

ПРОГРАММНАЯ МОДЕЛЬ ДЛЯ СТАТИСТИЧЕСКОГО МОДЕЛИРОВАНИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. Радюкевич

Аналитический анализ процессов, протекающих в синхронизируемых искусственных нейронных сетях (СИНС) представляет очень сложную задачу. В [1] сделана попытка ее решения в упрощенном варианте, позволяющем оценивать лишь общие тенденции влияния параметров.

В связи с этим разработана программная модель для статистического моделирования результатов исследования СИНС. При программной реализации наиболее эффективным инструментом ее исследования является метод имитационного моделирования, а точнее метод статистического моделирования, т.к. случайные процессы, имеющие место в реальной технологии, полностью совпадают с процессами, организованными в модели. Имитационная модель СИНС отличается от реальной программной реализации лишь наличием дополнительных функций, позволяющих анализировать свойства технологии такие как эффективность, безопасность, быстродействие.

Программная модель позволяет смоделировать методы, описанные в [2–4], а также выполнять исследования с учетом действий криптоаналитика. В программной модели существует возможность изменения начальных параметров СИНС, а также объема моделирования. Результаты моделирования представляются в виде таблиц и графиков для наглядного восприятия результатов.

Метод статистического моделирования позволяет вычислять вероятностные характеристики случайных величин и процессов в задачах практически любой сложности и широко применяется в настоящее время в физике, информатике, экономике и других областях науки и техники.

Литература

1. Neural Synchronization and Cryptography. Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades der Bayerischen Julius-Maximilians-Universität Würzburg vorgelegt von Andreas Ruttor aus Würzburg, 2006. 120 p.

2. Радюкевич М.Л., Голиков В.Ф. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей // Информатика. 2020. Т. 17, № 1. С. 75–81.

3. Радюкеви М.Л., Голиков В.Ф. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей // Доклады БГУИР. 2021. № 19 (1). С. 79–87.

4. Радюкевич М.Л. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей // Системный анализ и прикладная информатика. 2021. № 3. С. 51–58.