

Реализация предложенного метода использования сверточной нейронной сети позволяет получить полноценную и рабочую систему оптического распознавания рукописного текста и автоматизировать проверку бланков ответов по тестам. Разработанное программное обеспечение можно использовать в учреждениях образования, исследовательских центрах для проверки различных тестов.

УДК 519.715

И. А. Бирюк, магистрант  
(БГТУ, г. Минск)

### **МОДЕЛИРОВАНИЕ И АНАЛИЗ ПРОЦЕССА СИНХРОНИЗАЦИИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ**

В связи с бурными темпами развития сети интернет и как следствие увеличение количества информации, которая передаётся при помощи этой сети, все чаще и чаще поднимается вопрос об информационной безопасности. Для безопасной передачи информации применяются различные технологии, наиболее часто применяемая – криптографическое преобразование информации.

Для распределения ключей между пользователями компьютерной сети используются следующие основные способы:

- использование одного или нескольких центров распределения ключей;
- прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Одна из новых идей касающаяся распространения ключей, применяемых для шифрования, является использование нейронных сетей. Эта идея была выдвинута И. Кантером и В. Кинцелем и основано на использовании архитектуры ТРМ (англ. Tree Parity Machine, древо-видная машина четности). Развитием этой идеи является расширение множества используемых алгебр за счёт использования комплексных и гиперкомплексных чисел [1-3].

Было разработано программное средство для проведения исследований и анализа устойчивости двух искусственных нейронных сетей. Для анализа полученных результатов были рассчитаны индекс Брея-Кёртиса и расстояние по Хеллингеру для того чтобы провести сравнение подобие полученного во время проведения экспериментов

распределения к нормальному. Полученные результаты для опытов проведенных на основании кватернионов представлены в таблице 1.

**Таблица 1 = Результаты анализа**

Количество входных нейронов	Количество персептронов	Ограничение накладываемые на весовые коэффициенты	Стандартное отклонение числа итераций синхронизации	Индекс Брея-Кёртиса	Расстояние по Хэллингеру
5	5	-5;+5	212,3127	0,236778	39915,92
5	5	-6;+6	360,5353	0,254661	121378,9
5	6	-5;+5	214,9023	0,230132	29147,51
6	5	-6;+6	164,8493	0,205305	18992,93
6	6	-5;+5	147,7051	0,232275	40974,62
6	6	-6;+6	147,7025	0,184315	17536,88
6	6	-7;+7	272,0603	0,226647	38036,79
6	7	-6;+6	144,2508	0,173883	14911,65
6	7	-7;+7	273,0947	0,193843	30154,5
7	6	-6;+6	209,8088	0,215792	26438,17
7	6	-7;+7	385,8097	0,23227	51979,91
7	7	-6;+6	209,6789	0,206227	25823,96
7	7	-7;+7	284,9163	0,197808	33964,22
8	8	-8;+8	273,6395	0,184612	29033,77
9	9	-9;+9	605,6361	0,201454	74716,29

## ЛИТЕРАТУРА

1 Плонковски, М. Д. Модели передачи и криптографического преобразования информации на основе нейросетевых технологий и расширения поля используемых чисел: Диссертации на соискание ученой степени кандидата наук: 05.13.19/ М. Д. Плонковски – Минск, БГТУ, 2009 – 103 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 2006 г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 29.