Tool) позволяет выбрать все клипы на дорожке, которые расположены правее текущего положения курсора
	3	Инструмент монтажа со смещением (Ripple Edit Tool). В этом случае при вставке или удалении клипа происходит изменение длительности всей последовательности в большую или меньшую сторону на величину, равную длительности помещенного или удаленного клипа
	4	Инструмент монтажа с наложением (Rolling Edit Tool). При вставке клипа методом наложения общая длительность всей последовательности сохраняется, однако изменяется граница между клипами за счет наложения одного клипа на другой

	5	Инструмент масштабирования клипов (Rate Stretch Tool) изменяет длительность клипов за счет скорости воспроизведения. Следует осторожно применять этот инструмент для редактирования, чтобы избежать потери качества исходного материала
	6	Инструмент разрезания клипов (Razor Tool) делит один клип на два
	7	Инструмент монтажа с прокруткой (Slip Tool) изменяет входной и выходной маркеры редактируемого клипа. Длительность самого клипа при этом не изменяется
	8	Инструмент монтажа с совмещением (Slide Tool) изменяет входной и выходной маркеры за счет наложения на соседние клипы
	9	Инструмент «Перо» (Pen Tool)

6. Аналогично поместите изображение с 20 до 30 секунды.

7. Переместите звук из окна Проект (Project) на временную шкалу. Поместите его на временной шкале с 20 до 40 секунды (параллельно изображению и титрам)

Примечание. При необходимости создайте переходы (эффекты, которые применяются при смене одного изображения (или звукового фрагмента) на другой). Используйте окно Эффекты *(Effects)* 

.

Изменить длительность перехода можно двумя способами:

– установить требуемое значение *длительности перехода (Duration)* с клавиатуры во вкладке *Управление эффектом (Effect Controls*).

– навести мышку на конец или начало перехода в окне *Монтажный стол (Timeline)*; курсор приобретет соответствующую форму. Потянуть вправо (для увеличения) или влево (для уменьшения) за границу перехода для изменения его длительности.

8. Просмотрите весь проект с помощью окна *Программа (Program)*.

9. Сохраните проект (*File – Save)* и экспортируйте проект в SWF-формат *(File – Export – Movie)*.

Примечание. Проекты имеют расширение *.prproj. В проекте хранятся **ссылки** на исходные файлы. Помните об этом при переносе файла проекта с одного компьютера на другой.

Литература

1. Кирьянов, Д. В. Самоучитель Adobe After Effects CS3 / Д. Кирьянов, Е. Кирьянова. – СПб. : БХВ-Петербург, 2008. – 364 с.

2. Пташинский, В. С. Видеоэффекты и анимация в Adobe After Effects CS3 / В. Пташинский. – СПб. : Питер, 2008. – 256 с.

3. Столяров, А. М. Adobe Premiere CS3/CS4 / А. М. Столяров. – М. : Эксмо, 2009. – 656 с.

Вопросы для самоконтроля

1. Назовите основные характеристики, которые необходимо определить при подготовке анимационного медиатекста для последующего размещения в Интернете.

2. Проанализируйте особенности GIF- и FLASH-анимации. Обоснуйте свой выбор для выполнения задания 1.2.

3. Какое аппаратное и программное обеспечение вам понадобится для создания и редактирования анимационных медиатекстов?

4. Какое аппаратное и программное обеспечение вам понадобится для создания и редактирования видеомедиатекстов?

5. Приведите примеры использования видео и анимационных медиатекстов в профессиональной деятельности культуролога.

МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

к разделу I
«Прикладная математика»

Тема 2. Матрицы

Практическая работа 1. **Операции над матрицами. Определить матрицы**

Цель: научиться выполнять основные действия над матрицами.

Задача 1. Найти линейную комбинацию матриц A_{3x3} и B_{3x3}: ($aA + bB$). Транспонировать полученный результат. Матрицы A_{3x3} и B_{3x3} составляются произвольно из чисел от -15 до 15. Параметры a и b принимают значения -5 до 5.

Задача 2. Записать матрицу A размерности 4x4 и вектор B размерности 4x1 произвольно. Умножить матрицу A на вектор B.

Задача 3. Найти определитель матрицы A_{3x3} из задачи 1 разложением по строке либо столбцу.

Задача 4. Проверить результаты задач 1–3 с помощью онлайн калькулятора OnlineMschool на мобильном устройстве.

Тема 3. Системы линейных уравнений

Практическая работа 1. **Метод Гаусса решения систем линейных уравнений**

Цель: овладеть методом Гаусса решения систем линейных уравнений.

Решетить методом Гаусса системы линейных уравнений.

Задача 1.

$$\begin{cases} 8x_1 + 7x_2 + 3x_3 = 18, \\ -7x_1 - 4x_2 - 4x_3 = -11, \\ -6x_1 + 5x_2 - 4x_3 = -15. \end{cases}$$

Задача 2.

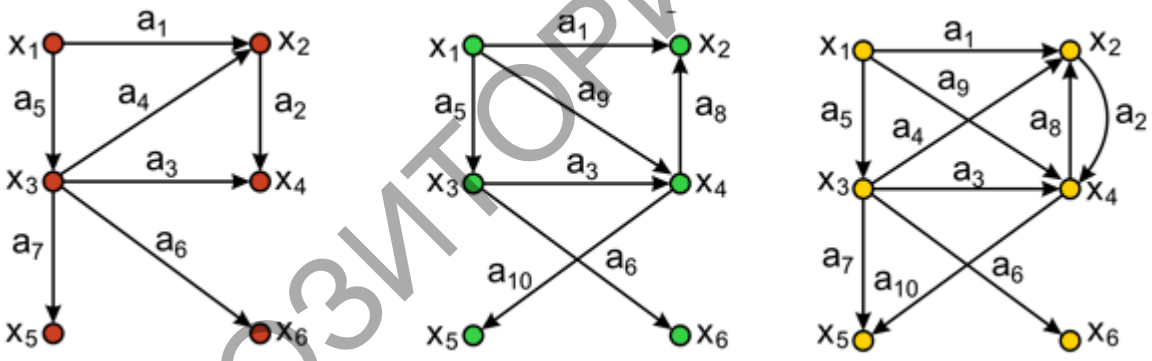
$$\begin{cases} 3x_1 + 2x_2 + x_3 + x_4 = 18, \\ x_1 - x_2 + 4x_3 - x_4 = -1, \\ -2x_1 - 2x_2 - 3x_3 + x_4 = 9, \\ x_1 + 5x_2 - x_3 + 2x_4 = 4. \end{cases}$$

Тема 5. Матричные представления графов

Практическая работа 1. Графическое и матричное представление графа

Цель: научиться решать задачи, с помощью графов, оперируя их графическим и матричным представлением.

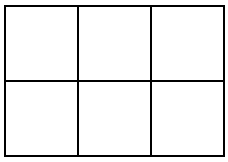
Задача 1. Записать матрицы смежности инциденций и достижимости следующих графов.



Задача 2. Шахматный турнир проводится по круговой системе. Это означает, что каждая пара игроков встречается между собой ровно один раз. В турнире участвуют семь школьников. Известно, что Ваня сыграл шесть партий, Толя – пять, Леша и Дима – по три, Семен и Илья – по две, Женя – одну. С кем сыграл Леша? Решить задачу двумя способами, с помощью графического и матричного представления графа.

Задача 3. В соревновании по круговой системе с 5 участниками провели все встречи. Сколько встреч было сыграно? Нарисовать матрицу смежности графа, отображающую проведенные встречи.

Задача 4. Какое наибольшее количество разрезов можно сделать в сетке (3x2) так, чтобы она не распалась? Какое количество нулей будет содержать матрица смежности графа, полученного в результате разреза.



Тема 6. Задачи оптимизации на графах

Практическая работа 1. Нахождение минимальных путей в графе

Цель: научиться решать задачи нахождения минимальных путей в графе с помощью алгоритма Дейкстры.

Задача. Задана матрица весов графа. Построить граф. Найти кратчайший путь из вершины 1 в вершину 9. Построить дерево минимальных путей. Построить матрицу смежности дерева минимальных путей.

Ниже приведены варианты матриц весов.

B1	s	1	2	3	4	t
s	∞	3	∞	3	∞	∞
2	∞	∞	1	4	∞	∞
3	∞	∞	∞	∞	7	2
4	∞	∞	2	∞	5	∞
6	∞	∞	∞	∞	∞	1
t	3	∞	∞	∞	∞	∞

B2	s	1	2	3	4	t
s	∞	3	∞	2	∞	∞
2	∞	∞	7	∞	4	∞
3	∞	∞	∞	∞	∞	8
4	∞	∞	9	∞	6	∞
6	∞	∞	∞	∞	∞	3
t	∞	∞	∞	5	∞	∞

B3	s	1	2	3	4	t
s	∞	3	∞	4	∞	∞
2	∞	∞	6	∞	4	∞
3	∞	∞	∞	∞	∞	8
4	∞	∞	3	∞	4	∞
6	∞	∞	∞	∞	∞	5
t	∞	∞	∞	2	∞	∞

B4	s	1	2	3	4	t
s	∞	3	5	3	∞	∞
2	∞	∞	4	7	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	3	∞
6	∞	∞	∞	6	∞	6
t	∞	∞	∞	∞	∞	∞

B5	s	1	2	3	4	t
s	∞	2	9	3	∞	∞
2	∞	∞	4	1	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	5	∞
6	∞	∞	∞	3	∞	6
t	∞	∞	∞	∞	∞	∞

B6	s	1	2	3	4	t
s	∞	6	7	8	∞	∞
2	∞	∞	4	3	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	3	∞
6	∞	∞	∞	2	∞	5
t	∞	∞	∞	∞	∞	∞

B7	s	1	2	3	4	t
s	∞	3	5	3	∞	∞
2	∞	∞	2	6	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	5	∞
6	∞	∞	∞	3	∞	3
t	∞	∞	∞	∞	∞	∞

B8	s	1	2	3	4	t
s	∞	2	6	3	∞	∞
2	∞	∞	3	5	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	2	∞
6	∞	∞	∞	3	∞	4
t	∞	∞	∞	∞	∞	∞

B9	s	1	2	3	4	t
s	∞	3	6	5	∞	∞
2	∞	∞	4	1	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	4	∞
6	∞	∞	∞	3	∞	2
t	∞	∞	∞	∞	∞	∞

B10	s	1	2	3	4	t
s	∞	9	2	3	∞	∞
2	∞	∞	4	1	∞	∞
3	∞	∞	∞	∞	∞	4
4	∞	∞	∞	∞	4	∞
6	∞	∞	∞	7	∞	5
t	∞	∞	∞	∞	∞	∞

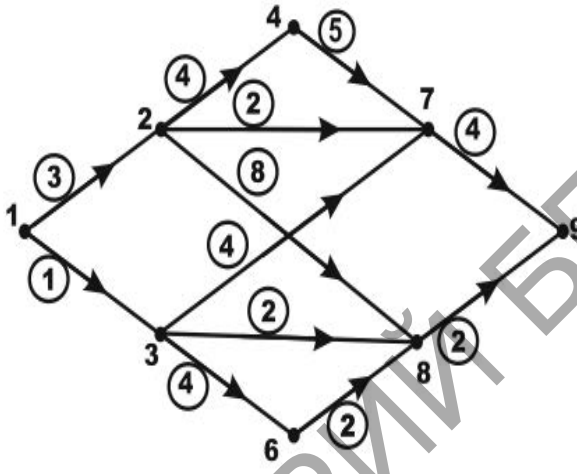
Пример решения

Пусть матрица весов имеет вид

.	1	2	3	4	6	7	8	9
1	∞	3^+	1^+	∞	∞	∞	∞	∞
2	∞	∞	∞	4^+	∞	2^+	8	∞
3	∞	∞	∞	∞	4^+	4	2^+	∞
4	∞	∞	∞	∞	∞	5	∞	∞
6	∞	∞	∞	∞	∞	∞	2	∞
7	∞	∞	∞	∞	∞	∞	∞	4
8	∞	∞	∞	∞	∞	∞	∞	2^+
9	∞	∞	∞	∞	∞	∞	∞	∞

Решение

Построим граф. Граф содержит 8 вершин, пронумерованных 1, 2, 3, 4, 6, 7, 8, 9. Матрица весов P представляет собой таблицу, где строки и столбцы соответствуют номерам вершин, а элемент p_{ij} равен соответствующему весу дуги, если из вершины i в вершину j есть дуга и $p_{ij} = \infty$, если из вершины i в вершину j нет дуги. Например, если из вершины 1 в вершину 2



есть дуга, то на пересечении строки 1 и столбца 2 будет стоять вес соответствующей дуги, в нашем случае это 3; если из вершины 9 в вершину 8 нет дуги, то на пересечении строки 9 и столбца 8 будет стоять ∞.

Применим алгоритм Дейкстры

$q_1 = 0$, $q_2 = \infty$, $q_3 = \infty$, $q_4 = \infty$, $q_5 = \infty$, $q_6 = \infty$, $q_7 = \infty$, $q_8 = \infty$, $q_9 = \infty$.

I. $i = 1$. Помечаем вершину 1 (на первом шаге i равно номеру вершины, из которой ищутся минимальные пути – в нашем случае 1).

Пересчитываем q_j для непомеченных вершин по формуле:

$q_j = \min\{ q_j, q_i + p_{ij}\}$

$q_2 = \min\{q_2, q_1 + p_{12}\} = \min\{\infty, 0+3\} = 3,$

$q_3 = \min\{q_3, q_1 + p_{\underline{13}}\} = \min\{\infty, 0+1\} = 1,$

$q_4 = \min\{q_4, q_1 + p_{14}\} = \min\{\infty, 0+\infty\} = \infty,$

$q_6 = \min\{q_6, q_1 + p_{16}\} = \min\{\infty, 0+\infty\} = \infty,$

$q_7 = \min\{q_7, q_1 + p_{17}\} = \min\{\infty, 0+\infty\} = \infty,$

$q_8 = \min\{q_8, q_1 + p_{18}\} = \min\{\infty, 0+\infty\} = \infty,$

$q_9 = \min\{q_6, q_1 + p_{19}\} = \min\{\infty, 0+\infty\} = \infty.$

j_{min} – индекс, на котором достигается $\min\{q_j\}$ (то есть выбираем самое маленькое q_j и запоминаем его номер. В нашем случае это $\min\{q_j\}=q_3=1$, запоминаем номер $j_{min}=3$. Помечаем дугу (1, 3) в таблице весов знаком «+». И помечаем вершину 3. Таким образом, имеем две помеченные вершины {1; 3}.

II. $i=j_{min}=3$, $q_3=1$. Пересчитываем q_j для непомеченных вершин:

$q_2 = \min\{q_2, q_3 + p_{32}\} = \min\{3, 1+\infty\} = 3,$

$q_4 = \min\{q_4, q_3 + p_{34}\} = \min\{\infty, 1+\infty\} = \infty,$

$q_6 = \min\{q_6, q_3 + p_{36}\} = \min\{\infty, 1+4\} = 5,$

$q_7 = \min\{q_7, q_3 + p_{37}\} = \min\{\infty, 1+4\} = 5,$

$q_8 = \min\{q_8, q_3 + p_{\underline{38}}\} = \min\{\infty, 1+2\} = 3,$

$q_9 = \min\{q_9, q_3 + p_{39}\} = \min\{\infty, 1+\infty\} = \infty.$

Выбираем самое маленькое q_j и запоминаем его номер: $\min\{q_j\}=q_8=3$, запоминаем номер $j_{min}=8$. Помечаем дугу (3, 8) в таблице весов знаком «+». Помечаем вершину 8. Таким образом, множество помеченных вершин имеет вид {1; 3; 8}.

III. $i=j_{min}=8$, $q_8=3$. Пересчитываем q_j для непомеченных вершин:

$q_2 = \min\{\boldsymbol{q_2}, q_8 + p_{82}\} = \min\{\boldsymbol{3}, 3+\infty\}=3,$

$q_4 = \min\{q_4, q_8 + p_{84}\} = \min\{\infty, 3+\infty\}=\infty,$

$q_6 = \min\{q_6, q_8 + p_{86}\} = \min\{5, 3+\infty\}=5,$

$q_7 = \min\{q_7, q_8 + p_{87}\} = \min\{5, 3+\infty\}=5,$

$q_9 = \min\{q_9, q_8 + p_{89}\} = \min\{\infty, 3+2\}=5.$

Выбираем самое маленькое q_j и запоминаем его номер: $\min\{q_j\}=q_2=3$, запоминаем номер $j_{min}=2$. Помечаем дугу (1, 2) – дуга, на которой было достигнуто значение $q_2=3$ (в нашем случае оно было достигнуто на I-ом шаге на дуге (1,2)) в таблице весов знаком «+». Помечаем вершину 2, добавляя ее к списку помеченных вершин {1; 3; 8, 2}.

IV. $i=j_{min}=2$, $q_2=3$. Пересчитываем q_j для непомеченных вершин:

$q_4 = \min\{q_4, q_2 + p_{24}\} = \min\{\infty, 3+4\} = 7,$

$q_6 = \min\{q_6, q_2 + p_{26}\} = \min\{5, 3+\infty\} = 5,$

$q_7 = \min\{q_7, q_2 + p_{\underline{27}}\} = \min\{5, 3+2\} = 5,$

$q_9 = \min\{q_9, q_2 + p_{29}\} = \min\{5, 3+\infty\} = 5.$

Выбираем самое маленькое q_j. Поскольку мы имеем дело с тремя одинаковыми значениями, можем выбрать одно из них,

кроме q_9 , так как вершина 9 конечна. И если на вершине *9* достигнуто одно из минимальных значений q_9=5, то на этом шаге мы можем построить минимальный путь из вершины 1 в вершину 9: (1, 3) → (3, 8) → (8, 9) и включить вершину 9 в список помеченных вершин

Выберем min$\{q_j\}$=q_7=5, запоминаем номер j_{min}=7. Помечаем дугу (2, 7) в таблице весов знаком «+». Помечаем вершину 7, добавляя ее к списку помеченных вершин {1; 3; 8; 2; 7; 9}.

V. i=j_{min}=7, q_7=5. Пересчитываем q_j для непомеченных вершин:

q_4 = min$\{q_4, q_7 + p_{74}\}$ = min$\{7, 5+\infty\}$=7,

q_6 = min$\{\boldsymbol{q_6}, q_7 + p_{76}\}$ = min$\{5, 5+\infty\}$=5.

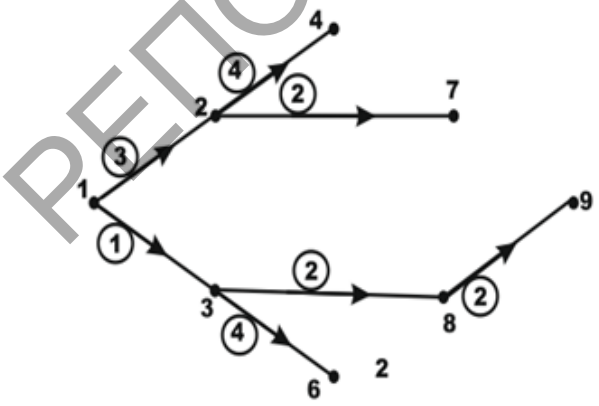
Выберем min$\{q_j\}$=q_6=5, запоминаем номер j_{min}=5. Помечаем дугу (3, 6) в таблице весов знаком «+». Помечаем вершину 6, добавляя ее к списку помеченных вершин {1; 3; 8; 2; 7; 6; 9}.

VI. i=j_{min}=6, q_6=5. Пересчитываем q_j для непомеченных вершин:

q_4 = min$\{\boldsymbol{q_4}, q_7 + p_{74}\}$ = min$\{7, 5+\infty\}$=7,

Помечаем дугу (2, 4) в таблице весов знаком «+». Помечаем вершину 4, добавляя ее к списку помеченных вершин {1; 3; 8; 2; 7; 6; 4; 9}. Таким образом, мы пометили все вершины.

Прорисовываем все дуги, отмеченные в таблице весов знаком «+», получаем дерево минимальных путей рассматриваемого графа. Матрица смежности минимальных путей будет иметь вид



	1	2	3	4	6	7	8	9
1	0	1	1	0	0	0	0	0
2	0	0	0	1	0	1	0	0
3	0	0	0	0	1	0	1	0
4	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0

Тема 7. Пространство событий

Практическая работа 1. **События и операции над ними**

Цель: изучить виды событий и операции над ними

Задача 1. Найдите сумму событий:

а) испытание – два выстрела по мишени; события: A – «попадание первым выстрелом», B – «попадание вторым выстрелом»;

б) испытание – бросание игральной кости; события: A – «появление одного очка», B – «появление двух очков», C – «появление трех очков»;

в) испытание – приобретение лотерейных билетов; события: A – «выигрыш 10 рублей», B – «выигрыш 20 рублей», C – «выигрыш 25 рублей».

Задача 2. Найдите произведение событий:

а) испытание – два выстрела по мишени; события: A – «попадание первым выстрелом», B – «попадание вторым выстрелом»;

б) испытание – бросание игральной кости; события: A – «непоявление трех очков», B – «непоявление пяти очков»; C – «появление нечетного числа очков».

Задача 3. При бросании игральной кости обозначим событие «появление двух очков» как A, «появление одного очка» – B и «появление трех очков» – C. Найдите событие: а) $A+B+C$; б) ABC; в) $AB+C$; г) $A+BC$; д) $A(B+C)+B$.

Ответ выберите из списка: а) «невозможное событие»; б) «появление одного очка»; в) «появление трех очков»; г) «появление двух очков»; д) «появление не более трех очков».

Задача 4. Пусть A, B и C – случайные события, выраженные подмножествами одного и того же множества элементарных событий. Используя операции сложения и умножения, запишите следующие события: а) произошло только событие А; б) произошло одно и только одно из данных событий; в) произошло

два и только два из данных событий; г) произошли все три события; д) произошло хотя бы одно из данных событий.

Ответ выберите из приведенного списка: а) $A+B+C$; б) ABC; в) $A\overline{B}\overline{C}$; г) $A\overline{B}\overline{C}+\overline{A}B\overline{C}+\overline{A}\overline{B}C$; д) $\overline{A}BC+A\overline{B}C+AB\overline{C}$.

Тема 8. Способы задания вероятностей

Практическая работа 1. **Вычисление вероятности**

Цель: научиться вычислять вероятности.

Задача 1. В коробке 100 шаров, помеченных номерами 1, 2, …, 100. Из коробки наугад вынимают один шар. Какова вероятность того, что номер вынутого шара содержит цифру 5?

Задача 2. В коробке 9 белых и 6 черных шаров. Из коробки вынимают два шара. Какова вероятность того, что оба шара окажутся белыми?

Задача 3. В партии из 8 деталей имеется 6 стандартных. Найдите вероятность того, что среди взятых наугад деталей ровно три стандартных.

Задача 4. Восемь различных книг расставляются наугад на одной полке. Найдите вероятность того, что две определенные книги окажутся поставленными рядом.

Задача 5. В книжном магазине на полке 10 различных книг, причем 5 книг стоят по 4 рубля каждая, 3 книги – по одному рублю и две книги – по 3 рубля. Найдите вероятность того, что взятые наугад две книги стоят 5 рублей.

Задача 6. Оля и Коля договорились встретить Новый год в компании десяти человек. Они оба хотели сидеть за праздничным столом рядом. Найдите вероятность исполнения их желания, если среди друзей принято места распределять по жеребьевке.

Задача 7. Бросаются одновременно две игральные кости. Найти вероятности следующих событий: а) сумма выпавших очков равна 8; б) произведение выпавших очков равно 8; в) сумма выпавших очков больше, чем их произведение;

г) сумма выпавших очков меньше, чем их произведение; д) сумма выпавших очков равна их произведению.

Ответ выберите из списка: а) 11/36; б) 1/36; в) 5/36; г) 1/18; д) 2/3.

Тема 9. Операции над вероятностями

Практическая работа 1. **Сложение, умножение вероятностей. Формула полной вероятности.**

Цель: научиться решать задачи на нахождение вероятности с применением правил сложения, умножения вероятностей и формулы полной вероятности.

Задача 1. Лаборатория получает изделия от заводов А, В и С. Вероятность поступления изделий от завода А равна 0,35, от завода В – 0,4. Найти вероятность того, что очередная партия изделий поступит от завода С.

Задача 2. Три стрелка стреляют по цели. Вероятность попадания в цель для первого стрелка равна 0,7, для второго – 0,8, для третьего – 0,9. Найти вероятность р того, что в цель попадет хотя бы один стрелок.

Задача 3. Инженер центра информационных состояний отвечает за исправное состояние компьютеров в трех лабораториях вычислительной техники кафедры информационных технологий в культуре. Вероятность того, что в течение дня потребует внимания 1-я лаборатория, равна 0,5; 2-я лаборатория – 0,6; 3-я лаборатория – 0,8. Найдите вероятности следующих событий: а) «ни одна лаборатория в течение дня не потребует внимания инженера»; б) «1-я лаборатория потребует внимания инженера, а 2-я и 3-я нет»; в) «1-я и 2-я лаборатории потребуют внимания инженера, а 3-я нет»; г) «хотя бы одна из лабораторий потребует внимания инженера в течение дня»; д) «не более одной лаборатории потребуется внимание инженера».

Задача 4. На кафедру информационных технологий в культуре поступают контрольные работы по дисциплине «Основы

высшей математики» от студентов 108, 111 и 112 группы факультета заочного обучения. Вероятность поступления контрольных работ от 108 группы равна 0,42, от 111 группы – 0,3. Найдите вероятность поступления контрольных работ от 112 группы.

Задача 5. Найдите вероятность выпадения: а) 3 гербов при подкидывании 3 монет; б) 4 цифр при подкидывании 4 монет; в) 2 очков при бросании игральной кости; г) 2 или 12 очков при бросании 2 игральных костей; д) 2 или 3 очков при бросании 2 игральных костей.

Ответ выберите из приведенного списка:

а) $\frac{1}{18}$; б) $\frac{1}{12}$; в) $\frac{1}{8}$; г) $\frac{1}{16}$; д) $\frac{1}{36}$.

Задача 6. На склад поступает продукция трех фабрик, причем продукция первой фабрики составляет 20 %, второй – 46 %, третьей – 34 %. Известно, что процент нестандартных изделий для первой фабрики равен 3 %, для второй – 2 %, для третьей – 1 %. Найдите вероятность того, что наудачу взятое нестандартное изделие произведено на первой фабрике.

Задача 7. Применяемый метод лечения приводит к выздоровлению в 90 % случаев. Какова вероятность того, что из 5 больных поправится не менее 4?

Задача 8. В квартире шесть электрических лампочек. Вероятность того, что каждая лампочка останется исправной в течение года, равна 5/6. Найдите вероятность того, что в течение года придется заменить две лампочки.

Задача 9. Вероятность попадания в мишень одним выстрелом равна 1/5. Найдите вероятность того, что из десяти выстрелов не будет ни одного попадания.

Задача 10. На факультете культурологии и социокультурной деятельности имеются 4 проектора. Вероятность того, что каждый проектор останется исправным в течение года, равна 3/4. Найдите вероятность того, что в течение года: а) все 4 проектора выйдут из строя; б) ни один проектор не выйдет из

строя; в) выйдет из строя хотя бы один проектор; г) выйдет из строя не более 2 проекторов; д) выйдет из строя не менее 2 проекторов.

Ответ выберите из списка: а) 67/256; б) 1/256; в) 81/256; г) 175/256; д) 243/256.

Тема 10. Дискретная случайная величина

Практическая работа 1. Математическое ожидание, дисперсия, среднее квадратическое отклонение случайной величины

Цель: научиться вычислять математическое ожидание, дисперсию и среднее квадратическое отклонение дискретной случайной величины.

Задача 1. Закон распределения дискретной случайной величины X задан следующей таблицей:

X	-2	-1	1	3
p	0,1	0,27	0,34	0,29

Найдите математическое ожидание, дисперсию и среднее квадратическое отклонение.

Задача 2. Случайная величина X распределена по нормальному закону. Математическое ожидание и среднее квадратическое отклонение этой величины соответственно равны 8 и 5. Найдите вероятность того, что X примет значение, принадлежащее интервалу (10; 20).

Задача 3. Найдите дисперсию случайной величины X, зная закон ее распределения:

X	0	1	2	3	4
p	0,2	0,4	0,3	0,08	0,02

Задача 4. Значения дискретной случайной величины X образованы количеством очков при бросании 4 игральных костей. Найдите математическое ожидание, дисперсию и среднее квадратическое отклонение.

Задача 5. Чему равно математическое ожидание количества: а) гербов при бросании 3 монет; б) очков при бросании 2 игральных костей; в) гербов при бросании 2 монет; г) гербов при бросании 4 монет; д) очков при бросании 3 игральных костей.

Ответ выберите из списка: а) 7; б) 1; в) 2; г) 1,5; д) 10,5.

Тема 14. Алгебраические и стохастические фракталы

Практическая работа 1. Комплексные числа и действия над ними

Цель: научиться выполнять основные арифметические действия с комплексными числами.

Задача 1. Даны числа $Z_1 = a_1 + b_1 i$ и $Z_2 = a_2 + b_2 i$. Найти 1) сумму двух чисел $Z_1 + Z_2$; 2) разность двух чисел $Z_1 - Z_2$; 3) произведение чисел $Z_1 Z_2$; 4) отношение двух чисел Z_1 / Z_2 ; 5) найти абсолютные значения чисел Z_1 и Z_2 . Изобразить сумму и разность двух комплексных чисел в виде суммы и разности соответствующих векторов в декартовой системе координат.

Задача 2. Вычислить и изобразить на координатной плоскости четыре первых члена последовательности $z_{n+1} = z_n^2 + c$, где $c = Z_1$

Варианты значений a_1, b_1, a_2, b_2:

Номер вар.	a_1	b_1	a_2	b_2
1	1	-2	3	-1
2	2	1	-3	1
3	1	-2	4	1
4	-2	4	1	3
5	-3	1	2	1
6	2	-3	1	-2
7	3	-2	-2	3
8	1	-4	1	-1
9	2	-1	3	2
10	1	-3	2	-3

к разделу III
«Медиакультура специалиста»

Тема 29. Медиатекст как средство художественно-творческой, воспитательной и организационно-методической деятельности учреждений культуры и искусств

Практическая работа 1. Использование графических медиатекстов в профессиональной деятельности культуролога

Цели:

– углубить и систематизировать имеющиеся знания, сформировать практические умения создания и использования графических медиатекстов в профессиональной деятельности культуролога;

– сформировать умения анализа электронных медиатекстов по категориям медиаобразования.

Задание для выполнения

Создайте графический медиатекст социокультурной направленности, опишите его по ключевым понятиям. Оцените его эффективность

Выполнение работы

Задача 1.

1. Разработайте концепцию медиатекста: определите его тематику и цели.

2. Выделите главные мысли и идеи, которые вы хотите донести до аудитории.

3. Опишите проект медиатекста по ключевым понятиям (табл. 3.3).

Таблица 3.3

Ключевые понятия для анализа медиатекста

№	*Вопросы к понятию*	*Ключевые понятия*
1	Кто передает медиатекст и почему?	Агентство медиа
2	Как он передан и в какой форме?	Категория медиа
3	Как он создан?	Технология медиа
4	Как мы узнаем, о чем он и что означает?	Язык медиа
5	Кто воспринимает этот текст?	Аудитория медиа
6	Как этот медиатекст преподносит свою тематику?	Репрезентация медиа

Примечание. Рассмотрите пример выполнения задачи 1 (табл. 3.4).

Таблица 3.4

Пример анализа графического медиатекста

<table>
<tr><td colspan="3">Графический медиатекст социокультурной направленности</td></tr>
<tr><td rowspan="3"> 
</td><td>Тема</td><td>Сохранение культурной идентичности</td></tr>
<tr><td>Цель</td><td>Обратить внимание на проблему потери детьми культурных основ своего народа</td></tr>
<tr><td>Главные мысли, идеи</td><td>Родители должны воспитывать в детях интерес к культуре народа, гордость за страну, в которой они живут. В обществе есть подростки, выпавшие из исторического и социокультурного контекста</td></tr>
<tr><td colspan="3">Ключевые понятия</td></tr>
<tr><td>1</td><td>Агентство медиа</td><td>Организация в области образования или культуры</td></tr>
<tr><td>2</td><td>Категория медиа</td><td>Социальный плакат в жанре призыва</td></tr>
<tr><td>3</td><td>Технология медиа</td><td>Графические редакторы</td></tr>
<tr><td>4</td><td>Язык медиа</td><td>Замена головы ребенка на тыкву, текстовые надписи и др.</td></tr>
<tr><td>5</td><td>Аудитория медиа (целевая)</td><td>Молодые родители
Люди подросткового возраста
Все общество</td></tr>
<tr><td>6</td><td>Репрезентация медиа</td><td>Формальное подражание чужим традициям делает из людей нелепых кукол</td></tr>
</table>

Задача 2. Используя любой графический редактор, создайте графический медиатекст.

Помните о ключевых понятиях анализа медиатекста, которые вы определили перед его созданием.

Задача 3.

1. Уточните основные понятия анализа медиатекста. Запишите их в виде дополнительного третьего столбца к таблице 3.4.

2. Предложите созданный медиатекст для анализа по ключевым понятиям сокурснику. Дополните получившуюся после выполнения п. 1 таблицу его ответами в виде четвертого столбца.

Задача 4. Соотнесите полученные оценки созданного медиатекста. Сделайте выводы об его эффективности.

Задача 5. Оформите отчет. Оцените ваши личные успехи при выполнении данной работы и предъявите результаты преподавателю.

Литература

1. Кириллова, Н. Б. Медиакультура: от модерна к постмодерну / Н. Б. Кириллова. – М. : Академический проект, 2005. – 448 с.

2. Сметанина, С. И. Медиа-текст в системе культуры: динамические процессы в языке и стиле журналистики конца XX века / С. И. Сметанина. – М. : Издательство Михайлова В. А., 2002. – 384 с.

3. Федоров, А. В. Медиаобразование и медиаграмотность : учеб. пособие для вузов / А. В. Федоров. – Таганрог : Кучма, 2004. – 340 с.

4. Федоров, А. В. Медиаобразование: история, теория и методика / А. В. Федоров. – Ростов : ЦВВР, 2001. – 708 с.

5. Федоров, А. В. Медиаобразование: социологические опросы / А. В. Федоров. – Таганрог : Кучма, 2007. – 228 с.

6. http://www.edu.of.ru/mediaeducation – электронный ресурс по медиаобразованию.

7. http://www.psyfactor.org/lybr.htm – материалы психологической и общегуманитарной тематики (медиавоздействие, медиаманипуляции).

8. http://www.ifap.ru – программа ЮНЕСКО «Информация для всех».

9. http://www.mediagram.ru – электронный ресурс по медиаграмотности.

Вопросы для самоконтроля

1. Каковы основные технологии создания графических медиатекстов? Приведите примеры.

2. Какие основные категории необходимо определить для создания эффективного медиатекста?

3. Какое программное обеспечение вам понадобится для создания и редактирования графических медиатекстов?

4. По каким критериям можно классифицировать медиатексты?

5. Приведите примеры использование графических медиатекстов в профессиональной деятельности культуролога.

Тема 31. Коммуникационное пространство. Сетевые сообщества

Практическая работа 1. Использование социальных сервисов Интернета в профессиональной деятельности культуролога

Цели:

– углубить и систематизировать имеющиеся знания, сформировать навыки применения социальных сервисов Интернета в профессиональной деятельности культуролога;

– сформировать умения использования Интернета для составления аннотированных списков социальных сервисов профессиональной тематики.

Задание для выполнения

Найдите социальные сервисы Интернета культурологической тематики и проанализируйте возможности их применения в вашей профессиональной деятельности

Выполнение работы

Задача 1.

Приведите примеры информационных ресурсов по каждому из видов социальных сервисов. Результаты представьте в виде таблицы 3.5.

Таблица 3.5

Социальные сервисы сети Интернет

Вид социального сервиса Интернета	Название	URL-адрес	Основной контент	Возможность использования в профессиональной деятельности культуролога (поиск, консультирование, реклама и т. д.)
Блог				
Вики				
Географический сервис				
Социальная сеть				
Социальное хранилище				
Форум				

Задача 2.

Проанализируйте возможности модератора, участника и владельца в блоге, форуме и социальной сети. По результатам анализа заполните таблицу 3.6.

Таблица 3.6

Анализ прав и возможностей модератора, участника и владельца

	Блог	Форум	Социальная сеть
Кто управляет коммуникацией?			
Кто имеет право задавать темы для обсуждения?			
Кто имеет право на редактирование сообщений?			
Кто регламентирует права участников коммуникации?			
Кто осуществляет контроль соблюдения правил общения?			

Задача 3.

1. Найдите и изучите социальные сервисы Интернета искусствоведческой тематики.

2. Составьте аннотированное описание найденных ресурсов.

Аннотированное описание может включать следующие элементы:

1) название и URL-адрес;

2) основное контентное наполнение;

3) организация обратной связи;

4) используемые средства навигации;

5) возможность использования в профессиональной деятельности культуролога.

Пример. Белорусский онлайн-фотобанк [Электронный ресурс] / Белорусский банк фотографий. – Режим доступа: http://fotobank.by – Дата доступа: 11.04.11 – цифровая онлайн-библиотека изображений нового поколения, специализируется на сборе, сортировке и хранении цифровых копий изображений широкого спектра и правового статуса. Ресурс рассчитан на широкий круг посетителей и служит идеям информатизации общества и упорядочивания оборота изображений в сети. Имеется возможность регистрации, поиска по категориям, расширенного поиска, отправки сообщения и полная контактная информация. Полезен для поиска и размещения фотоматериалов.

3. Проанализируйте социальные сети из списка найденных по возможности их использования в профессиональной деятельности культуролога (результаты представьте в виде таблицы 3.7).

Таблица 3.7

Анализ информационных ресурсов

№	Название информационного ресурса	URL-адрес	Основной контент	Дизайн (оценить по 10-балльной системе)		Возможность использования в профессиональной деятельности культуролога (поиск информации, консультирование, реклама и т. д.)
				Удобство навигации	Цветовая гармония	

Задача 4. Оформите отчет.

Задача 5. Оцените ваши личные успехи при выполнении данной работы и предъявите результаты преподавателю.

Литература

1. Гусев, В. С. Internet: учеба, работа, полезные ресурсы. Краткое руководство / В. С. Гусев. – М. и др. : Диалектика, 2005. – 254 с.

2. Жданевич, И. М. Коммуникативное пространство. Личность и межличностное взаимодействие в сети Internet / И. М. Жданевич, Е. И. Кучерявый. – М. : Компак, 2002. – 286 с.

3. Костина, А. В. Интернет-сообщества. Что обсуждается в Интернете? / А. В. Костина. – М. : Либроком, 2011. – 176 с.

4. Кучников, Т. В. Общение в Интернет / Т. В. Кучников. – М. : Альянс-пресс, 2004. – 128 с.

5. Лазарев, В. Г. Рассылки как средство маркетинга и рекламы / В. Г. Лазарев, Г. Г. Савин. – М. : Эрудит, 2005. – 301 с.

Вопросы для самоконтроля

1. Что такое социальные сервисы Интернета, их преимущества и недостатки.

2. Какие социальные сервисы сети Интернет вы предложили бы использовать для организационной деятельности культуролога?

3. Раскройте сущность и назначение социальных закладок.

4. Приведите примеры и охарактеризуйте социальные сервисы сети Интернет.

5. Что такое сетевой этикет?

Тема 34. Программные средства создания, редактирования и управления медиатекстами

Пактическая работа 1. Способы и средства обработки графических изображений

Цели:

– углубить и систематизировать знания по использованию графических редакторов;

– сформировать умения использования информационных ресурсов, содержащих базы данных графических медиатекстов и материалы по их созданию.

Задание для выполнения

Проанализируйте возможности использования различных видов графики и графических форматов в профессиональной деятельности культуролога

Выполнение работы

Задача 1.

1. Проанализируйте возможности растровой, векторной и фрактальной графики. Заполните таблицу 3.8.

Таблица 3.8

Таблица анализа видов компьютерной графики

	Растровая графика	Векторная графика	Фрактальная графика
Основной элемент изображения			
Изменение качества изображения при масштабировании (с ухудшением или без изменения качества)			
Соотношение цвета и формы (отделены или не отделены)			
Фотореалистичность (да, нет)			
Форматы			
Графические программы			
Примеры применения в профессиональной деятельности культуролога			

2. По результатам анализа сделайте вывод о целесообразности использования различных видов графики в профессиональной деятельности культуролога.

3. Используя графические редакторы Microsoft Paint, Adobe Photoshop, CorelDraw, проанализируйте их возможности по следующим критериям: создание рисунка (режим ручной прорисовки, с использованием инструментов); манипулирование рисунком (выделение фрагментов, проработка мелких деталей); оформление рисунка текстом (выбор шрифта); работа с цветом (создание своей палитры, создание своего узора для закраски); дополнительные возможности (выбор формы кисти, выбор размера распыления, включение отображения координат курсора, использование направляющих, фильтрация, «размывание» рисунка, изменение размера шрифта, создание анимации). По результатам анализа составьте таблицу, где поставьте плюс (возможность присутствует) или минус (возможность отсутствует).

Задача 2.

1. Проанализируйте свойства и возможности цветовых моделей, используемых в компьютерной графике. Заполните таблицу 3.9.

Таблица 3.9

Анализ цветовых моделей

	RGB	CMYK	LAB	HSB
Способ получения цвета				
Для какого класса устройств предназначена				
Аппаратная зависимость				
Цветовой охват				
Область применения				

2. Проанализируйте возможности, которые поддерживают различные графические форматы. Заполните таблицу 3.10.

Таблица 3.10

Анализ графических форматов

Формат	Слои	Цветовая модель	Прозрачность	Сохранение анимации
BMP				
JPG				
GIF				
PNG				
TIFF				
PSD				

Задача 3.

1. Найдите и изучите информационные ресурсы, содержанием которых являются базы графических изображений и технологии их создания.

2. Составьте аннотированное описание каждого из изученных информационных ресурсов.

3. Проанализируйте информационные ресурсы по возможности их использования в профессиональной деятельности культуролога (результаты представить в виде таблицы).

Задача 4. Оформите отчет.

Задача 5. Оцените ваши личные успехи при выполнении данной работы и предъявите результаты преподавателю.

Литература

1. Гурский, Ю. Компьютерная графика Photoshop CS5, CorelDRAW X5, Illustrator CS5. Трюки и эффекты / Ю. Гурский, А. Жвалевский, В. Завгородний. – СПб. : Питер, 2011. – 704 с.

2. Немцова, Т. И. Компьютерная графика и Web-дизайн. Практикум по информатике (+ CD-ROM) / Т. И. Немцова, Ю. В. Назарова. – М. : Форум : Инфра-М, 2010. – 288 с.

3. Петров, М. Н. Компьютерная графика (+ CD-ROM) / М. Н. Петров. – СПб. : Питер, 2011. – 544 с.

4. Тимофеев, С. М. Новейшая энциклопедия компьютерной графики / С. М. Тимофеев. – М. : Эксмо-пресс. – 2009. – 512 с.

Вопросы для самоконтроля

1. Какое программное обеспечение вы будете использовать для создания транспаранта большого размера? Обоснуйте свой выбор.

2. На вашем компьютере установлены: Microsoft Paint, Adobe Photoshop, CorelDRAW. Какое программное обеспечение вы будете использовать для создания анимации?

3. Приведите примеры использования графических редакторов в профессиональной деятельности культуролога?

4. Какие из сетевых информационных ресурсов, содержащих базы данных графических медиатекстов и материалы по их созданию, будут наиболее полезны в вашей профессиональной деятельности?

5. В каких случаях вы будете использовать редакторы фрактальной графики в своей профессиональной деятельности?

РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

ПЕРЕЧЕНЬ РЕКОМЕНДОВАННЫХ СРЕДСТВ ДИАГНОСТИКИ

Об учебных достижениях студентов свидетельствуют выполненные в соответствии с целями и задачами лабораторные работы. В качестве одного из элементов диагностического инструментария для выявления уровня учебных достижений студента рекомендуется использовать критериально-ориентированные тесты. Они представляют собой совокупность тестовых заданий закрытой формы с одним или несколькими вариантами правильных ответов; заданий на установление соответствия между элементами двух множеств с одним или несколькими соотношениями и равным или разным количеством элементов в множествах; заданий открытой формы с формализованным ответом; заданий на установление правильной последовательности.

Для измерения степени соответствия учебных достижений студента требованиям образовательного стандарта также рекомендуется использовать проблемные, творческие задачи, предполагающие эвристическую деятельность и неформализованный ответ.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ, ЗАЧЕТУ И ИТОГОВОЙ АТТЕСТАЦИИ

к разделу I
«Прикладная математика»

Вопросы к экзамену

1. Операции над матрицами.
2. Определитель матрицы.
3. Обратная матрица.
4. Системы линейных уравнений. Решение систем линейных уравнений.
5. Решение систем линейных уравнений методом Гаусса.
6. Формулы Крамера решения систем линейных уравнений.
7. Понятие графа.
8. Матричные представления графа.
9. Дерево. Покрывающее граф дерево.
10. Построение матрицы достижимостей. Нахождение пути длины р.
11. Поток на графе. Поиск максимального потока.
12. Нахождение минимального пути между двумя вершинами графа.
13. Испытания и события. Полная группа событий.
14. Операции над событиями.
15. Вероятность. Классическое определение вероятности.
16. Геометрический и статистический методы задания вероятностей.
17. Свойства вероятностной меры.
18. Элементы комбинаторики: перестановки, сочетания, размещения.
19. Операции над вероятностями. Вероятность суммы событий.
20. Вероятность произведения событий.
21. Формула полной вероятности.
22. Формула Байса.
23. Распределение дискретной случайной величины.

24. Математическое ожидание и его свойства.
25. Дисперсия и квадратическое отклонение.
26. Распределение Бернули.
27. Гамма-функция и ее свойства.
28. Нормальное распределение.
29. Распределение хи-квадрат.
30. Распределение Стьюдента.
31. Распределение Фишера.
32. Генеральная совокупность.
33. Выборочная совокупность.
34. Частоты. Относительные частоты. Накопленные частоты.
35. Эмпирическая функция распределения.
36. Статистические оценки параметров.
37. Основные геометрические фракталы.
38. Рекурсивные алгоритмы.
39. Области применения фракталов.
40. Понятие комплексного числа. Графическое представление комплексного числа.
41. Операции над комплексными числами.
42. Фрактал Мандельброта.
43. Мультифракталы.

Задачи к экзамену

1. В коробке 8 белых и 6 черных шаров. Из коробки наугад вынимаются два шара. Найдите вероятность того, что:

а) оба шара черные;

б) оба шара разного цвета.

2. 32 буквы русского алфавита написаны на карточках разрезной азбуки. Пять карточек вынимаются наугад одна за другой и укладываются на стол в порядке появления. Найдите вероятность того, что получится слово «конец».

3. Экзаменационный билет содержит три вопроса. Вероятность того, что студент ответит на первый вопрос, равна 0,9, на второй – 0,9, на третий – 0,8. Найдите вероятность того, что студент сдаст экзамен, если необходимо ответить хотя бы на два вопроса билета.

4. Вероятность подключения абонента к каждой из четырех АТС соответственно равна 0,2; 0,36; 0,16; 0,28. Вероятность соединения с абонентом в случае его подключения к первой АТС равна 0,12, ко второй – 0,125, к третьей – 0,3, к четвертой – 0,75. Какова вероятность соединения ?

5. Вероятность того, что машина, взятая напрокат, будет возвращена исправной, равна 0,8. Какова вероятность, что из 4 возвращенных машин 3 окажутся исправными ?

6. В группе 30 студентов, из которых отличников – 8, хорошо успевающих – 13 и слабо успевающих – 9. На предстоящем экзамене отличники могут получить только оценки «5», хорошо успевающие могут получить с равной вероятностью оценки «4» и «5», слабо успевающие могут получить с равной вероятностью оценки «3», «4» и «5». Для сдачи экзамена вызывается наугад один студент. Найдите вероятность того, что он получит оценку не ниже «4».

7. У рыбака есть три излюбленных места рыбалки, которые он посещает с одинаковой вероятностью. Вероятность клева на первом месте равна 1/3, на втором – 1/2, на третьем – 1/4. Рыбак забросил удочку три раза, а рыба клюнула только один раз. Найдите вероятность того, что он удил рыбу на первом месте.

8. В первом ящике содержится 20 деталей, из них 15 стандартных, во втором 30 деталей, из них 24 стандартных, в третьем – 10 деталей, из них 6 стандартных. Найдите вероятность того, что наугад извлеченная деталь из наудачу взятого ящика – стандартная.

9. Какие из событий являются частью другого события:

а) A – «попадание в мишень первым выстрелом», B – «попадание в мишень по меньшей мере одним из 4 выстрелов», C – «попадание точно в мишень одним из 2 выстрелов», D – «попадание в мишень не более чем 5 выстрелами»;

б) A – «появление 3 очков при бросании игральной кости», B – «появление не более 3 очков при бросании игральной кости», C – «появление не более 4 очков при бросании игральной кости»?

10. Событие A – «появление 6 очков при бросании игральной кости»; событие B – «появление 5 очков при бросании игральной кости», событие C – «появление 4 очков при бросании игральной кости».

В чем состоит событие $A+B+C$?

11. Событие A_1 – «появление четного числа очков при бросании игральной кости», событие A_2 – «появление 2 очков при бросании игральной кости», событие A_3 – «появление 4 очков при бросании игральной кости», событие A_4 – «появление 6 очков при бросании игральной кости».

Докажите, что:

1) $A_1\overline{A}_4=A_2+A_3$; 2) $\overline{A}_1A_2\overline{A}_3A_4=V$; 3) $A_1\overline{A}_3\overline{A}_4=A_2$; 4) $A_1A_2=A_2$;

5) $A_1\overline{A}_2\overline{A}_3=A_4$; 6) $A_2A_3=V$;

12. Рассмотрев конкретные события A, B, C, убедитесь в том, что:

$AB=BA$; $A(BC)=(AB)C$; $A(B+C)=AB+AC$; $A+BC=(A+B)(A+C)$;

$\overline{AB}=\overline{A}+\overline{B}$; $\overline{A+B}=\overline{A}\,\overline{B}$; $(A+B)(A+C)(B+C)=AB+AC+BC$.

13. Наудачу отобранная деталь может оказаться или первого сорта (событие A), или второго (событие B), или третьего (событие C).

В чем состоят события: $A+B$; $\overline{A+C}$; AC; $AB+C$?

14. Пусть A, B и C – случайные события, выраженные подмножествами одного и того же множества элементарных событий. Запишите событие, означающее, что:

а) произошло только событие A;

б) произошло одно и только одно из данных событий;

в) произошло два и только два из данных событий;

г) произошли все три события;

д) произошло хотя бы одно из данных событий.

15. Событие A – «получение достаточной для сдачи экзамена оценки», событие B – получение «девятки». В чем состоят события $A–B$, $A-\overline{B}$, $\overline{A}-B$, $\overline{A-B}$ и $\overline{A}-\overline{B}$?

16. Событие A – «появление 3 очков при бросании игральной кости», событие B – «появление нечетного числа очков», событие C – «появление не больше 5 очков». В чем состоит событие $AB - \overline{C}$?

17. Расположите случайные события в порядке возрастания их вероятностей: а) при бросании игральной кости выпало 4 очка; б) при двух бросаниях игральной кости выпало в сумме не менее 3 очков; в) при бросании игральной кости выпало нечетное число очков.

18. Десять лучших спортсменов университета будут участвовать в межуниверситетских соревнованиях по бегу. Сколькими способами можно отобрать: а) 2 человека для участия в соревнованиях по бегу на 100 м; б) 4 человека для участия в эстафете 4 по 100 м; в) 4 человека для участия в эстафете 100 м + 200 м + 400 м + 800 м; г) 3 человека для участия в забеге на 3 км?

19**.** Три стрелка стреляют по цели. Вероятность попадания в цель для первого стрелка равна 0,5, для второго – 0,7, для третьего – 0,9. Найти вероятность p того, что в цель попадет хотя бы один стрелок.

20. Имеется шесть карточек с буквами М, М, И, О, А, З. Найти вероятность того, что случайным образом разложив карточки, мы получим слово мимоза.

21. Закон распределения дискретной случайной величины X задан следующей таблицей:

X	0	1	2	3	4
p	0,13	0,35	0,35	0,15	0,02

Найдите математическое ожидание, дисперсию и среднее квадратическое отклонение.

22. Найдите математическое ожидание случайной величины X и дисперсию, если закон ее распределения задан таблицей:

X	1	2	3	4
p	0,3	0,1	0,2	0,4

к разделу II
«Основы теории информации и криптологии»

Вопросы к экзамену

1. Проблема информации в современной науке.
2. Понятие информации. Информация как свойство объекта.
3. Связь информации с процессами передачи и восприятия.
4. Сигнал как способ проявления информации.
5. Этапы обращения информации: восприятие, подготовка и обработка.
6. Этапы обращения информации: отображение, воздействие, передача и хранение.
7. Автоматизированные информационные системы.
8. Разновидности систем передачи информации.
9. Структурная схема системы передачи информации.
10. Дискретные и непрерывные сообщения. Алфавит источника сообщений.
11. Кодирование и декодирование информации.
12. Модуляция и демодуляция.
13. Понятие линии связи. Помехи. Верность передачи.
14. Уровни проблем передачи информации: синтактический, семантический, прагматический.
15. История возникновения теории информации.
16. Использование идей теории информации. Теоретико-информационный подход.
17. Энтропия как мера неопределенности выбора. Понятие ансамбля.
18. Формула энтропии дискретного источника информации.
19. Свойства энтропии.
20. Объединение ансамблей. Понятие условной энтропии.
21. Свойства условной энтропии.
22. Представление информации в цифровом виде.
23. Арифметические и логические операции в двоичной системе.
24. Системы счисления. Код Грея.

25. Двоично-десятичный код.

26. Криптология как наука. Основная терминология.

27. Этапы развития криптологии.

28. Основные понятия: сообщения, ключи, зашифрованные сообщения.

29. Шифр Цезаря.

30. Шифр простой подстановки.

31. Модулярный шифр.

32. Гомофоническое шифрование.

33. Полиграммное шифрование.

34. Биграммная криптосхема Хилла.

35. Многоалфавитное подстановочное шифрование.

36. Перестановочные шифры.

37. Шифр Вернама.

38. Понятие электронной цифровой подписи.

39. Обобщенная модель электронной цифровой подписи.

40. Свойства односторонней функции с секретом. Подпись. Подписанное сообщение.

41. Общий алгоритм электронной цифровой подписи.

42. Алгоритмы хеширования. Коллизии.

43. Алгоритмы хеширования в базах данных.

44. Метод средних квадратов. Метод деления.

45. Сдвиг разрядов. Анализ отдельных разрядов.

46. Метод складывания. Метод Лина.

47. Общая схема генерации простых чисел.

Задачи к экзамену

1. Вычислите сумму: $3A5B_{16} + 4E7C_{16}$.

2. Вычислите произведение: $35B_{16} * 17C_{16}$.

3. Вычислите сумму: $3257_8 + 4472_8$.

4. Вычислите произведение: $357_8 * 175_8$.

5. Переведите код Грея $10110_{ГР}$ в двоичное число.

6. Переведите двоичное число 10110_2 в код Грея.

7. Переведите десятичное число 2016 в шестнадцатеричное.

8. Переведите десятичное число 2016 в восьмеричное.

9. Переведите десятичное число 2016 в двоичное.

10. Переведите шестнадцатеричное число 2016_{16} в десятичное.

11. Переведите восьмеричное число 2016_8 в десятичное.

12. Переведите ключ записи 234138 в четырехзначный адрес методом деления. В качестве делителя возьмите число 9991.

13. Переведите ключ записи 234138 в четырехзначный адрес методом средних квадратов.

14. Переведите ключ записи 23413834 в четырехзначный адрес методом сдвига разрядов.

15. Переведите ключ записи 23413834 в четырехзначный адрес методом складывания. Переведите ключ записи 234138 в четырехзначный адрес преобразованием в систему счисления с основанием 11.

16. Переведите ключ записи 234138 в четырехзначный адрес методом Лина. Используйте $q^m=97^2$.

17. Используйте гомофоническое шифрование для шифрования слова task.

18. Используйте шифр Плейфера для шифрования слова task. Квадрат с английскими буквами выберите сами.

19. Примените биграммную криптосхему Хилла для шифрования слова task, используя $M = \begin{pmatrix} 2 & 5 \\ 3 & 3 \end{pmatrix}$.

20. Используйте шифр Виженера для шифрования слова task. В качестве ключа возьмите слово keys.

21. Используйте шифр Вернама для шифрования слова task. В качестве ключа возьмите слово keys.

к разделу III
«Медиакультура специалиста»

Вопросы к экзамену

1. Проблема информации в современной науке.
2. Место информации в процессе общественного познания: онтологическое и методологическое понимание.
3. Информация, коммуникация, социальная информация.
4. Информационное общество. Эволюционно-информационные стадии развития человеческой цивилизации.
5. Информационное общество. Основные характеристики. Основные определения, процессы и принципы.
6. Медиа. Мультимедиа. Массмедиа. История и основные понятия.
7. Исследования Маршала Маклюэна о формирующем воздействии электрических и электронных коммуникаций на человека. Media is the message.
8. Медиасреда. Различные подходы к определению понятия. Мультимедиа.
9. Медиавосприятие и развитие аудитории в области медиакультуры: основные понятия и проблемы. Медиаграмотность как показатель развития медиакультуры аудитории.
10. Медиавоздействие – основная функция медиатекста. Медиаманипуляция как форма медиавоздействия.
11. Новые СМИ и аудитория: изменение традиционной модели взаимодействия.
12. Медиакультура (media culture). Медиаграмотность (media literacy). Основные понятия и определения.
13. Медиаобразование (media education). Основные цели и задачи. Основные категории.
14. Место и роль медиасреды и медиаобразования в профессиональной деятельности культуролога.
15. Медиатекст (media text, media construct). Классификация. Примеры. Анализ медиатекста, виды анализа.

16. Медиатекст – результат медиапроизводства. Жанровая структура медиа. Синтез жанров – характерное явление современной медиакультуры. Условность жанровых делений.

17. Медиатекст (текст-очерк, реклама, новости, информационно- аналитические тексты): условное расположение их на шкале сообщение – влияние.

18. Медиавирус. Источники и виды.

19. Мультимедийная информация как профессиональный ресурс культуролога. Общая характеристика медиасреды.

20. Медиасреда: принципы развития по Тоффлеру.

21. Медиасреда как коммуникативное пространство деятельности культуролога. Специфика общения, контакта аудитории с медиасредой. Психолого-педагогические аспекты восприятия мультимедийной информации.

22. Коммуникация: основные определения и виды.

23. Социальная коммуникация. Объекты, цели и формы.

24. Социальная коммуникация. Типы коммуникационной деятельности, примеры.

25. Коммуникация. Модели коммуникации.

26. Социальная коммуникация. Стили коммуникации.

27. Информационные ресурсы социокультурной сферы, технологии их поиска и передачи. Основные характеристики и классификация информационных ресурсов. Текстовые, графические, аудио-, фото- и видеоресурсы. Мультимедийные ресурсы. Определение и сохранение адреса (ссылки) Интернет-ресурса.

28. Информационные ресурсы социокультурной сферы. Основные характеристики и классификация информационных ресурсов. Создание списка аннотированных ссылок профессиональных ресурсов культуролога.

29. Информационные ресурсы социокультурной сферы. Интернет-каталоги тематические (предметные), иерархическая структура материала, встроенная система автоматического поиска по ключевым словам, примеры.

30. Интернет-сообщества как информационный ресурс. Правила регистрации, участия и доступа к медиаресурсам (музы-

кальным, графическим, фото-, видео- и др.) Интернет-сообществ.

31. Сетевые сообщества. Формы Интернет-сообществ (социальные сети, веб-форумы, блоги, вики, чаты, списки рассылки и т. д.). Технологии создания и регулирования деятельности сетевых сообществ. Примеры.

32. Форум. Принципы организации. Правила поведения на форуме. Разграничение доступа. Модератор и администратор: обязанности и функции. Тематика форума. Возможности использования в профессиональной деятельности культуролога. Примеры.

33. Чат. ICQ. Характерные особенности. История организации и развития. Технология организации. Правила организации переписки, поиск пользователей в системе. Возможности использования в профессиональной деятельности культуролога.

34. Блог. История возникновения. Характеристики записей блога. Отличия блога от традиционного дневника. Разновидности блогов. Мотивация участия и функции блогов. Возможности использования в профессиональной деятельности культуролога. Примеры.

35. Вики. Википедия. История. Концепции Википедии. Признаки. Возможности применения в профессиональной деятельности культуролога-менеджера.

36. Рассылки как средство маркетинга и рекламы в профессиональной деятельности культуролога. Сервер списков рассылок. Рассылки электронной почты. Виды рассылок. Список рассылки. Групповой адрес. Информационная и/или рекламная рассылка. Спам, фишинг.

37. Авторское право и информационная безопасность в Интернете. Условия соблюдения авторских прав при использовании информационных ресурсов Интернета. Особенности белорусского правового поля. Элементы специального знака авторского права.

38. Электронные публикации. Правила цитирования электронных источников.

39. Компьютерные среды для работы с медиаприложениями. Браузеры. Программное обеспечение для навигации и просмотра веб-ресурсов. Браузеры, их сравнительные характеристики и возможности. Статистика использования браузеров в Интернете.

40. Медиапроект социально-культурной тематики как способ организации профессиональной деятельности культуролога. Оформление материалов для размещения в Интернете.

Практические задания

1. Медиатекст в виде анимации (GIF и FLASH).
2. Анализ медиатекста по категориям медиа и раскадровка анимации (схематично-описательно).
3. Выступление на семинаре.

Примеры тестовых заданий

Какое расширение файлов является в Adobe Photoshop основным?

1. JPG
2. PSD
3. BMP
4. GIF

Какие графические редакторы вы бы применили для ретуширования и реставрирования фотографий?

1. Векторные
2. Растровые
3. Фрактальные
4. Трехмерные

В модели CMYK при нулевом значении всех компонентов получается ...

1. Белый цвет
2. Черный цвет
3. Коричневый цвет

В каком формате можно сохранить анимацию?

1. JPG
2. PSD
3. BMP
4. GIF
5.CDR
6. FLA

Технология одновременного использования (представления и обработки) информации в различных формах (текст, аудио, изображение и видео, анимация, интерактивное взаимодействие и др.) в едином объекте – «медиатексте» или «медиапродукте».

ОТВЕТ ЗАПИШИТЕ_____

Результатом медиаобразования является ...

1. медиа
2. мультимедиа
3. медиаграмотность
4. диплом

Коммуникант, источник медиатекста (источник воздействия: человек, организация – тот, кто организует коммуникацию)

1. язык
2. агентство
3. аудитория
4. технология
5. категория
6. репрезентация

Спрайтовая анимация реализуется при помощи ...

1. преобразования одного объекта в другой за счет генерации заданного количества промежуточных кадров
2. языка программирования
3. датчиков на теле человека
4. поочередной смены рисунков, каждый из которых нарисован отдельно
5. специальных программ трехмерного моделирования

ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

Теоретические основы информационных технологий : учебная программа учреждения высшего образования по учебной дисциплине для специальности 1–21 04 01 Культурология (по направлениям), направления специальности 1-21 04 01-02 Культурология (прикладная) специализации 1-21 04 01-02 04 Информационные системы в культуре / П. В. Гляков, Т. С. Жилинская, Т. И. Песецкая. – Минск : БГУКИ, 2014. – 24 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ СЕМИНАРОВ

Семинарские занятия предлагается проводить в форме веб-занятий. Веб-занятие – это занятие, осуществляемое с помощью электронных (компьютерных) коммуникаций на базе веб-ресурсов. При проведении веб-занятий используются функциональные возможности чата, блога, форума и других средств коммуникации. Чат-занятия проводятся синхронно, то есть все участники имеют одновременный доступ к чату. Отличительными особенностями использования форума и блога являются возможность более длительной (многодневной) работы и асинхронный характер взаимодействия студента и преподавателя. Для проведения семинара в форме сетевой конференции проводится подготовительная работа в виде рассылок с использованием электронной почты.

Для каждого семинара определена тема, цель, основные понятия, вопросы и литература. Основные понятия помогают ак-

центировать внимание студентов на ключевых аспектах изучаемой темы. Указанная литература помогает студентам при самостоятельной подготовке к семинарским занятиям.

При оценке результатов работы студентов на семинарских занятиях учитываются:

– своевременность подготовки материала;

– точность и полнота подготовленного материала;

– привлечение знаний из других областей;

– умение аргументировать свои заключения, выводы;

– эстетика подготовленного материала;

– использование технических средств для презентации материала.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Для каждой лабораторной работы определена цель, приведены краткие теоретические сведения, акцентирующие внимание на основных вопросах, которые должны быть усвоены при ее выполнении. Формулируется общее задание, затем описывается последовательность выполнения работы с пошаговой детализацией. В конце каждой работы приведены вопросы для самоконтроля, которые помогут студентам самостоятельно проверить уровень усвоения материала, и литература по изучаемой теме. Лабораторные работы по учебной дисциплине «Теоретические основы информационных технологий» выполняются студентами в виде *тематических проектов*.

Отчет о выполнении лабораторной работы должен включать титульный лист, пояснительную записку, печатный и электронный вариант выполненного проекта. В пояснительной записке автор проекта описывает алгоритм и результаты выполнения заданий, делает выводы о возможностях доработки проекта и его использования в профессиональной деятельности культуролога. Защита лабораторной работы заключается в

представлении отчета (с выполненным проектом) и в устных ответах на вопросы по проекту.

При оценке проекта учитываются:

– своевременность сдачи законченного проекта;

– точность и полнота выполнения заданий, указанных в каждой лабораторной работе;

– применение знаний из других областей;

– доказательность принимаемых решений, умение аргументировать свои заключения, делать выводы;

– эстетика оформления проекта и отчета в целом.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Самостоятельная работа студентов направлена на обогащение их умений и навыков по дисциплине «Теоретические основы информационных технологий» в свободное от обязательных учебных занятий время. Цель самостоятельной работы студентов – содействие усвоению в полном объеме содержания учебной дисциплины через систематизацию, планирование и контроль собственной деятельности. Преподаватель дает задания по самостоятельной работе и регулярно проверяет их выполнение.

С учетом содержания, целей и задач дисциплины «Теоретические основы информационных технологий» студентам предлагается осуществлять такие виды самостоятельной работы по дисциплине, как контент-анализ публикаций по использованию информационных технологий в сфере культуры, разработка тематических презентаций, выполнение задач, связанных с использованием информационных технологий.

При изучении дисциплины используются следующие формы самостоятельной работы:

– контролируемая самостоятельная работа в виде решения индивидуальных задач в аудитории во время проведения лабораторных занятий под контролем преподавателя в соответствии с расписанием;

– управляемая самостоятельная работа, в том числе в виде выполнения индивидуальных заданий с консультациями преподавателя;

– подготовка рефератов и презентаций по индивидуальным темам.

Самостоятельная работа студентов ориентирована на изучение отдельных вспомогательных тем дисциплины, решение дополнительных рекомендованных задач и подбор практических примеров, иллюстрирующих теоретические основы информационных технологий. Результаты самостоятельной работы выявляются как при ответах на теоретические вопросы, так и при решении задач. Текущий контроль осуществляется при выполнении и сдаче лабораторных работ.

Оценка уровня знаний студента производится по десятибалльной шкале.

Для оценки достижений студента рекомендуется использовать следующий диагностический инструментарий:

– устный опрос во время практических занятий;

– проведение текущих контрольных работ (заданий) по отдельным темам;

– защита выполненных на практических занятиях индивидуальных заданий;

– защита выполненных в рамках управляемой самостоятельной работы индивидуальных заданий;

– выступление студента на конференции по подготовленному реферату;

– защита индивидуальной работы;

– сдача зачета по дисциплине.

ЛИТЕРАТУРА

к разделу I
«Прикладная математика»

Основная

1. Гляков, П. В. Основы высшей математики / П. В. Гляков, Т. И. Песецкая ; М-во культуры Респ. Беларусь, Белорус. гос. ун-т культуры и искусств. – Минск : БГУКИ, 2012. – 194 с.

2. Жданович, В. Ф. Задания к лабораторным работам по курсу теории вероятностей и математической статистики в двух частях / В. Ф. Жданович, Н. В. Лазакович, Н. Я. Радыно. – Минск : БГУ, 1998. – Ч. 1. – 36 с.

3. Жданович, В. Ф. Задания к лабораторным работам по курсу теории вероятностей и математической статистики в двух частях / В. Ф. Жданович [и др.]. – Минск : БГУ, 1999. – Ч. 2. – 47 с.

4. Критофидес, Н. Теория графов. Алгоритмический подход / Н. Кристофидес. – М. : Мир, 1978. – 432 с.

5. Морозов, А. Д. Введение в теорию фракталов / А. Д. Морозов. – М. ; Ижевск : Ин-т компьютерных исследований, 2002. – 162 с.

6. Нешитой, В. В. Математико-статистические методы анализа в библиотечно-информационной деятельности : учеб.-метод. пособие / В. В. Нешитой. – Минск : Белорус. гос. ун-т культуры и искусств, 2009. – 203 с.

7. Справочник по математике для экономистов / В. Е. Барбаумов [и др.] ; под ред. В. И. Ермакова. – М. : Инфра-М, 2009. – 464 с.

Дополнительная

8. Белько, И. В. Высшая математика для экономистов. I семестр : экспресс-курс / И. В. Белько, К. К. Кузьмич. – М. : Новое знание, 2002. – 140 с.

9. Белько, И. В. Высшая математика для экономистов. II семестр : экспресс-курс / И. В. Белько, К. К. Кузьмич. – М. : Новое знание, 2003. – 88 с.

10. Божокин, С. В. Фракталы и мультифракталы / С. В. Божокин, В. А. Паршин. – Ижевск : НИЦ «Регулярная и хаотическая динамика», 2001. – 128 с.

11. Кирьянов, Д. В. Mathcad 13 / Д. В. Кирьянов. – СПб. : БХВ-Петербург, 2006. – 598 с.

12. Лазакович, Н. В. Теория вероятностей / Н. В. Лазакович, С. П. Сташуленок, О. Л. Яблонский. – Минск : БГУ, 2007. – 311 с.

13. Мельников, О. И. Теория графов в занимательных задачах / О. И. Мельников. – М. : Либрком, 2009. – 232 с.

14. Плис, А. И. MathCAD : математический практикум для экономистов и инженеров / А. И. Плис, Н. А. Сливина. – М. : Финансы и статистика, 2003. – 656 с.

к разделу II
«Основы теории информации и криптологии»

Основная

1. Жельников, В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1996. – 335 с.

2. Коробейников, А. Г. Математические основы криптологии : учеб. пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПбГУ ИТМО, 2004. – 106 с.

3. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

4. Кудряшов, Б. Д. Теория информации : учеб. пособие / Б. Д. Кудряшов. – СПб. : СПбГУ ИТМО, 2010. – 188 с.

5. Об информации, информатизации и защите информации : Закон Респ. Беларусь 10 нояб. 2008 г. № 455-З : принят Палатой представителей 9 окт. 2008 г. : одобр. Советом Респ. 22 окт. 2008 г. [Электронный ресурс]. – Режим доступа: http://www.pravo.by/webnpa/text.asp?start=1&RN=H10800455. – Дата доступа: 10.09.2010.

6. Об электронном документе и электронной цифровой подписи : Закон Респ. Беларусь 28 дек. 2009 г. № 113-З : принят Палатой представителей 4 дек. 2009 г. : одобр. Советом Респ. 11 дек. 2009 г. [Электронный ресурс]. – Режим доступа: http://www.pravo.by/webnpa/text.asp?RN=H10900113. – Дата доступа: 10.09.2010.

7. Фурсов, В. А. Лекции по теории информации : учеб. пособие / В. А. Фурсов / под ред. Н. А. Кузнецова. – Самара : Самар. гос. аэрокосм. ун-т, 2006. – 148 с.

Дополнительная

8. Герасименко, В. А. Основы защиты информации : учеб. пособие / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

9. Клочева, Е. А. Теория информации : учеб. пособие / Е. А. Клочева ; Сыкт. лесн. ин-т. – Сыктывкар : СЛИ, 2013. – 80 с.

10. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы / Д. Кнут. – М. : Вильямс, 2007. – 832 с.

11. Мартин, Дж. Организация баз данных в вычислительных системах / Дж. Мартин. – М. : Мир, 1978. – 616 с.

12. Тарасенко, Ф. П. Введение в курс теории информации / Ф. П. Тарасенко. – Томск : Изд-во ТГУ, 1963. – 240 с.

к разделу III
«Медиакультура специалиста»

Основная

1. Жилинская, Т. С. Медиакультура специалиста : учеб.-метод. пособие / Т. С. Жилинская. – Минск : Белорус. гос. ун-т культуры и искусств, 2011. – 64 с.

2. Кириллова, Н. Б. Медиакультура: от модерна к постмодерну / Н. Б. Кириллова. – М. : Академический проект, 2005. – 448 с.

3. Обручев, В. Adobe After Effects CC. Официальный учебный курс / В. Обручев. – М. : ЭКСМО, 2013. – 432 с.

4. Федоров, А. В. Медиаобразование и медиаграмотность : учеб. пособие для вузов / А. В. Федоров. – Таганрог : Кучма, 2004. – 340 с.

Дополнительная

5. Брайант, Дж. Основы воздействия СМИ / Дж. Брайант, С. Томпсон ; пер. с англ. – М. : Вильямс, 2004 – 432 с.

6. Вебер, Л. Эффективный маркетинг в Интернете. Социальные сети, блоги, Twitter и другие инструменты продвижения в Сети / Л. Вебер. – М. : Манн, Иванов и Фербер, 2010. – 320 с.

7. Гундарина, Е. Корпоративный блог / Е. Гундарина, М. Гундарин. – СПб. : Феникс, 2013. – 160 с.

8. Иванов, А. Идеальный поиск в Интернете глазами пользователя / А. Иванов, И. Ашманов. – СПб. : Питер, 2011. – 208 с.

9. Кирьянов, Д. В. Самоучитель Adobe After Effects CS3 / Д. Кирьянов, Е. Кирьянова. – СПб. : БХВ–Петербург, 2008. – 364 с.

10. Костина, А. Интернет-сообщества. Что обсуждается в Интернете? От думеров – до фурри. От игнора – до троллинга / А. Костина. – СПб. : Питер, 2011. – 176 с.

11. Кремнев, Д. Продвижение в социальных сетях / Д. Кремнев. – СПб. : Питер, 2011. – 160 с.

12. Пташинский, В. С. Видеоэффекты и анимация в Adobe After Effects CS3 / В. С. Пташинский [и др.] . – СПб. : Питер Пресс, 2008. – 254 с.

13. Ульрих, Е. Интерактивная Web-анимация во Flash / Е. Ульрих. – М. : ДМК Пресс, 2009. – 568 с.

13. Федоров, А. В. Медиаобразование: история, теория и методика / А. В. Федоров. – Ростов : ЦВВР, 2001. – 708 с.

14. Хассей, Т. WordPress. Создание сайтов для начинающих / Т. Хассей. – М. : ЭКСМО, 2012. – 432 с.

15. Шарков, Ф. И. Коммуникология. Социология массовой коммуникации / Ф. И. Шарков. – М. : Дашков и Ко, 2013. – 320 с.

Рекомендуется использовать следующие электронные ресурсы:

http://www.edu.of.ru/mediaeducation – электронный ресурс по медиаобразованию.

http://www.psyfactor.org/lybr.htm – материалы психологической и общегуманитарной тематики (медиавоздействие, медиаманипуляции).

http://www.britannica.com – энциклопедия Britannica.

http://www.ifap.ru – программа ЮНЕСКО «Информация для всех».

http://www.mediagram.ru – электронный ресурс по медиаграмотности.

http://uroki-flash-as3.ru – уроки по ActionScript 3.0.

http://www.render.ru – ресурс по 3D графике и анимации.

Учебное издание

С о с т а в и т е л и :
Гляков Петр Владимирович,
Жилинская Татьяна Степановна,
Песецкая Татьяна Ивановна

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебно-методический комплекс

Редактор Е. А. Добрицкая
Технический редактор Л. Н. Мельник
Дизайн обложки А. И. Пармон

Подписано в печать 2017. Формат 60x84 $^{1}/_{16}$.
Бумага офисная. Ризография.
Усл. печ. л. 18,50. Уч.-изд. л. 10,61. Тираж 50 экз. Заказ .

Издатель и полиграфическое исполнение:
учреждение образования
«Белорусский государственный университет культуры и искусств».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/177 от 12.02.2014.
ЛП № 02330/456 от 23.01.2014.
Ул. Рабкоровская, 17, 220007, г. Минск.