КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Лисица Е.В., 5 курс,
Урбанович П.П., д.т.н., профессор,
УО «Белорусский государственный технологический университет»

Являясь самым дорогим продуктом в сфере межличностных отношений, информация нуждается в защите от несанкционированного доступа. Этой проблемой занимается наука криптография, главная цель которой – поиск и исследование математических методов и средств преобразования информации для повышения уровня ее защиты.

В настоящее время используются два вида криптографических систем для передачи информации: симметричная и асимметричная. В симметричных системах отправитель и получатель используют один и тот же ключ, который должен оставаться известным только этим двум сторонам, участвующим в обмене информацией. В связи с этим при практической реализации таких систем шифрования возникает проблема обмена ключами и их распределения. Это обусловлено необходимостью передачи сгенерированного секретного ключа другой стороне для выполнения обратного преобразования.

В 1975 году для решения этой проблемы У. Диффи и М. Хеллман предложили систему криптопреобразования с открытым (публичным) ключом, для которой не нужен абсолютно надежный канал для рассылки секретных ключей либо сообщений.

В 2002 году В.Кинцель и И.Кантер предложили совершенно новое направление обмена конфиденциальной информацией, которое объединило в себе две науки: криптографию и науку об искусственных нейронных сетях. Протокол обмена использует способность нейронных сетей к взаимному обучению путем обмена открытой информацией между ними и генерации на этой основе общего секретного ключа. Таким образом, протокол Кинцеля-Кантера решает по-новому проблему распределения ключей симметричных систем.

В протоколе Кинцеля-Кантера используется архитектура TPM (tree parity machine). Она состоит из *K* скрытых единиц (независимых персептронов), каждая из которых характеризуется *N*-элементным вектором входов и вектором весовых коэффициентов. Элементы вектора входа – бинарные и принимают значения *1* либо *-1*. Весовые коэффициенты – целые числа из интервала *[-L; L]*. Выходы нейронов составляют *K* значений, которые равны скалярному произведению вектора входных значений на вектор весов. Далее полученные значения выходов проходят через пороговую биполярную функцию активации. Выход целой архитектуры TPM равен произведению значений выходов всех скрытых единиц. В начальный момент времени отправитель и получатель инициализируют векторы весов. Затем на каждом шаге обучения *t* генерируются вектора входных значений и вычисляются значения выхода целой архитектуры TPM. Эти данные являются открытыми и передаются по публичному каналу. Для обучения сетей используются классические правила обучения.

Разработана компьютерная модель криптографической системы на основе нейросетевой технологии. Данная модель позволяет экспериментально изучить протокол Кинцеля-Кантера, оценить его быстродействие и эффективность при различных правилах обучения, количества персептронов, количества входов и синаптической глубины весовых коэффициентов. Так результаты моделирования процесса синхронизации при K = 3, N = 102 и различных значениях синаптической глубины L, с применением правил обучения Hebbian, Anti-Hebbian, Random walk отображены в таблице.

Таблица – Результаты моделирования процесса синхронизации

Синаптическая глубина L	Среднее время синхронизации T для N=102, K=3		
	Hebbian	Anti-Hebbian	Random walk
3	~ 250	~ 500	~ 350
4	~ 500	~ 5000	~ 480
5	~ 550	~ 52000	~ 750
6	~ 650	> 200000	~ 1100