Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №16**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

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

****

Рисунок 1.1 — Вариант

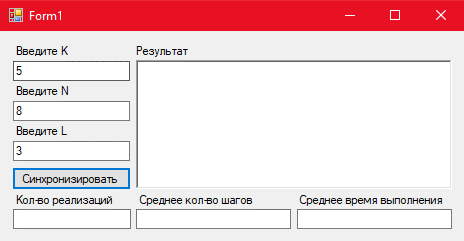
****

Рисунок 1.2 — Приложение

Проверим работоспособность приложения:

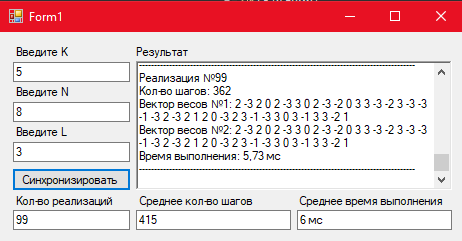


Рисунок 1.3 — Результат

В результате выполнения операций была выполнена синхронизация, используя алгоритм Хэбба и указанные значения для параметров. Всего реализаций было сделано 100 (от 0 до 99), и каждая содержит количество шагов, после которых была выполнена успешная синхронизация; первый вектор весов и второй, а также время выполнения каждой реализации. В конце были посчитаны среднее количество шагов и среднее время выполнения.

Составим соотношение вида «число синхронизаций – число шагов». Результат представлен на рисунке 1.4

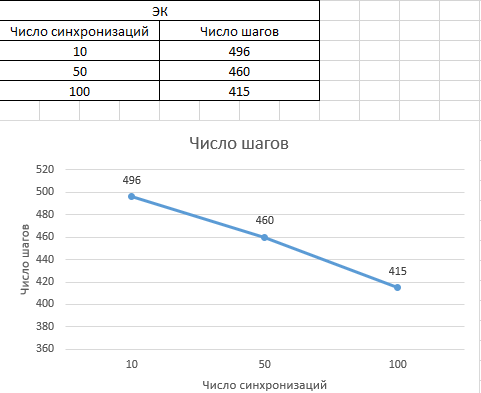


Рисунок 1.4 — Соотношение

Как видно из получившегося графика, чем больше число синхронизаций, тем меньше становится шагов для ее реализации. Так, 10 синхронизаций заняли 496 шагов, 50 – 460, а 100 – 415.

**Вывод**

В ходе лабораторной работы были изучены основы построения и функционирования искусственных нейронных сетей (ИНС), а также использования ИНСв криптографии; приобретены практические навыки программной реализации алгоритма согласования ключевой информации на основе технологии ИНС.