Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 16»**

“ СОГЛАСОВАНИЕ КРИПТОГРАФИЧЕСКИХ

КЛЮЧЕЙ НА ОСНОВЕ ТЕХНОЛОГИЙ

ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Сапегина Екатерина Игоревна,

Вариант 11 (1)

Минск 2023

***Цель:*** изучение основ построения и функционирования искусственных нейронных сетей (ИНС), а также использования ИНС в криптографии; приобретение практических навыков программной реализации алгоритма согласования ключевой информации на основе технологии ИНС.

***Задачи:***

1. Закрепить теоретические знания по основам построения и функционирования ИНС.

2. Усвоить особенности построения, основные алгоритмы взаимного обучения двух связанных нейронных сетей на основе модели ТРМ.

3. Разработать приложение для реализации модели ТРМ с целью согласования двумя сторонами совместного тайного ключа.

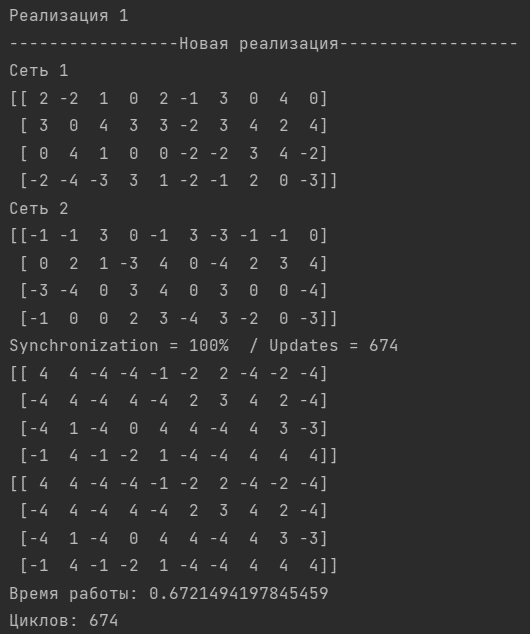
4. Познакомиться с методиками оценки криптостойкости алгоритма на основе ТРМ.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

***Практическая часть:***

Приложение, реализующее модель TCP.

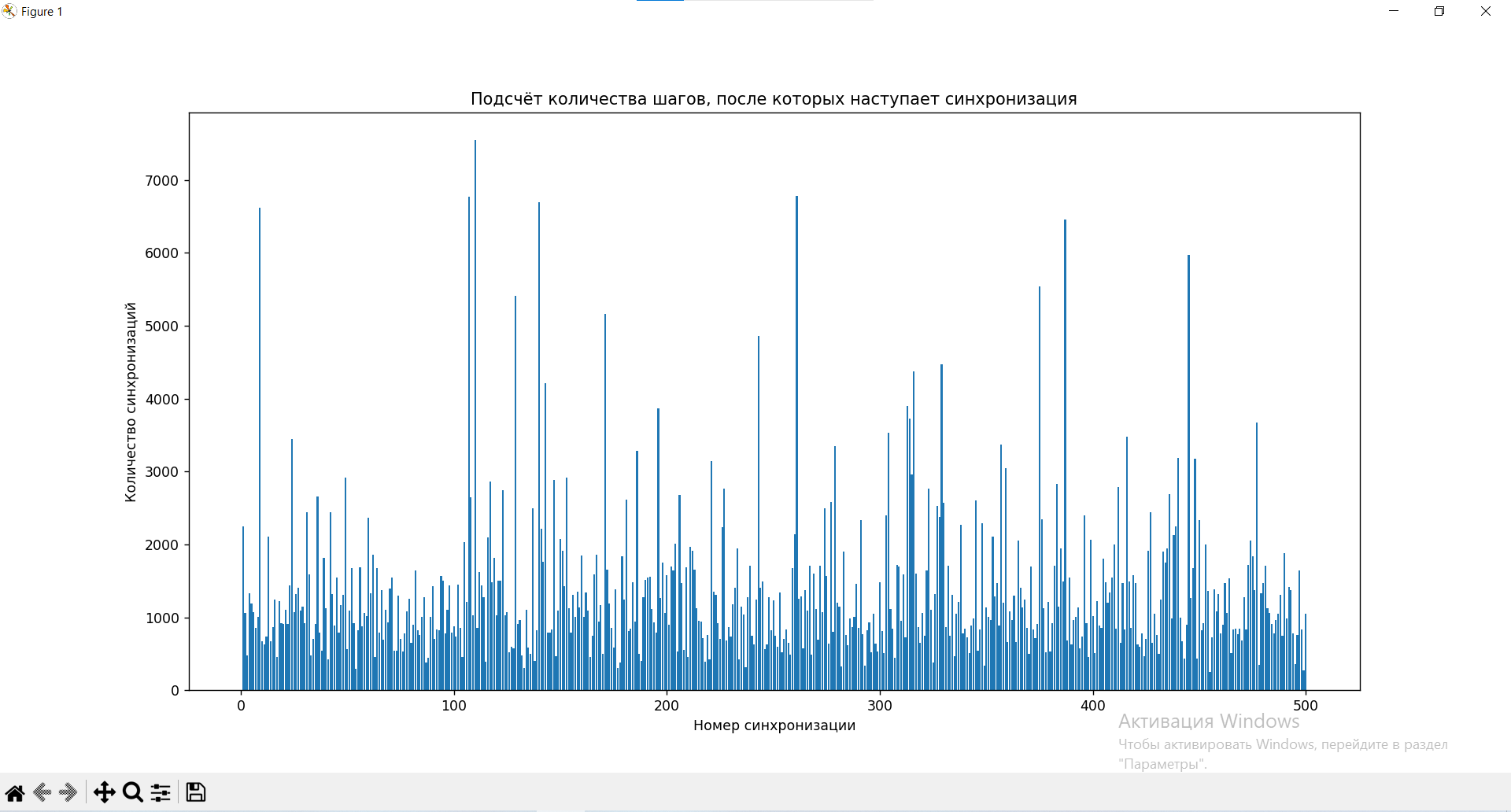
Вывод одной реализации алгоритма для двух сетей:.



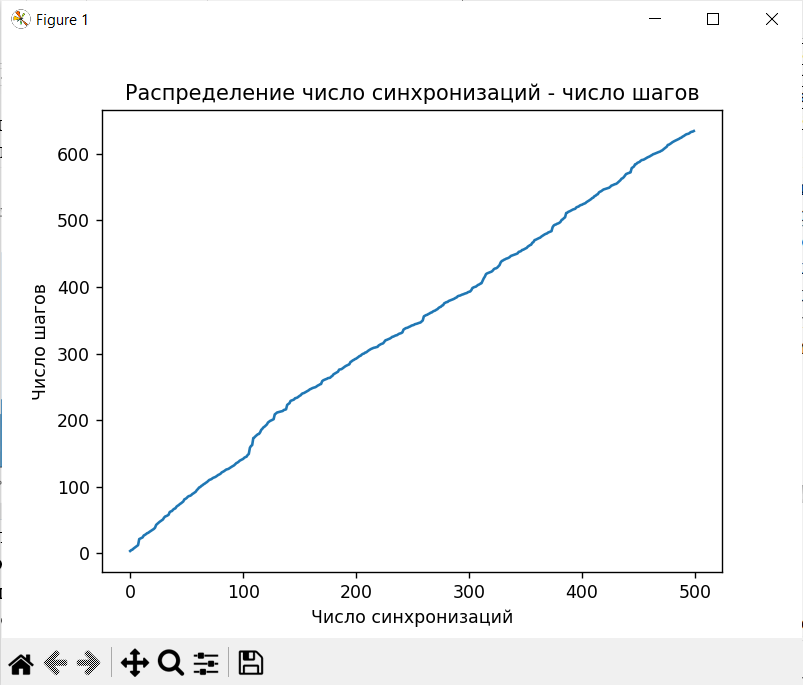
Каждая модель нейросети состоит из 4 персептронов с 10 входами.

Было проведено 500 экспериментов синхронизаций и в каждом посчитано количество шагов, после которых наступает синхронизация.

Гистограмма подсчета количества шагов, после которых наступает синхронизация для каждого эксперимента:

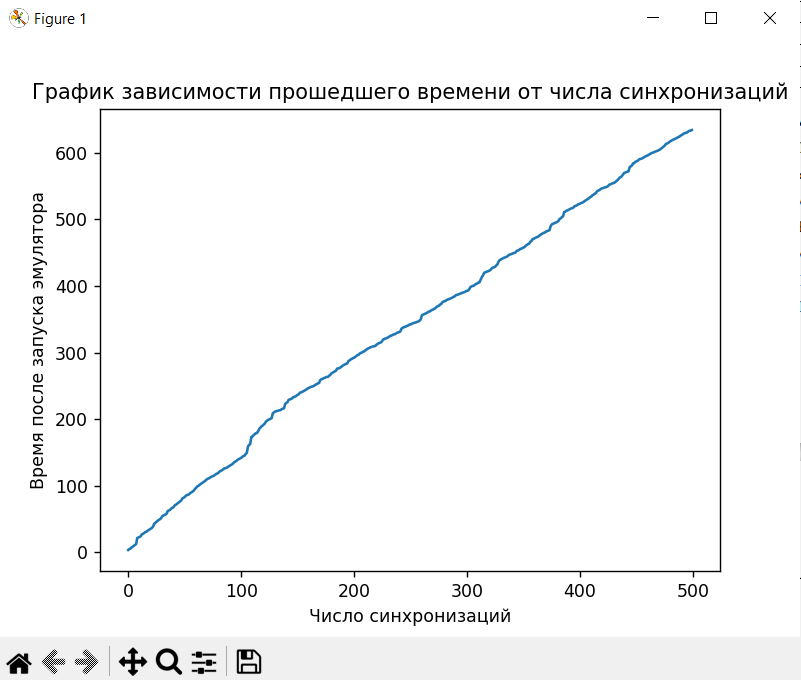


Так же было построено распределение число синхронизаций – число шагов в виде графика.



В каждом из опытов выполнен контроль промежутка времени наступления синхронизации после запуска эмулятора и подсчитано среднее время процесса синхронизации, которое равно 1.27 секунд.

График зависимости прошедшего времени от числа синхронизаций:



Алгоритм Хебба:

(*wi*)*A*(*t* + 1) = (*wi*)*A*(*t*) + (*уi*×*xi*)*А*×Θ((*уi*)*А*×(*ОB*))×Θ((–*О*)*А*×(*ОB*))

*wi* – *i*-ый вес на шаге *t*, *уi* – значение выходного сигнала, *xi* – значение входного сигнала Θ(*a*) принимает значение в зависимости от *a*, если *а* >=0, то Θ(*a*) = 1, иначе Θ(*a*) = 0. *ОA/B* – выходная величина.

*ОA/B* = Произведение (*y*k)*A/B*