Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Криптографические методы защиты информации**

**Лабораторная работа №16**

СОГЛАСОВАНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Вариант №6

Выполнил:

Студент 3 курса 4 группы ФИТ

Левша Марк Сергеевич

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.

**Практическое задание**

Было разработано приложение, реализующее модель TCP. Вывод одной реализации алгоритма для двух сетей представлен на рисунке 1.

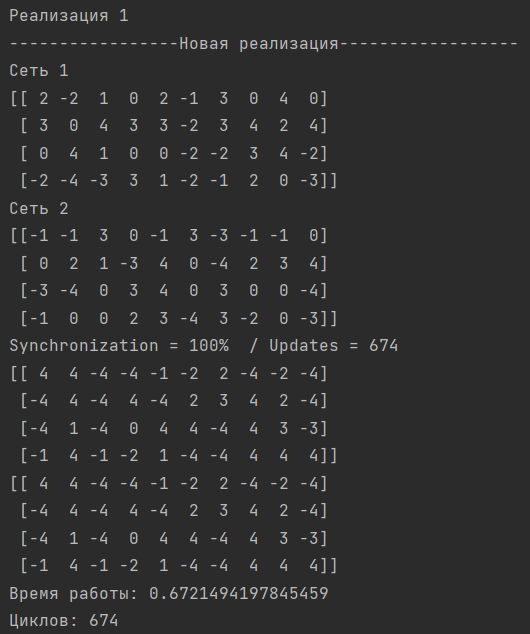


Рис. 1 – вывод одной реализации алгоритма

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 представлена на рисунке 2.

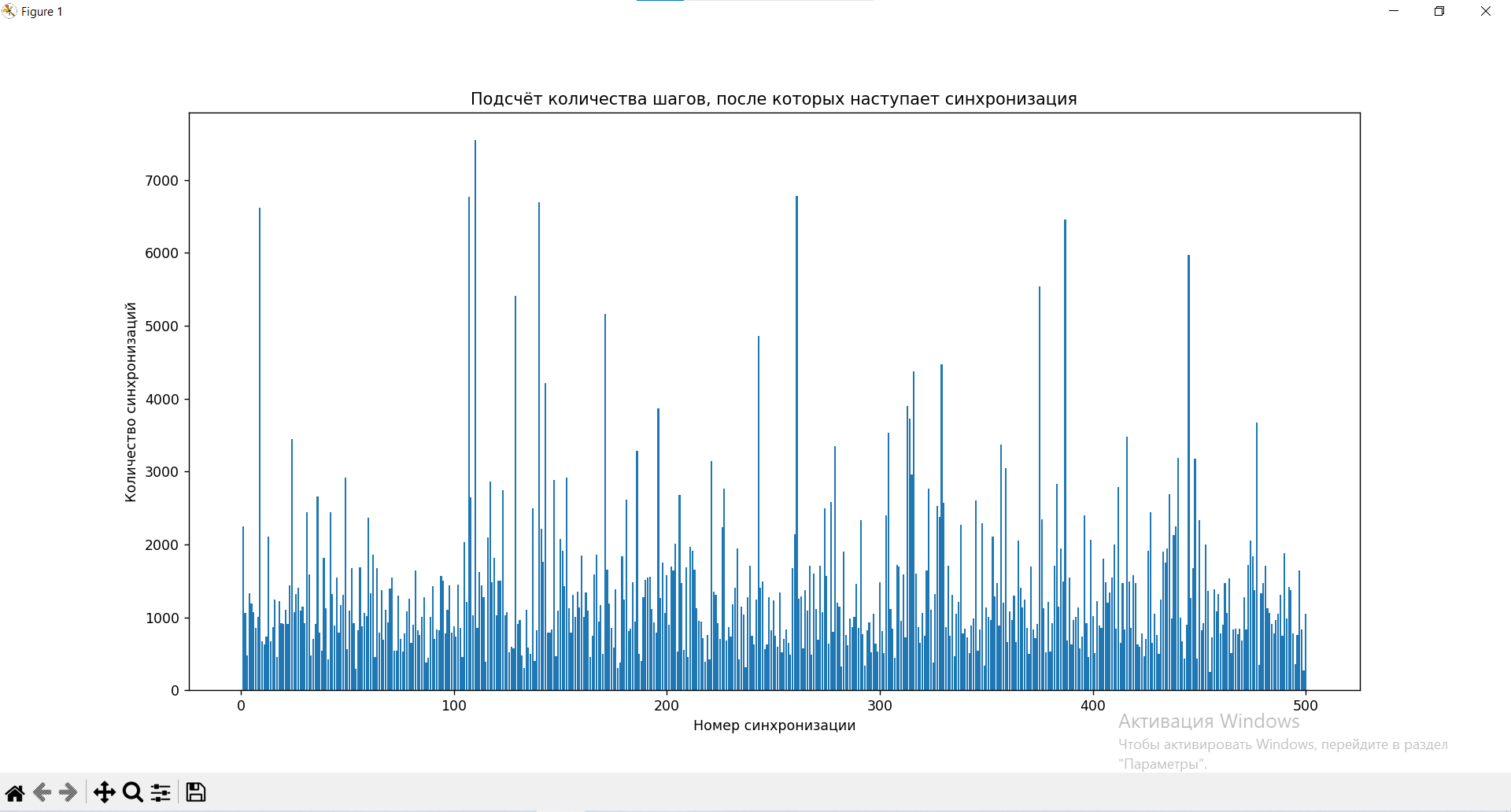


Рис. 2 – гистограмма подсчета количества шагов, после которых наступает синхронизация

Так же было построено распределение число синхронизаций – число шагов в виде графика, которое представлено на рисунке 3.

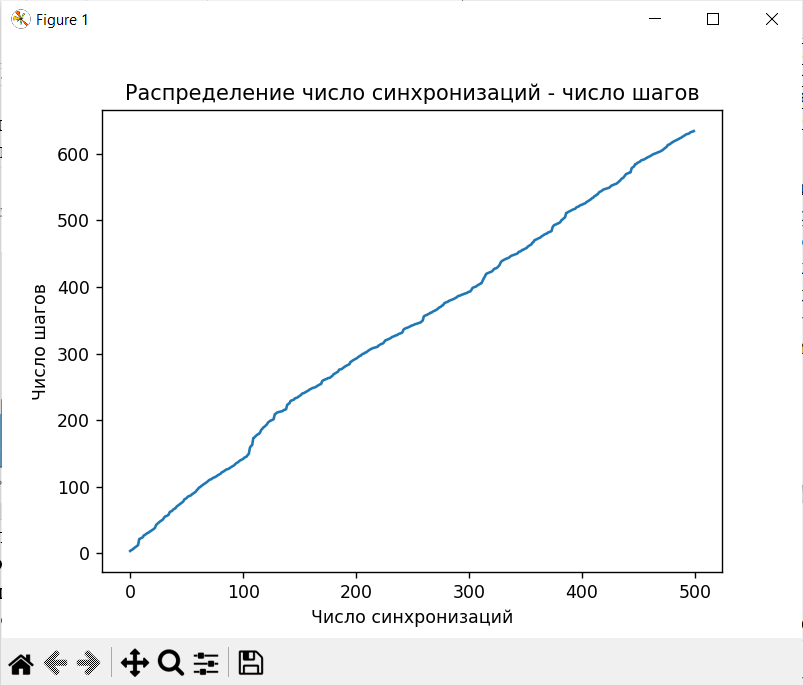


Рис. 3 – распределение число синхронизаций – число шагов.

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 представлен на рисунке 4.

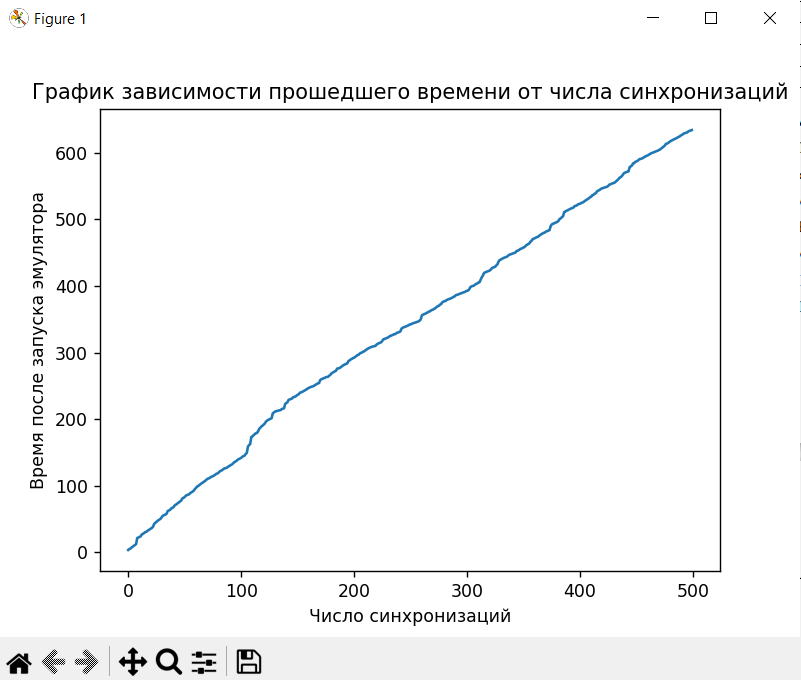


Рис. 4 – График зависимости прошедшего времени от числа синхронизаций

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*

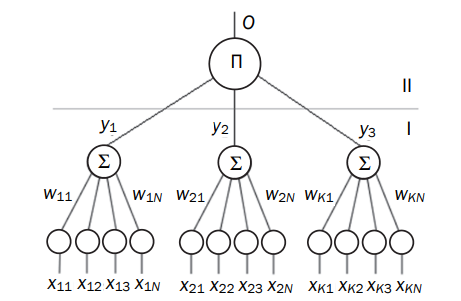
****

Рис. 5 – схема двух уровней модели TPM

**Вывод**: в ходе лабораторной работы были изучены основы посторенние ИНС и реализована модель из двух нейросетей, выполняющих синхронизацию по алгоритму Хебба.