ЛИТЕРАТУРА

1. Wikipedia. Электронная энциклопедия [Электронный ресурс]: Кернинг. – Режим доступа: https://ru.wikipedia.org. – Дата доступа: 23.04.2017.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

УДК 003.26+347.78

Студ. О.Л. Панченко
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ УСТОЙЧИВОСТИ ПРОЦЕССА СИНХРОНИЗАЦИИ ДВУХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

Для безопасной передачи данных применятся наиболее популярная технология – криптографическое преобразование информации. Криптографические системы подразделяются на асимметричные и симметричные. Их особенности заключаются в том, что в первом случае для зашифрования и расшифрования используются разные ключи, а во втором – один.

Симметричным системам свойственна проблема распределения ключей. Одни из способов решения данной проблемы является использование нейронных сетей. Данная идея была предложена И. Кантером и В. Кинцелем. В ее основе лежит использование архитектуры TPM (англ. Tree Parity Machine, древовидная машина четности). Возможно достижение состояния так называемой синхронизации нейронных сетей, под которой следует понимать равенство значений весовых коэффициентов нейронных сетей. Это и служит основой для протокола выработки общего ключа.

Нейронные сети представляют собой математическую модель, построенную на основе принципов работы биологических нейросетей. Нейрон представляет собой единицу обработки информации в нейронной сети. В этой модели можно выделить три основных элемента (рис. 1).

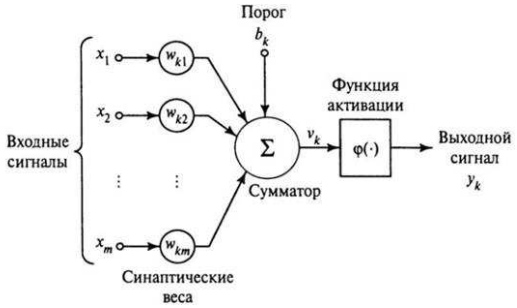

Рисунок 1 – Модель нейрона

Набор синапсов или связей, каждый из которых характеризуется своим весом. В частности, сигнал на входе синапса *j*, связанного с нейроном *k*, умножается на вес w_{kj}. Сумматор складывает входные сигналы, взвешенные относительно соответствующих синапсов нейрона. Эту операцию можно описать как линейную комбинацию.

Функция активации ограничивает амплитуду выходного сигнала нейрона. Эта функция также называется функцией сжатия. Обычно нормализованный диапазон амплитуд выхода нейрона лежит в интервале [0, 1] или [-1, 1].

Исходя из этого, нейронная сеть должна состоять из нейронов. Такую самую простую сеть с прямой связью составляет одиночный нейронный слой. Первым такую сеть предложил Фрэнк Розенблатт и назвал её одиночный персептрон. В таком слое каждый нейрон получает одинаковый набор входных сигналов, и каждый из их имеет свой собственный вектор.

Весовые коэффициенты существенным образом влияют на результаты работы сети, поскольку они решают, правильно ли сеть действует. Представленная модель нейронной сети в принципе бесполезна, так как она не способна решать поставленные задачи до тех пор, пока не будет соответствующим способом «натренирована». Этот процесс называется обучением и основан на соответствующем подборе коэффициентов вектора весов в контексте решаемой задачи.

Обучение сети может быть реализовано двумя основными методами:

- обучение с учителем. Учитель дает сети правильный ответ – какое выходное значение она должна дать на представленный входной сигнал;
- обучение без учителя. Цель обучения не определена в виде конкретных образцов, так что, используя полученные данные, сеть учится сама [1].

Взаимное обучение сетей А и Б касается простейшей однонаправленной модели, в которой участвуют два персептрона. Роли таких нейронных сетей заранее не определены, каждая может выполнять функции как учителя, так и ученика. Это значит, что сети учатся друг у друга, используя для этого полученные результаты и, стремясь к общей цели, находят общие элементы в результате своих вычислений [2].

Эта модель обучения, благодаря своим свойствам, может быть использована в криптографии, а именно: в определении общего для А и Б криптографического ключа. Именно эта модель используется в приложении. Процесс синхронизации сетей происходит следующим образом:

1. Задаются случайные значения весовых коэффициентов;
2. Затем выполняются следующие шаги, пока не наступит синхронизация;
3. Генерируется случайный входной вектор X;
4. Вычисляются значения скрытых нейронов;
5. Вычисляются значение выходного нейрона;
6. Сравниваются выходы двух TPM:
7. Если Выходы разные: переход к п.3;
8. Если Выходы одинаковые: применяется выбранное правило к весовым коэффициентам.

После полной синхронизации, сети А и Б могут использовать веса в качестве ключа [3].

Нами разработать программное средство для проведения анализа устойчивости процесса синхронизации двух нейронных сетей в задачах генерации криптографического ключа.

В приложении пользователь вводит такие параметры как (рис. 2):

— количество входных нейронов у персептрона – N;
— количество персептронов – K;
— диапазон изменения L.

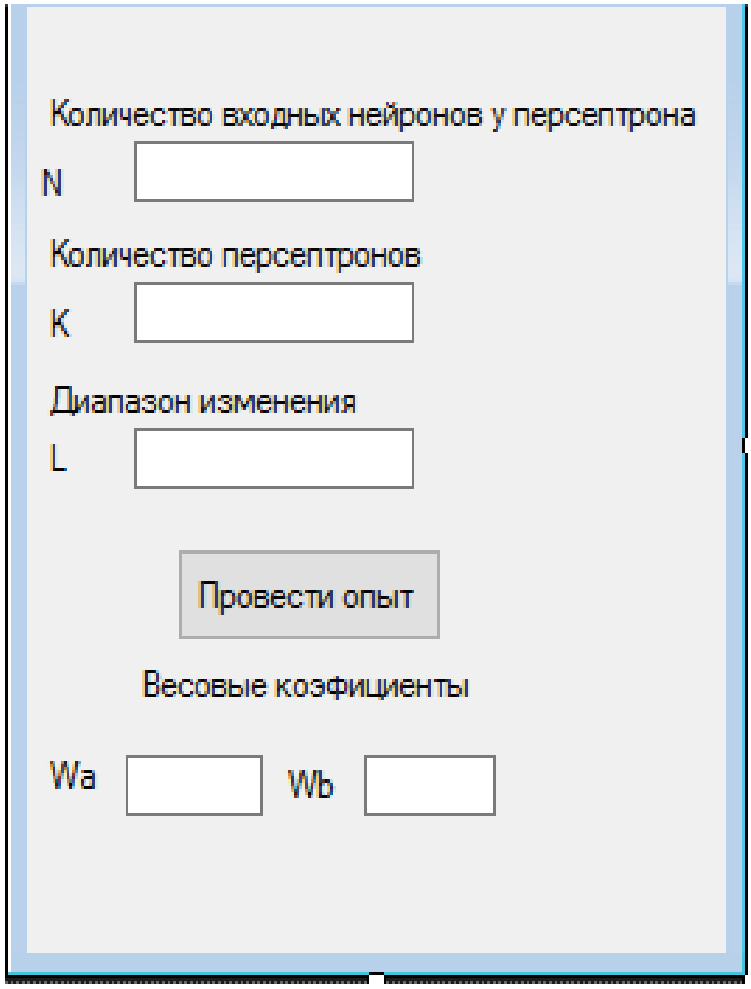

Рисунок 2 – Окно программного средства

В результате пользователю выводятся весовые коэффициенты каждой сети, что позволяет проверить результат. Проведя достаточное количество экспериментов, можно произвести анализ устойчивости двух нейронных сетей в процессе синхронизации.

ЛИТЕРАТУРА

1. Харин Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. — Минск: БГУ, 1999. – 319 с.

2. Плонковски, М. Д. Криптографическое преобразование информации на основе нейросетевых технологии / М. Д. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск: БГТУ, 2005. – С. 161–164.

3. Плонковски, М. Д. Синхронизация криптографических ключей на основе нейросетевых технологий / М. Д. Плонковски, П. П. Урбанович // Материалы междунар. науч.-практ. конф., апрель 2006г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 29.