ОЦЕНКА УРОВНЯ КОНФИДЕНЦИАЛЬНОСТИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА, СФОРМИРОВАННОГО ВЗАИМОДЕЙСТВУЮЩИМИ НЕЙРОННЫМИ СЕТЯМИ

Д.С. Гранцевич, В.Ф. Голиков

В настоящее время широко используются асимметричные криптографические системы. Одним из недостатков таких систем является сложность математических операций, которые значительно увеличивают время, необходимое на выполнение вычислений. Другим недостатком является тот факт, что их безопасность основывается на сложности вычислительных операций в задачах из теории чисел. Это означает, что с появлением квантовых компьютеров алгоритмы асимметричных криптосистем (например, RSA) станут бесполезными. Поэтому большой интерес представляет разработка новых методов, не использующих в своей конструкции теорию чисел.

В настоящее время большой интерес представляет использование искусственных нейронных сетей в криптографии. Идея использования нейронных сетей для формирования ключей с использованием незащищенных каналов связи впервые предложена И. Кантером и В. Кинцелем. Технология формирования ключевой информации на основе нейронных сетей рассматривается как альтернатива классической схеме Диффи–Хеллмана, которая заключается в трудности, связанной с решением задачи дискретного логарифмирования. Протокол обмена ключами, использующий нейронные сети, базируется на синхронном обучении сетей. Обучение двух нейронных сетей с использованием их общих выходных величин ведёт к возникновению идентичных векторов весов. Сети обмениваются между собой выходными и входными величинами, при этом секретными остаются значения векторов весов. Предполагается, что третья сторона, следящая за обменом информации между обеими сетями, не в состоянии вычислить значения векторов весов ни одной из сетей. Следовательно, вектор весов может составлять секретный ключ, использующийся для дальнейшей передачи информации по незащищенным каналам.

Однако до сих пор недостаточно изучены вопросы криптографической стойкости предлагаемой технологии и потенциальные возможности криптоаналитика по компрометации формируемого ключа. Поэтому оценка эффективности формирования ключевой информации с помощью нейронных сетей представляет собой актуальную задачу.