БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №14**

**«Согласование криптографических ключей на основе**

**технологий искусственных нейронных сетей**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

**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.

**Ход работы**

**Задание.** Разработать приложение, которое реализует модель TCP.

На рисунке 1 представлен процесс выполнения программы синхронизации на основе алгоритма случайного блуждания.

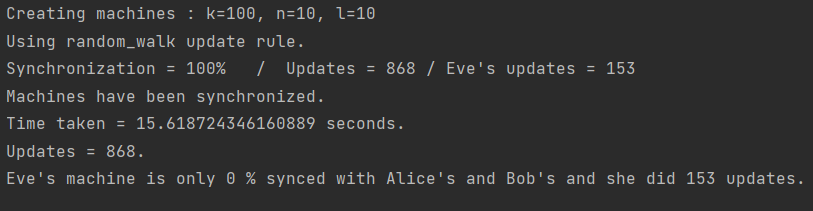


Рисунок 1 – Выполнение программы

На рисунке 2 представлен график, иллюстрирующий процесс синхронизации.

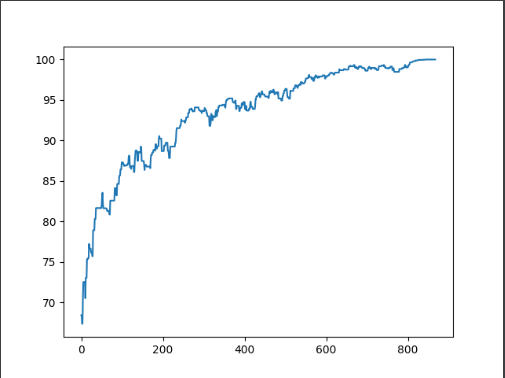


Рисунок 2 – График синхронизации

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по основам построения и функционирования ИНС, усвоены особенности построения, основные алгоритмы взаимного обучения двух связанных нейронных сетей на основе модели ТРМ, изучены методики оценки криптостойкости алгоритма на основе ТРМ, а также разработано приложение для реализации модели ТРМ с целью согласования двумя сторонами совместного тайного ключа.