ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. Радюкевич

Проведенный анализ технологии формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей [1–3] показывает, что данная технология может быть использована в условиях компрометации методов, базирующихся на применении классических односторонних функций. Однако, уровень конфиденциальности формируемого секрета, быстродействие предлагаемой технологии нуждается в серьезном повышении и обосновании.

В работах [4–6] предложены методы повышения конфиденциальности формируемого общего секрета и уменьшения количества обменов информации по сравнению с технологией Neural key generation. Первым был предложен метод усиления секретности, суть которого заключалась в смешивании некоторого числа результатов отдельных синхронизаций (свертки). В качестве функции смешивания использовалась свертка векторов весовых коэффициентов сетей побитовым сложением по модулю 2 всех результатов отдельных синхронизаций. Данный метод позволил экспоненциально уменьшить успех криптоаналитика. При дальнейших исследованиях был предложен комбинированный метод, который состоял из двух этапов: формирование частично совпадающих бинарных последовательностей с помощью синхронизируемых искусственных нейронных сетей и устранение несовпадающих битов путем открытого сравнения четностей пар битов. Данный метод позволил существенно сократить количество обменов информации. Проанализировав возможные атаки на комбинированный метод было предложено добавить досрочное прерывание процесса синхронизации на первом этапе и внесение изменений в полученную бинарную последовательность путем инвертирования случайным образом некоторого количества бит. Эти изменения получили название комбинированного метода формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей, который обеспечивает высокую его криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации.

Литература

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

2. Kanter I., Kinzel W., Kanter E. Secure exchange of information by synchronization of neural networks. arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.

3. Kanter I., Kinzel W. The Theory of Neural Networks and Cryptography // Quantum Computers and Computing. 2005. Vol. 5, No. 1. P. 130−140.

4. 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.

5. 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.

6. 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.