ВЛИЯНИЕ ПАРАМЕТРОВ ИСКУССВЕННЫХ НЕЙРОННЫХ СЕТЕЙ НА СКОРОСТЬ ВХОЖДЕНИЯ В СИНХРОНИЗМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Брич Н. В.

Голиков В. Ф. – д-р. техн. наук, профессор

Использование синхронизируемых искусственных нейронных сетей (ИНС) является одним из перспективных решений задачи формирования общего секретного ключа. Для определения стойкости алгоритма к атакам необходимо проанализировать зависимость времени, необходимого для вхождения ИНС в синхронизм, от параметров ИНС.

Архитектура на стороне отправителя и получателя представляет собой двуслойный персептрон (TPM-архитектура), состоящий из K внутренних персептронов, каждый из которых имеет N входов (рис.1).

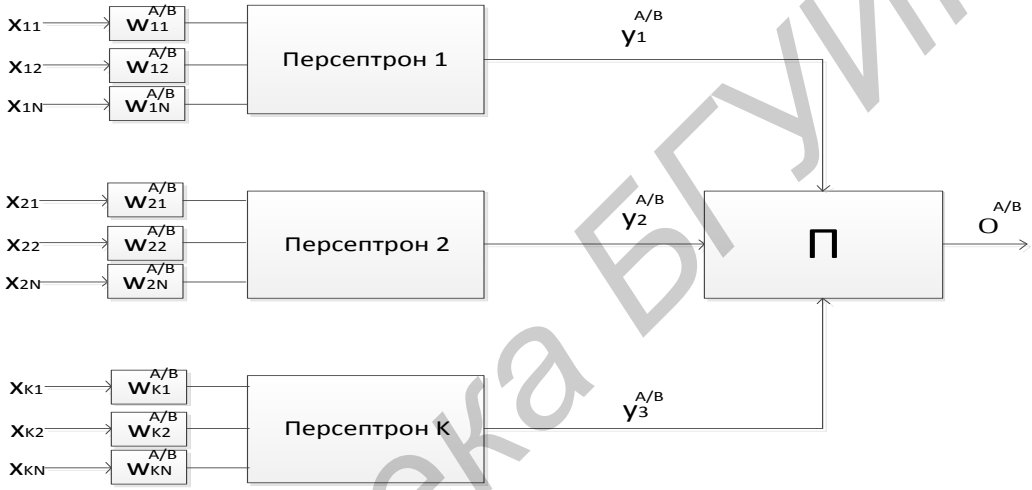

Рис. 1 – Синхронизируемая ИНС

Значения дискретной входной величины с равномерным распределением обозначено как $x_{kj} = \pm 1$, где $k = 1,2,...,K$, $j = 1,2,...,N$ Значение на выходе *k*-го внутреннего персептрона отправителя (получателя) обозначено как y_k^{AB}; w_{kj}^{AB} – вектор весовых коэффициентов сети, причем $|w_{kj}^{AB}| \le L$, где L – граничное значение весового коэффициента.

Для изучения особенностей сетей Кинцеля была разработана имитационная модель (консольное приложение) на языке высокого уровня Python 3.2. На рисунках 2-4 приведены полученные в результате моделирования зависимости времени синхронизации ИНС от параметров ИНС (1000 испытаний для каждого значения аргумента).

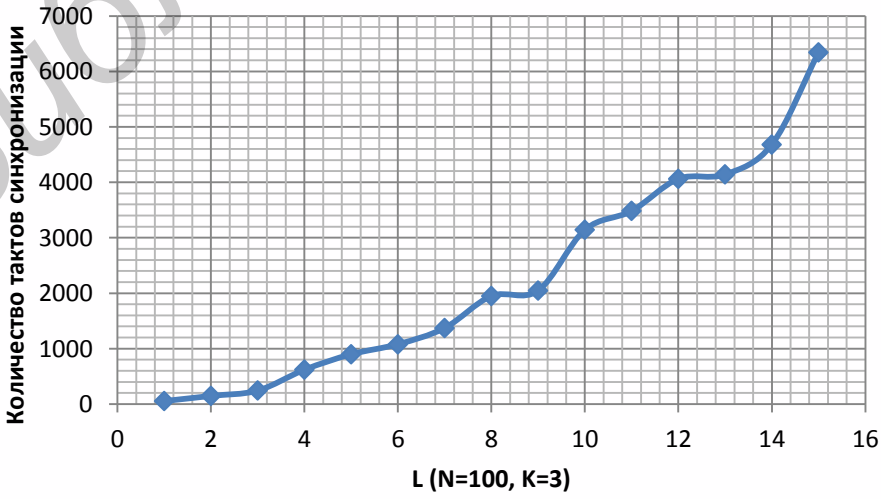

Рис. 2 – Зависимость количества тактов синхронизации от максимального значения весовых коэффициентов

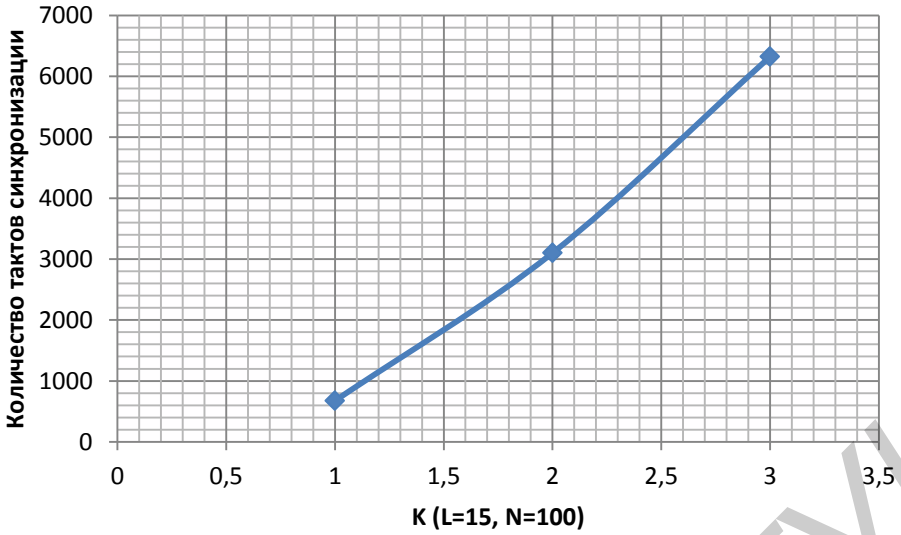

Рис. 3 – Зависимость количества тактов синхронизации от количества персептронов в ИНС

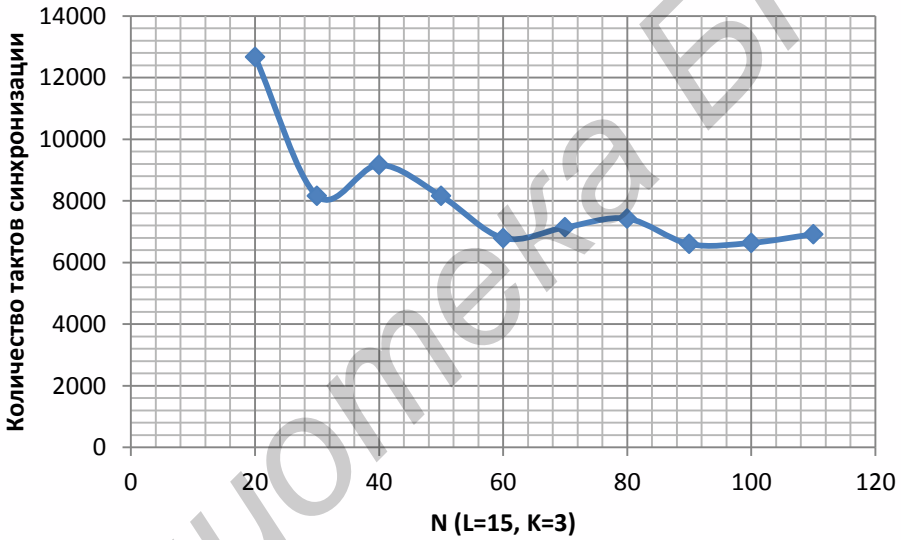

Рис. 4 – Зависимость количества тактов синхронизации от количества входов персептронов в ИНС

Таким образом, быстрее входят в синхронизм ИНС с наименьшим граничным значением весовых коэффициентов L и количеством персептронов K. Обратная зависимость скорости синхронизации от количества входов в персептрон объясняется механизмами коррекции весовых коэффициентов при обучении ИНС.

Однако формирование общего ключа с использованием синхронизируемых ИНС можно считать успешным, только если величина времени обучения ИНС легитимных пользователей меньше, чем время обучения ИНС злоумышленника. Поэтому следующий этап в исследовании −моделирование наиболее распространенных типов атак и выявление параметров ИНС, при которых атаки будут неэффективны.

Список использованных источников:

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. − 2005. – Vol. 5, n.1. – P. 130−140.

2. Kinzel, W. Neural Cryptography /W.Kinzel, I. Kanter// 9th International Conference on Neural Information Processing, Singapore, 2002.