Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Теоретической и прикладной математики

Лабораторная работа № 1

по дисциплине «ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИИ КРИПТОГРАФИИ»

ОСНОВНЫЕ АСПЕКТЫ ТЕОРИИ ИНФОРМАЦИИ

Факультет:	ПМИ
Группа:	ПМИ-02
Вариант:	7
Студент:	Сидоров Даниил,
	Дюков Богдан
Преподаватель:	Авдеенко Татьяна Владимировна,
	Сивак Мария Алексеевна.

Новосибирск

2026

Цель работы

Приобретение навыков решения практических задач, отражающих основные свойства источников дискретных сообщений (ИДС).

Задача №1

По двоичному каналу с шумом передаются сообщения x_1, x_2, x_3 с вероятностями 0.2, 0.3 и 0.5. На выходе канала появляются сигналы y_1, y_2, y_3. Вероятности искажения в канале (условные вероятности переходов) заданы в таблице:

$P(y_i \mid x_j)$	x_1	x_2	x_3
y_1	$\frac{3}{4}$	$\frac{1}{8}$	$\frac{1}{8}$
y_2	$\frac{1}{8}$	$\frac{3}{4}$	$\frac{1}{8}$
y_3	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{3}{4}$

Вычислить взаимные информации $I(x_1; y_3)$ и $I(x_3; y_1)$.

Решение:

По определению **взаимной информации**, количество информации символа сообщения x_j, доставляемое символом y_k, можно определить как логарифм отношения апостериорной вероятности к априорной:

$$I(x_j; y_k) = \log \frac{P(x_j \mid y_k)}{P(x_j)};$$

Найдем взаимные информации:

$$I(x_1; y_3) = \log \frac{P(x_1 \mid y_3)}{P(x_1)} = \log \frac{\frac{1}{8}}{0.2} = -0.204 \text{ бит};$$

$$I(x_3; y_1) = \log\frac{P(x_3 | y_1)}{P(x_3)} = \log\frac{\frac{1}{8}}{0.5} = -0.602 \text{ бит.}$$

Ответ: -0.204 бит, -0.602 бит.

Задача №2

По дискретному каналу передаются сообщения x_1 и x_2. Вследствие шумов на выходе канала появляются сигналы y_1, y_2, y_3. Вероятности их совместного появления $P(x_i, y_j)$:

$P(x_i, y_j)$	y_1	y_2	y_3
x_1	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{8}$
x_2	$\frac{1}{8}$	$\frac{3}{16}$	$\frac{1}{4}$

Необходимо найти взаимную информацию $I(X; y_1)$.

Решение:

Информация, содержащаяся в реализации y_k принятого сигнала относительно ансамбля передаваемых сообщений X, определяется следующей формулой:

$$I(X; y_k) = \sum_{j=1}^{n} P(x_j \mid y_k)\, I(x_j; y_k),$$

$$\text{где } P(x_j \mid y_k) = \frac{P(x_j;\, y_k)}{P(y_k)},\ \ I(x_j; y_k) = \log\frac{P(x_j \mid y_k)}{P(x_j)},$$

$$P(x_j) = \sum_{i=1}^{3} P(x_j; y_k),\quad P(y_k) = \sum_{i=1}^{2} P(y_k; x_i).$$

Найдем вероятности сообщений x_1 и x_2:

$$P(x_1) = \sum_{i=1}^{3} P(x_1; y_i) = \frac{1}{4} + \frac{1}{16} + \frac{1}{8} = \frac{7}{16};$$

$$P(x_2) = \sum_{i=1}^{3} P(x_2; y_i) = \frac{1}{8} + \frac{3}{16} + \frac{1}{4} = \frac{9}{16};$$

Найдем вероятность сигнала y_1:

$$P(y_1) = \sum_{i=1}^{2} P(y_1; x_i) = \frac{1}{4} + \frac{1}{8} = \frac{3}{8};$$

Найдем взаимную информацию:

$$I(X; y_1) = \sum_{j=1}^{2} P(x_j \mid y_1)\, I(x_j; y_1) = P(x_1 \mid y_1) I(x_1; y_1) + P(x_2 \mid y_1) I(x_2; y_1)$$

$$= \frac{P(x_1;\, y_1)}{P(y_1)} \log \frac{\frac{P(x_1;\, y_1)}{P(y_1)}}{P(x_1)} + \frac{P(x_2;\, y_1)}{P(y_1)} \log \frac{\frac{P(x_2;\, y_1)}{P(y_1)}}{P(x_2)} = \frac{2}{3} \log \frac{32}{21} + \frac{1}{3} \log \frac{16}{27}$$

$= 0.046$ *бит.*

Ответ: 0.046 бит.

Задача №3

Вероятности появления символов сообщения X:

Вариант	$P(x_1)$	$P(x_2)$	$P(x_3)$	$P(x_4)$	$P(x_5)$
7	0.1	0.2	0.3	0.1	0.3

Сигнал Y является последовательностью двоичных символов, связанных с сообщением X по следующему правилу:

Вариант	$x_1 \rightarrow$	$x_2 \rightarrow$	$x_3 \rightarrow$	$x_4 \rightarrow$	$x_5 \rightarrow$
7	0	0	00	1	1

Найти средние безусловную и условную энтропии сообщения X при условии, что было получено сообщение Y.

Решение:

Безусловная энтропия вычисляется по формуле:

$$H(\xi) = -\sum_{i=1}^{n} P(x_i)\, log\, P(x_i)\,;$$

Для нашего случая:

$$H = -\sum_{i=1}^{5} P(x_i) \log_2 P(x_i) = 2 \cdot 0.1 \cdot 3.322 + 0.2 \cdot 2.322 + 2 \cdot 0.3 \cdot 1.737 = \\ = 2.171 \text{ бит.}$$

Средняя **условная энтропия** вычисляется по формуле:

$$H(X \mid Y) = \sum_{j=1}^{n} P(y_j) H(X \mid y_j),$$

где $P(y_j) = \sum_{k=1}^{n} P(x_k) \cdot P(y_j \mid x_k)$ – полная вероятность,

$H(X \mid y_j) = \sum_{i=1}^{n} P(x_i \mid y_j) \cdot \log_2 \frac{1}{P(x_i \mid y_j)}$ – отдельно взятая энтропия,

$P(x_i \mid y_j) = \frac{P(x_i) \cdot P(y_j \mid x_i)}{P(y_j)}$ – формула Байеса.

Обозначив $y_1 = 0,\ y_2 = 00,\ y_3 = 1$, найдем условные и безусловные вероятности сигнала:

$$P(y_1 \mid x_1) = P(y_1 \mid x_2) = 1, \quad P(y_1 \mid x_3) = P(y_1 \mid x_4) = P(y_1 \mid x_5) = 0;$$
$$P(y_2 \mid x_3) = 1, \quad P(y_2|x_1) = P(y_2|x_2) = P(y_2|x_4) = P(y_2|x_5) = 0;$$
$$P(y_3 \mid x_4) = P(y_3 \mid x_5) = 1 \quad P(y_3 \mid x_1) = P(y_3 \mid x_2) = P(y_3 \mid x_3) = 0;$$

$$P(y_1) = \sum_{k=1}^{5} P(x_k) \cdot P(y_1 \mid x_k) = 0.1 \cdot 1 + 0.2 \cdot 1 = 0.3;$$

$$P(y_2) = \sum_{k=1}^{5} P(x_k) \cdot P(y_2 \mid x_k) = 0.3 \cdot 1 = 0.3\ ;$$

$$P(y_3) = \sum_{k=1}^{5} P(x_k) \cdot P(y_3 \mid x_k) = 0.1 \cdot 1 + 0.3 \cdot 1 = 0.4;$$

$$H(X \mid y_1) = \sum_{i=1}^{n} \frac{P(x_i) \cdot P(y_1 \mid x_i)}{P(y_1)} \cdot \log_2 \frac{P(y_1)}{P(x_i) \cdot P(y_1 \mid x_i)} = \frac{0.1 \cdot 1}{0.3} \log_2 \frac{0.3}{0.1 \cdot 1} +$$
$$+ \frac{0.2 \cdot 1}{0.3} \log_2 \frac{0.3}{0.2 \cdot 1} = 0.918;$$

$$H(X, y_2) = \frac{0.3 \cdot 1}{0.3} \log_2 \frac{0.3}{0.3 \cdot 1} = 0;$$

$$H(X, y_3) = \frac{0.1 \cdot 1}{0.3} \log_2 \frac{0.3}{0.1 \cdot 1} + \frac{0.3 \cdot 1}{0.3} \log_2 \frac{0.3}{0.3 \cdot 1} = 0.528;$$

Найдем среднюю условную энтропию:

$$H(X \mid Y) = 0.3 \cdot \ 0.918 + 0.3 \cdot 0 + 0.4 \cdot 0.528 = 0.487 \text{ бит.}$$

Ответ: 0.487 бит.