|  |  |  |
| --- | --- | --- |
| 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 | | |
| 2022 | | |

**Цель р****а****боты**

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

**З****адача №1**

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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Вычислить взаимные информации и .

**Решение:**

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

Найдем взаимные информации:

**Ответ:** .

**Задача №2**

По дискретному каналу передаются сообщения . Вследствие шумов на выходе канала появляются сигналы . Вероятности их совместного появления:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Необходимо найти взаимную информацию .

**Решение:**

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

Найдем вероятности сообщений :

Найдем вероятность сигнала :

Найдем взаимную информацию:

*бит.*

**Ответ:** .

**Задача №3**

Вероятности появления символов сообщения Х:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант |  |  |  |  |  |
| 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 |  |  |  |  |  |
| 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:

Для нашего случая:

Средняя **условная энтропия** вычисляется по формуле:

Обозначив , найдем условные и безусловные вероятности сигнала:

*;*

Найдем среднююусловную энтропию:

**Ответ:**