ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Основные понятия и определения теории информации

При взаимодействии сигналов с физическими телами возникают изменения свойств.

Это явление называется ***регистрацией*** сигналов.

Зарегистрированные сигналы называют ***данными***.

Наиболее распространены следующие определения информации:

Информация – это совокупность сведений, подлежащих хранению, передаче, обработке и использованию в человеческой деятельности.

Информация – это данные и методы их обрабатывающие**.**

Информация – это продукт взаимодействия данных и адекватных им методов преобразования данных**.**

Основные понятия и определения

Кодирование - это преобразование сообщений в сигнал, т.е. преобразование сообщений в кодовые комбинации.

Код - система соответствия между элементами сообщений и кодовыми комбинациями.

Кодер - устройство, осуществляющее кодирование.

Декодер - устройство, осуществляющее обратную операцию, т.е. преобразование кодовой комбинации в сообщение.

Алфавит - множество возможных элементов кода, т.е. элементарных символов (кодовых символов) $X = \{x_i\}$, где $i = 1, 2, \ldots, m$.

Задачи теории информации и кодирования

К теории информации относят результаты решения ряда фундаментальных теоретических вопросов:

-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.

Теория кодирования - *раздел теории информации, связанный с задачами кодирования и декодирования сообщений, поступающих к потребителям и посылаемых из источников информации.*

Цели Кодирования

1) Повышение эффективности передачи данных, за счет достижения максимальной скорости передачи данных.

-> ***Теория экономичного (эффективного, оптимального) кодирования*** занимается поиском кодов, позволяющих в каналах без помех повысить эффективность передачи информации за счет устранения избыточности источника и наилучшего согласования скорости передачи данных с пропускной способностью канала связи.

2) Повышение помехоустойчивости при передаче данных.

-> ***Теория помехоустойчивого кодирования*** занимается поиском кодов, повышающих достоверность передачи информации в каналах с помехами.

Виды информации

По признаку *«область возникновения»* информация делится на:

♦ элементарную — отражает процессы и явления неодушевленной природы;

♦ биологическую — отражает процессы растительного и животного мира;

♦ социальную — отражает процессы человеческого общества.

По способу передачи и восприятия различают информацию:

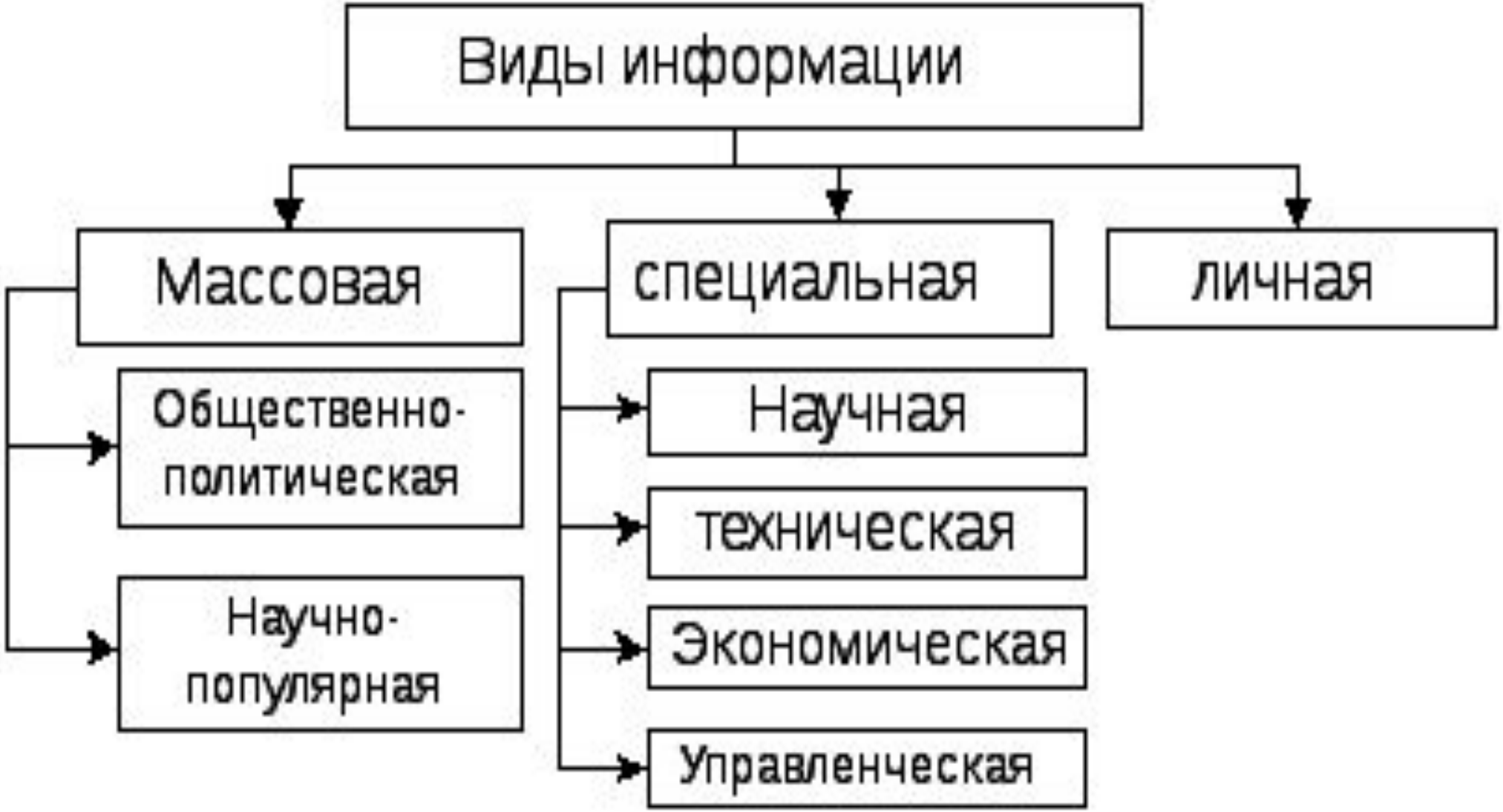
♦ визуальную — передается видимыми образами и символами;

♦ аудиальную — передается звуками;

♦ тактильную — передается ощущениями;

♦ органо-лептическую — передается запахами и вкусом;

♦ машинную — выдаваемую и воспринимаемую средствами вычислительной техники.


Виды информации
Массовая
специальная
личная
Общественно-политическая
Научно-популярная
Научная
техническая
Экономическая
Управленческая

Свойства информации

- *полезность*;
- *полнота;*
- *достоверность*;
- *новизна, актуальность*;
- *ценность*;
- *ясность;*
- *защищенность.*

Качество информации

- Репрезентативность;
- Содержательность;
- Достаточность;
- Доступность;
- Актуальность;
- Своевременность;
- Точность;
- Достоверность;
- Устойчивость.

Этапы обращения информации в автоматизированных системах

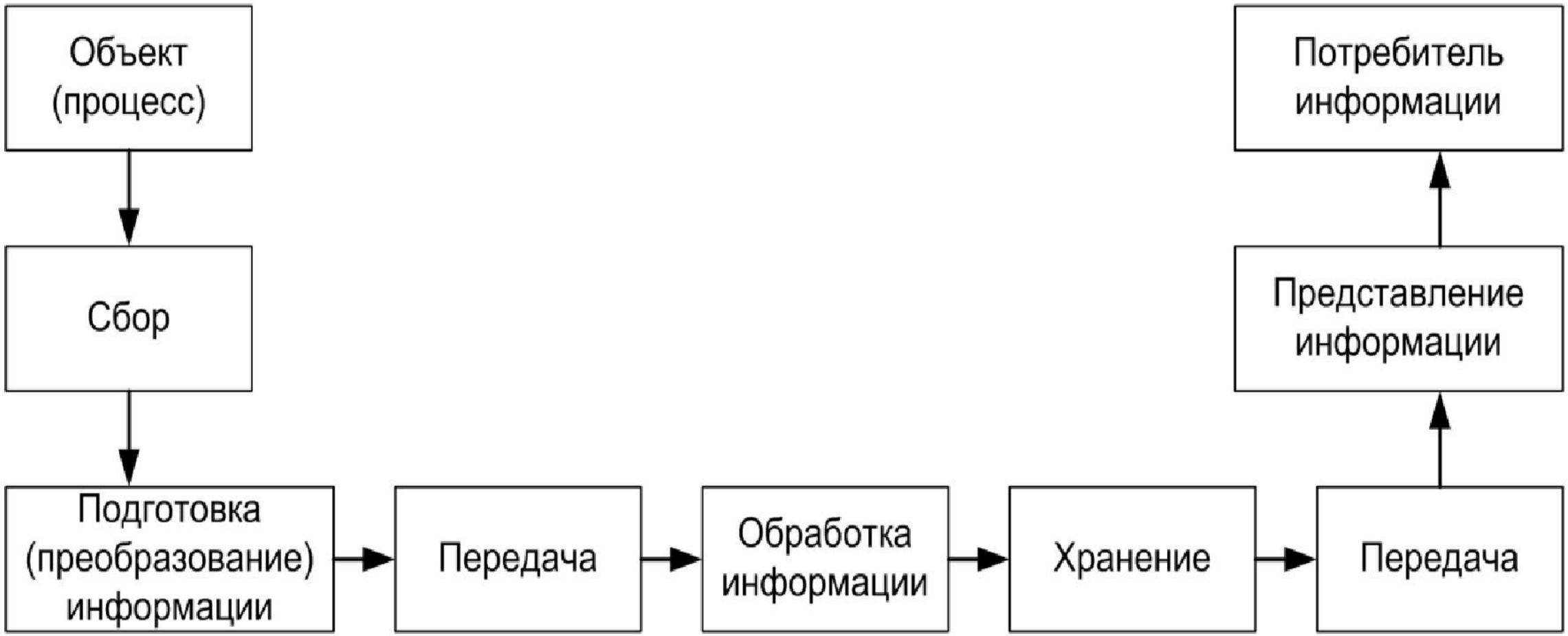
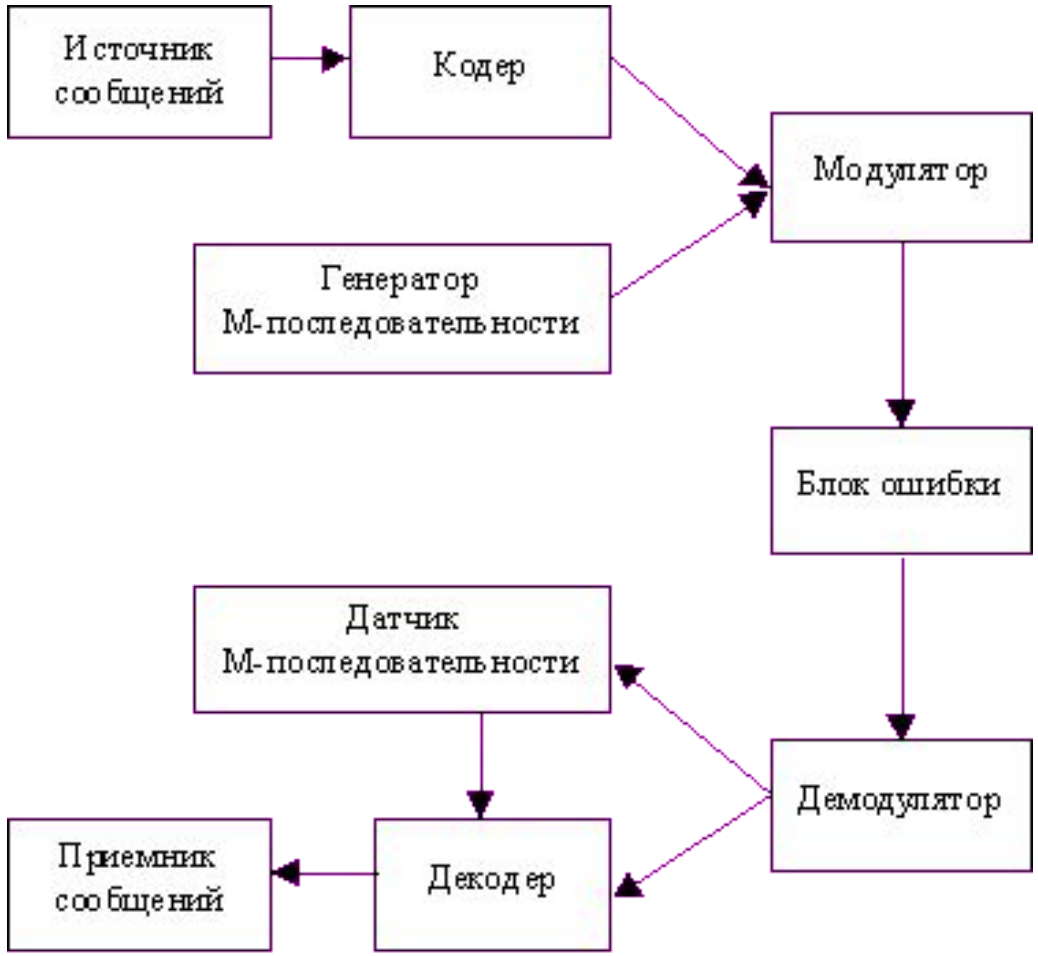


Схема системы передачи информации

Модель системы передачи дискретной информации



Фиг.1

Методы и модели оценки количества информации

- структурные (объёмные);
  - ***Геометрическая;***
  - ***Комбинаторная;***
  - ***Аддитивная;***
- энтропийный (статистический);
- алгоритмический.

Геометрическая мера информации

предполагает измерение параметра геометрической модели информационного сообщения (длины, площади, объема и т. п.) в дискретных единицах.

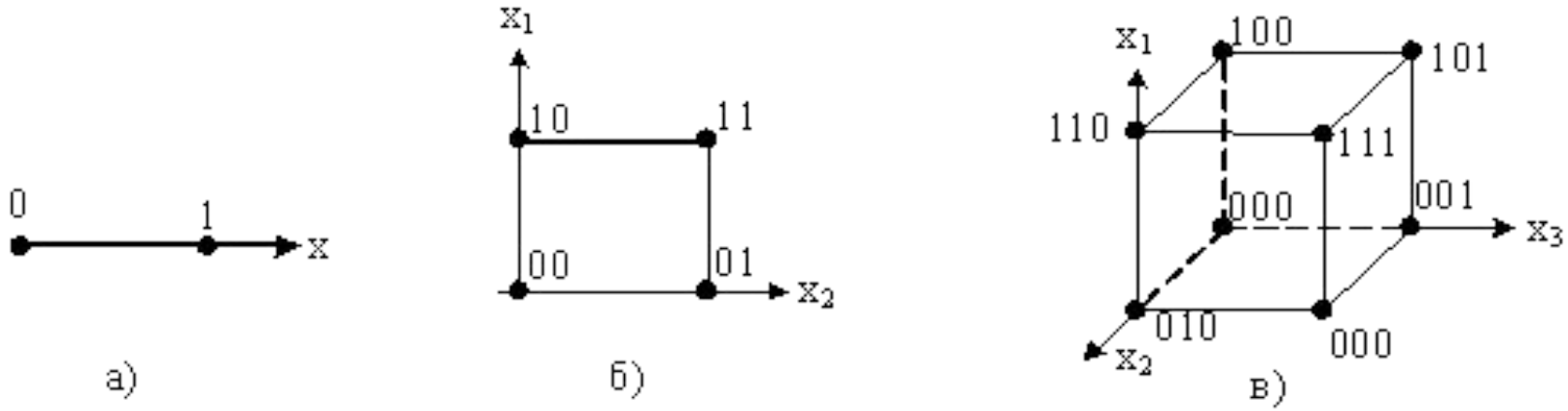


Рис. 1.1.

В комбинаторной мере количество информации вычисляется как количество различных комбинаций элементов, содержащихся в сообщении.

$L=m^n$

m- число элементов алфавита, n – число элементов в сообщении

Количество информации по Хартли определяется по формуле

$$I = l \log_2 h \ [\text{бит}],$$

где *h* - основание системы счисления (количество состояний, которое может принимать элемент, хранящий данное число);

l - число элементов.

Десятичная приставка (СИ)				Двоичная приставка		
Множитель		Обозначение		Множитель		
значение (вес)	название	англо-язычное	русско-язычное	значение (вес)	обозначение	название
10^3	кило	k	к	2^{10}	KiB	киби
10^6	мега	M	М	2^{20}	MiB	меби
10^9	гига	G	Г	2^{30}	GiB	гиби
10^{12}	тера	T	Т	2^{40}	TiB	теби
10^{15}	пета	P	П	2^{50}	PiB	пеби
10^{18}	экза	E	Е	2^{60}	EiB	экзби
10^{21}	зетта	Z	З	2^{70}	ZiB	зеби
10^{24}	йотта	Y	Й	2^{80}	YiB	йоби

$$H(x) = -\sum_{i=1}^{n} p(i) \log_2 p(i).$$

$$\log_2 \frac{1}{p(i)}$$

$$C = F \cdot \log\left(1 + \frac{P_s}{P_n}\right) = F \cdot \log\left(1 + \frac{P_s}{N_0 F}\right),$$

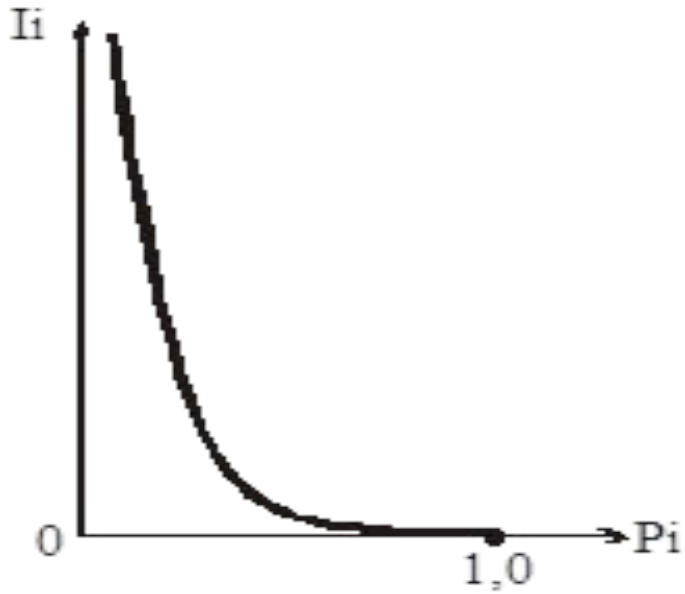


Рис. 1.2.

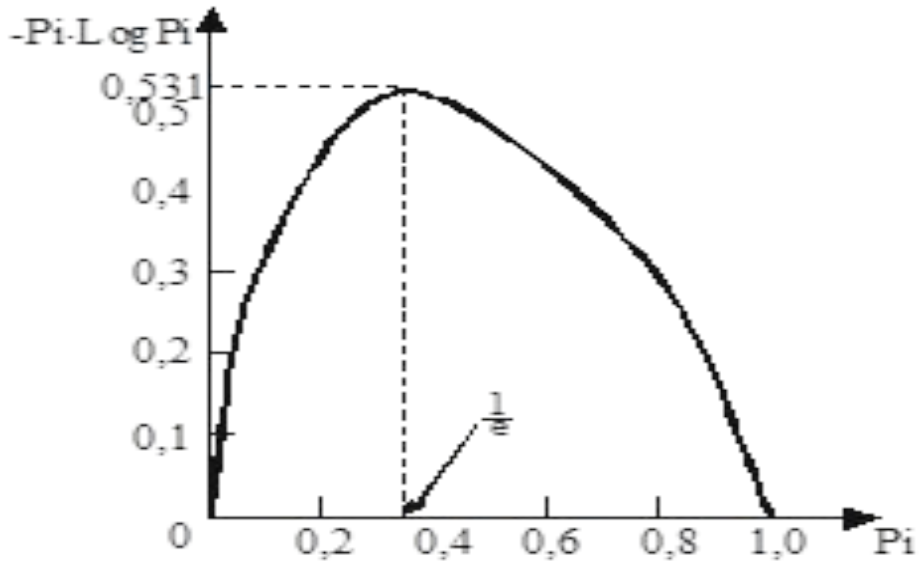


Рис. 1.3.

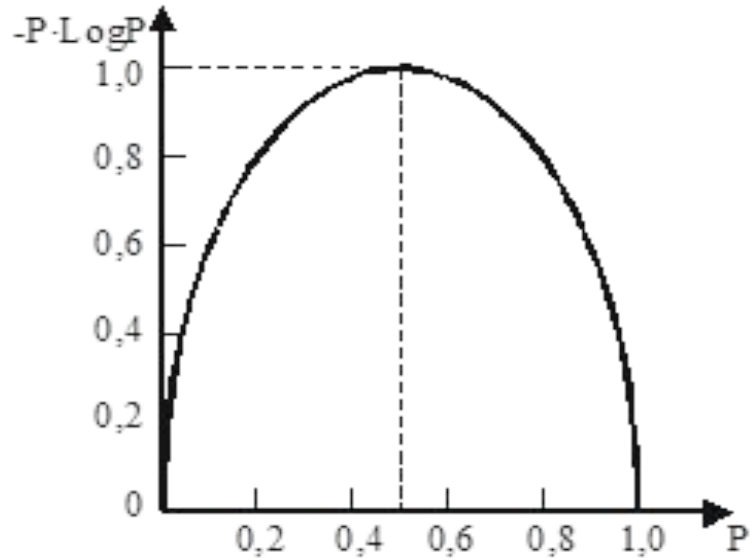
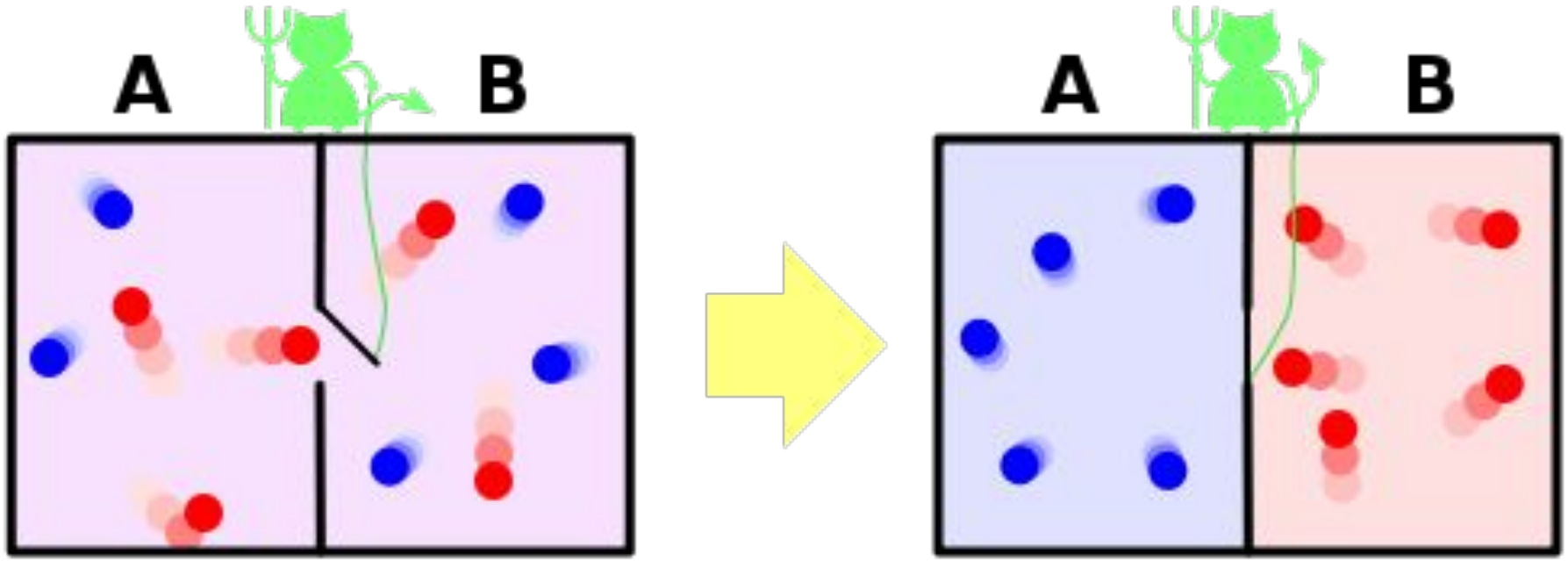


Рис. 1.4.

Схематическое изображение демона Максвелла



Буква p_i	(-) 0,175	О 0,090	Е, Ё 0,072	А 0,062	И 0,062	Т 0,053	Н 0,053	С 0,045
Буква p_i	Р 0,040	В 0,038	Л 0,035	К 0,028	М 0,026	Д 0,025	П 0,023	У 0,021
Буква p_i	Я 0,018	Ы 0,016	З 0,016	Ь, Ъ 0,014	Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Буква p_i	Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006	Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002