ПРИМЕНЕНИЕ ПРОБЛЕМНО ОРИЕНТИРОВАННЫХ НЕЙРОННЫХ СЕТЕЙ В КРИПТОГРАФИИ

д-р техн. наук, проф. В.Д. Дмитриенко, д-р техн. наук, проф . С.Ю. Леонов, магистр К.С. Капшук, Национальный технический университет "Харьковский политехнический институт", г. Харьков

Применение современных вычислительных систем для обработки данных требует решения ряда проблем, среди которых одной из важнейших является проблема защиты информации как при её обработке, так и при её хранении и передаче. Криптография для обеспечения безопасности работы вычислительных систем разработала большой набор различных средств, среди которых ключ является основным секретом в сохранении информации.

Симметричные криптографические системы с открытым ключом предполагают наличие только одного секретного ключа, известного двум абонентам, обменивающимся информацией [1]. Основное достоинство таких криптографических систем – высокая скорость обработки входной информации, а недостаток – необходимость разработки дополнительных механизмов, обеспечивающих безопасность использования систем с открытым ключом. Для повышения информационной безопасности функционирования симметричных систем с открытым ключом при решении прикладных задач используются различные методы совершенствования таких систем [2]. Одним из наиболее перспективных методов преодоления недостатков систем с открытым ключом – это развитие нейросетевого направления в криптографии [2, 3]. Одно из достоинств этого направления – существенное повышение производительности криптографических систем из-за массового параллелизма вычислительных систем на основе нейронных сетей, что позволяет решать задачи большой размерности за время на порядки меньшее, чем требуется компьютерам традиционной архитектуры.

Однако это достоинство нейронных сетей во многих случаях в криптографических системах перечеркивается при смене ключа, когда необходимо полное и трудоемкое переобучение нейронной сети. В связи с этим для криптографических систем были разработаны проблемно ориентированные нейронные сети со специфическими архитектурами и алгоритмами функционирования. В настоящее время наиболее эффективными среди таких сетей считаются нейронные сети конечного кольца (НСКК), структура которых определяется алгоритмом шифрования. Нашли своё применение в проблемно ориентированных нейроструктурах криптографии и другие нейронные сети: хаотические [4], нейроные сети с обратными связями [5] и некоторые другие. В докладе рассматриваются

достоинства и недостатки этих нейронных сетей и примеры их применения.

Список литературы: **1.** *Горбенко І.Д.* Прикладна криптологія. Теорія. Практика. Застосування: монография / *І.Д. Горбенко, Ю.І. Горбенко*. – Харків: Видавництво"Форт", 2012. – 870 с. **2**. *Червяков Н.И.* Применение искусственных нейронных сетей и системы остаточных классов в криптографии / *Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко, А.В. Лавриненко*. – М.: ФИЗМАТЛИТ, 2012. – 280 с. **3**. *Kinzel W.* Interacting neural networks and cryptography / *W. Kinzel, I Kanter* // Advances in Solid State Physics. – Springer Verlag, 2002. – Vol. 42. – 383 – 391. **4**. *Lian S.* A fast MPEG4 video encryption scheme based on chaotic neural network / *S. Lian, J. Sun, Z. Li, Z. Wang* // ICONIP 2004, LNCS 3316. – 2004. – P. 720-725. **5**. *Ruttor A.* Neural cryptography with feedback / *A. Ruttor, W. Kinzel* // Physical Review E., 2004. – Vol. 69. – P. 1915-1924.