НИЯУ «МИФИ»

Кафедра №42 «Криптология и Кибербезопасность»

Защита информации от утечки по скрытым каналам

**Домашнее задание №1. Оценка пропускной способности скрытых каналов.**

*Ст. группы Б17-505*

*Герасимов Федор*

Дан скрытый канал, передающий N символов. На передачу символа «i» требуется i секунд (к примеру, на передачу символа «1» требуется 1 секунда, на передачу символа «2» требуется 2 секунды, и так далее).

**Случай 1: Канал без ошибок, =1/N**

Для оценки пропускной способности воспользуемся методом основанном на оценке взаимной информации случайных величин X и Y, описывающих входные и выходные характеристики скрытого канала соответственно. Формула расчёта пропускной способности, следующая:

τ — среднее время передачи одного пакета, а взаимная информация случайных величин X и Y оценивается согласно формуле:

Однако в данном случае канал без ошибок, поэтому Н(𝑌|𝑋) = 0, следовательно:

Энтропия H(Y) рассчитывается по формуле:

Среднее время передачи 1 пакета:

Таким образом для

*i = 1:*

= 0

*i = 2:*

= 0,67

*i = 3:*

= 0.792

И так далее. будет расти до некоторого предела, после которого происходит перегиб и снижение пропускной способности.

На языке Python формула была автоматизирована:

def bandwidth(n):  
 t = (n + 1) / 2  
 h = 0  
 for n\_tmp in range(1, n + 1):  
 h += ((1 / n) \* math.log2(1 / n)) \* (-1)  
 banw = h/t  
 return banw

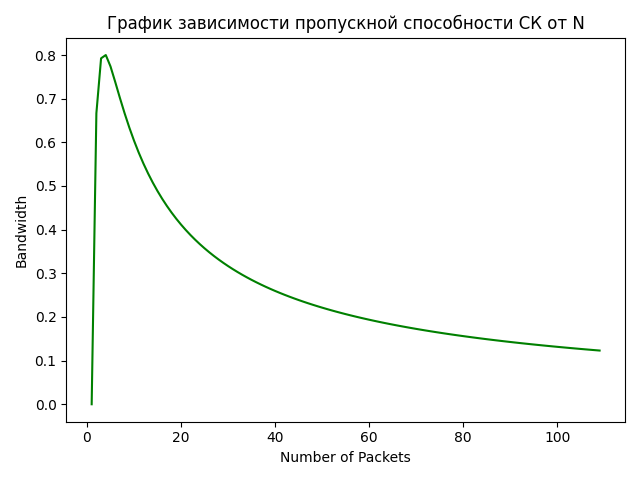
С ее помощью было найдено:

***Максимальная пропускная способность = 0.8***

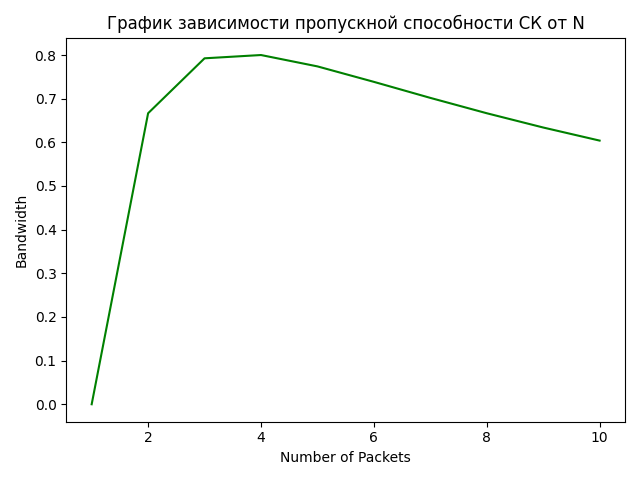
***Число пакетов = 4.***

График зависимости пропускной способности от числа передаваемых символов:

1. Для N = 100



1. Для N = 10



**Случай 2: Канал с ошибками.**

В этом случае  где H(Y|X) = .

Согласно условию, каждый символ можно спутать только с соседними (с предыдущим 0.2, с самим собой 0.6 и со следующим 0.2). В остальных случаях будет как в канале без ошибок - равновероятно.

Таким образом:

if i == j:  
 h\_ex += 0.6 \* math.log2(0.6) \* (-1)  
elif i == (j - 1) or i == (j + 1):  
 h\_ex += 0.2 \* math.log2(0.2) \* (-1)  
else:  
 h\_ex += (1/i) \* math.log2(1/i) \* (-1)

Полная функция расчёта пропускной способности имеет следующий вид:

def bandwidth\_with\_errors(n):  
 t = (n + 1) / 2  
 h = 0  
 for i in range(1, n + 1):  
 h\_y\_x = 0  
 for j in range(1, n + 1):  
 h\_ex = 0  
 if i == j:  
 h\_ex += 0.6 \* math.log2(0.6) \* (-1)  
 elif i == (j - 1) or i == (j + 1):  
 h\_ex += 0.2 \* math.log2(0.2) \* (-1)  
 else:  
 h\_ex += (1/i) \* math.log2(1/i) \* (-1)  
 h\_y\_x = (-1) \* (1/j) \* h\_ex  
 h += ((1 / n) \* math.log2(1 / n)) \* (-1) - h\_y\_x  
 banw = h / t  
 return banw

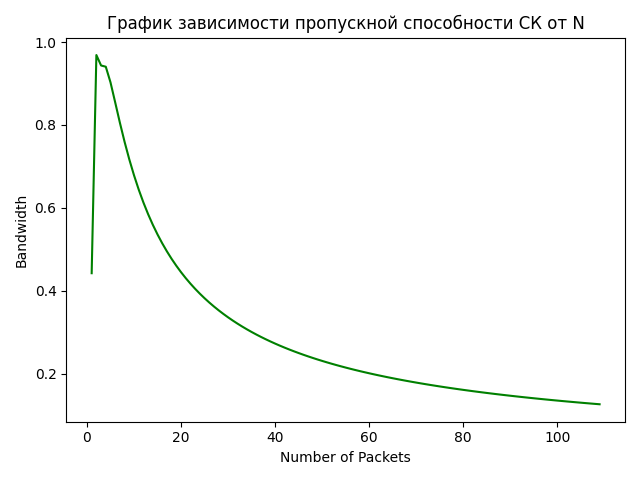
В результате получено:

***Максимальная пропускная способность = 0.9688549918257321***

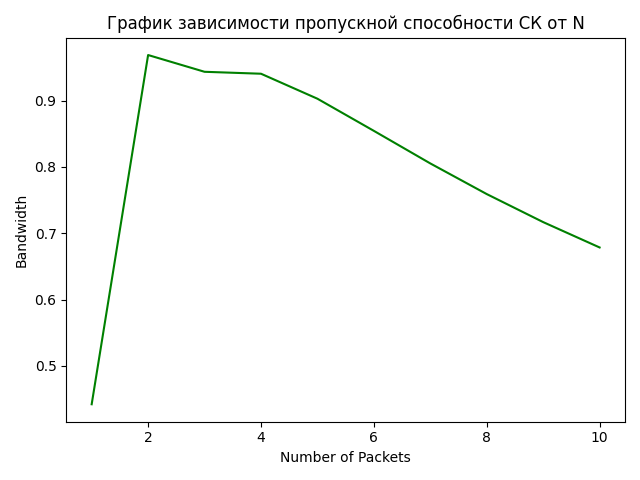
***Число пакетов = 2***

Графики:

1. Для N=110



1. Для N=10



**Случай 3: Канал без ошибок**

В данном случае все вычисления совпадают с пунктом А, однако формула для расчета энтропии выглядит следующим образом:

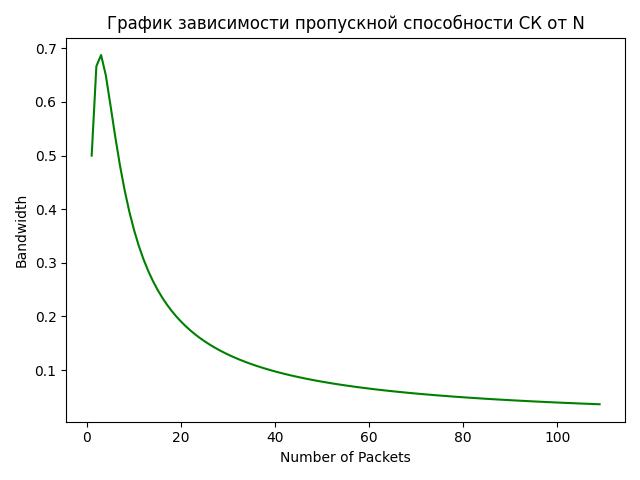
В функции расчёта пропускной способности из случая один заменим формулу и получим результат.

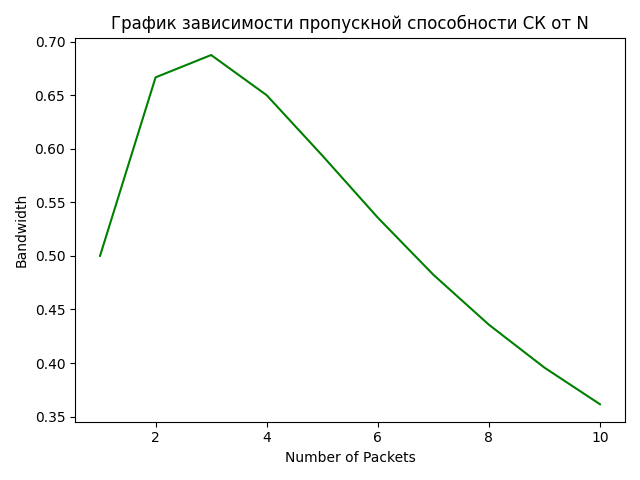
def bandwidth(n):  
 t = (n + 1) / 2  
 h = 0  
 for i in range(1, n + 1):h += ((1 / 2 \*\* i) \* math.log2(1 / 2 \*\* i)) \* (-1)  
 banw = h/t  
 return banw

***Максимальная пропускная способность = 0.6875.***

***Число пакетов = 3.***

Графики для N=100 и N=10 соответсвенно:





**Заключение**

В ходе выполнения практической работы были получены навыки расчета пропускной способности каналов с ошибками и без ошибок с использованием подхода, основанном на оценке взаимной информации случайных величин, описывающих входные и выходные характеристики скрытого канала.

Были получены результаты расчётов для трех случаев:

1. *Случай 1: Канал без ошибок с одинаковой вероятностью входных символов*

* Максимальная пропускная способность = 0.8
* Число пакетов = 4.

1. *Случай 2: Канал с ошибками*

* Максимальная пропускная способность = 0.9688549918257321
* Число пакетов = 2

1. *Случай 3: Канал без ошибок*

* Максимальная пропускная способность = 0.6875.
* Число пакетов = 3.

На основе полученных результатов сделан вывод о том, что максимальная пропускная способность достигается при малой длине сообщения, а канал с ошибками имеет наивысшую пропускную способность на сообщении длины 2 за счет граничного условия.

**Приложение**

Код программы для расчёта пропускной способности и построения графика зависимости пропускной способности скрытого канала от N.

import math  
import matplotlib.pyplot as plt  
  
bw = 0  
n\_final = 0  
  
bw\_array = []  
n\_array = []  
  
  
def bandwidth(n):  
 t = (n + 1) / 2  
 h = 0  
 for n\_tmp in range(1, n + 1):  
 h += ((1 / n) \* math.log2(1 / n)) \* (-1)  
 banw = h/t  
 return banw  
  
  
for n in range(1, 110):  
 bw\_tmp = bandwidth(n)  
 if bw\_tmp > bw:  
 bw = bw\_tmp  
 n\_final = n  
 bw\_array.append(bw\_tmp)  
 n\_array.append(n)  
  
print(bw)  
print(n\_final)