Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.21

Грицкевич
Татьяна Викторовна

Методы построения криптографических систем на основе нейронных сетей

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение
вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Иванюк Александр
Александрович
д. т. н., доцент

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

Проблема обеспечения необходимого уровня защиты информации всегда являлась важной задачей, но оказалась (и это предметно подтверждено как теоретическими исследованиями, так и опытом практического решения) весьма сложной, требующей для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специфических средств и методов, а создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации.

В настоящее время задача создания и использования новых криптографических методов построения в информационных системах стала особо актуальна.

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически нераскрываемыми.

Таким образом, на сегодняшний день остро встает проблема поиска новых методов построения криптографических систем, одним из которых является нейросетевой подход — это один из новых подходов для построения криптографических систем. Разумеется, нейросетевым технологиям в их нынешнем состоянии не под силу создать что-либо, хоть отдаленно напоминающее по сложности человеческий мозг, однако уже очень многие его функции вполне поддаются моделированию, хотя и в весьма упрощенном варианте. В том числе и прямая передача информации от одной нейронной сети другой в процессе взаимного обучения.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью данной работы является обоснование возможности применения методов построения криптографических систем, в основе которых лежат нейронные сети. Оптимизации существующих подходов к построению криптографических систем на основе нейронных сетей. Реализация, анализ и оценка данных методов. Изучение возможности модификации реализованных алгоритмов, а также возможностей для эффективного их применения в различных областях.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать существующие подходы к построению криптографических систем на основе нейронных сетей.
2. Показать возможность использования нейронных сетей в криптографических системах.
3. Достигнуть адекватно быстрое время синхронизации нейронных сетей в построенной криптографической системе.
4. Проанализировать математический аппарат, для построения криптографических систем.
5. Показать работоспособность представленных математических методов построения криптографических систем, разработав программный модуль.
6. Предложить новые и модификации методов построения криптографических систем на основе нейронных сетей.
7. Показать работоспособность и эффективность модифицированных и новых методов построения криптографических систем, разработав программный модуль.
8. Экспериментальным путем показать эффективность использования модифицированных методов построения криптографических систем с помощью нейронных сетей.
9. Экспериментальным путем показать, эффективность применения нейронных сетей, как базы для построения криптографических систем.

Объектом исследования являются методы построения криптографических систем на основе нейронных сетей.

Предметом исследования является изучение свойств модификаций и новых методов методов построения криптографических систем на основе нейронных сетей, а так же возможность их применения.

Практическая актуальность исследования связана с необходимостью предоставления новых производительных методов построения криптографических систем.

Особенно актуальным является возможность использования модифицированных и оптимизированных методов построения криптографических систем с использованием нейронных сетей.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы » (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя А. А. Иванюка, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на «51-ой научной конференции аспирантов, магистрантов и студентов БГУИР» (БГУИР, Минск, Беларусь, 2015) по направлению компьютерные системы и сети [1-А]; III Международная научно-техническая интернет конференция "Информационные технологии в образовании, науке и производстве" (Международный институт дистанционного образования (МИДО) БНТУ, Минск, Беларусь, 2015) [2-А].

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 1 работа в материалах конференции аспирантов, магистрантов и студентов БГУИР и 1 работа в сборнике трудов и материалов международной конференции.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников и списка публикаций автора.

В первой главе представлен анализ предметной области, рассматриваются базовые понятия в области криптографии и нейрокриптографии. Анализируются существующие подходы к построению криптографических систем. Проведен анализ осуществимости и безопасности алгоритмов и возможных вариантов атак.

Вторая глава представляет собой обзор математических моделей, методов и алгоритмов построения криптографических систем на основе нейронных сетей. Данная глава содержит описание основных математических идей, являющихся основой алгоритмов построения криптографических систем, а также методов реализации на базе различных нейронных сетей и предварительную оценку каждого из подходов.

В третьей главе описаны эксперименты, проведенные над различными новыми и модификациями методов построения криптографических систем на основе нейронных сетей. Представлены результаты сравнения производительности методов. Приведены результаты экспериментальных исследований с различными исходными параметрами. Также приведены результаты возможных оптимизаций в скорости работы.

Общий объем работы составляет 51 страницу, из которых основного текста – 40 страниц, 21 рисунков на 10 страницах, 3 таблицы, список использованных источников из 29 наименований на 2 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Пояснительная записка состоит из 4 основных разделов.

Во **введение** была обоснована актуальность темы диссертационной работы, Определена область и указаны основыные направления исследований. Обозначена практическая ценность работы

В **первой главе** проводится анализ предметной области.

В разделе 1.1 даются определения основных понятий по искусственным нейронным сетям, их разновидностям.

В разделе 1.2 происходит рассмотрение основ нейрокриптографии и уже существующих подходов в этой области.

В разделе 1.3 рассматривается распределение ключей по открытому каналу и подробно объясняется протокол Диффи-Хеллмана, а также его плюсы и минусы.

В разделе 1.4 представлена информация про Tree Parity Machine, рассматривается осуществимость и безопасность данной схемы построения криптографической системы, а также приводится общий алгоритм синхрониизации, используемый для синхронизации TPM.

В разделе 1.5 рассматривается используемая далее ККК схема обмена ключами.

В разделе 1.6 рассматриваются подходы, которые дальше будут использоваться для распараллеливания работы алгоритмов.

Во **второй главе** «Математические модели» были подробно рассмотрены основные модели и математический аппарат, на основе которого будет происходить построение криптографической системы на основе рассмотренных нейронных сетей

В разделе 2.1 рассматривается модель на базе синхронизации нейронных сетей и хаотичных отображений.

В разделе 2.2 рассматривается модель на базе нейронной криптографии с обратной связью.

В разделе 2.3 рассматривается модель на базе нейронной сети RAAM.

В **третьей главе** описываются эксперименты, проведенные над методами построения криптографических систем на основе нейронных сетей. Тут производиться оценка эффективности метода построения криптографической системы на основе синхронизации нейронных сетей различных видов. Приводятся результаты испытаний эффективности реализованных алгоритмов. критерием оценки в которых является среднее

количество сообщений при синхронизации нейронных сетей, среднее затраченное время CPU при синхронизации, средний размер передаваемых данных при синхронизации нейронных сетей с различными параметрами. В качестве тестируемых методов были выбраны 3 алгоритма построения криптографической системы на основе следующих нейронных сетей: TPM, нейронных сетей с хаотичными отображениями, нейронных сетей с обратной связью, нейронных сетей RAAM.

В разделе 3.1 приводятся результаты для синхронизации TPM.

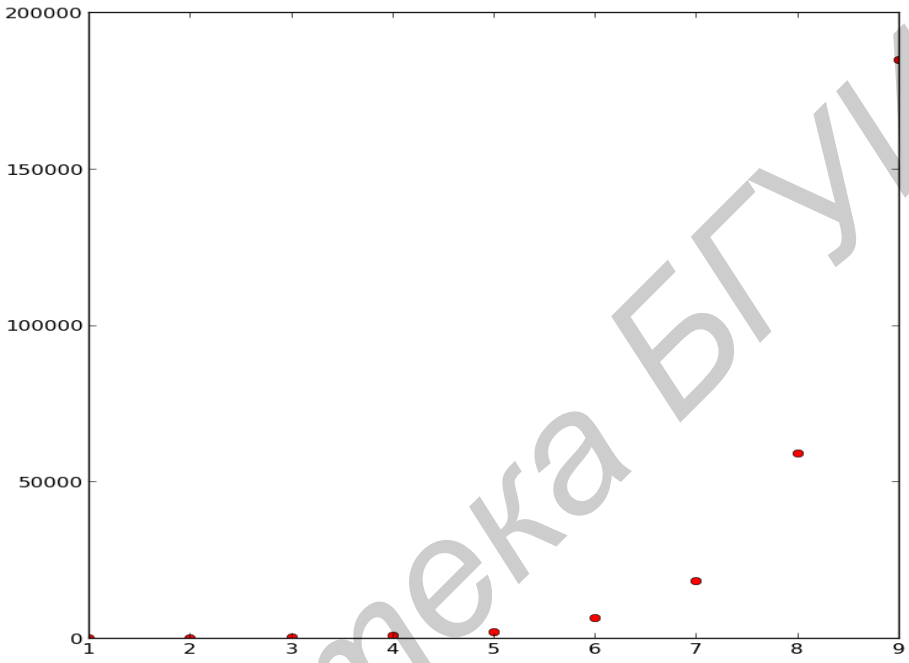

Рисунок 1 – График зависимости среднего количества сообщений от L при конфигурации сети TPM с параметрами K=4, N=4

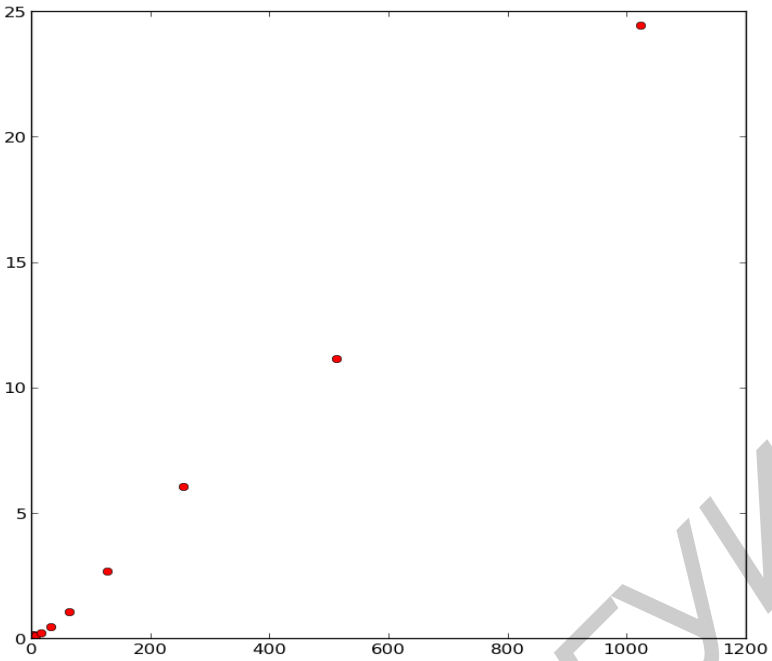

Рисунок 2 – График зависимости среднего времени CPU от N при конфигурации сети TPM с параметрами K=4, L=3

В разделе 3.2 приводятся результаты для синхронизации нейронных сетей с хаотичными отображениями.

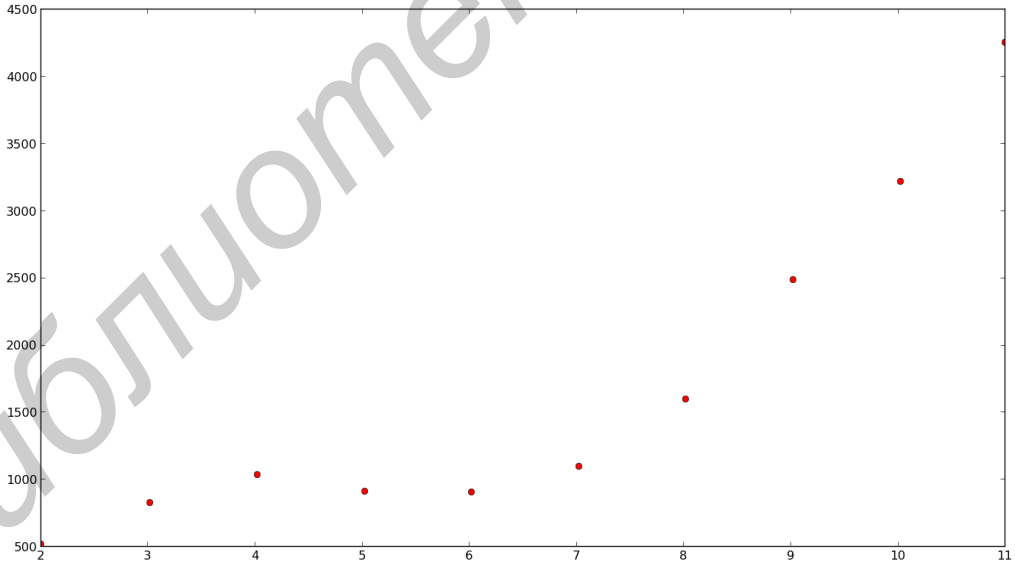

Рисунок 3 – График зависимости среднего количества сообщений от L при конфигурации сети с хаотичными отображениями с параметрами K=4, N=4

В разделе 3.3 приводятся результаты для синхронизации нейронных сетей с обратной связью.

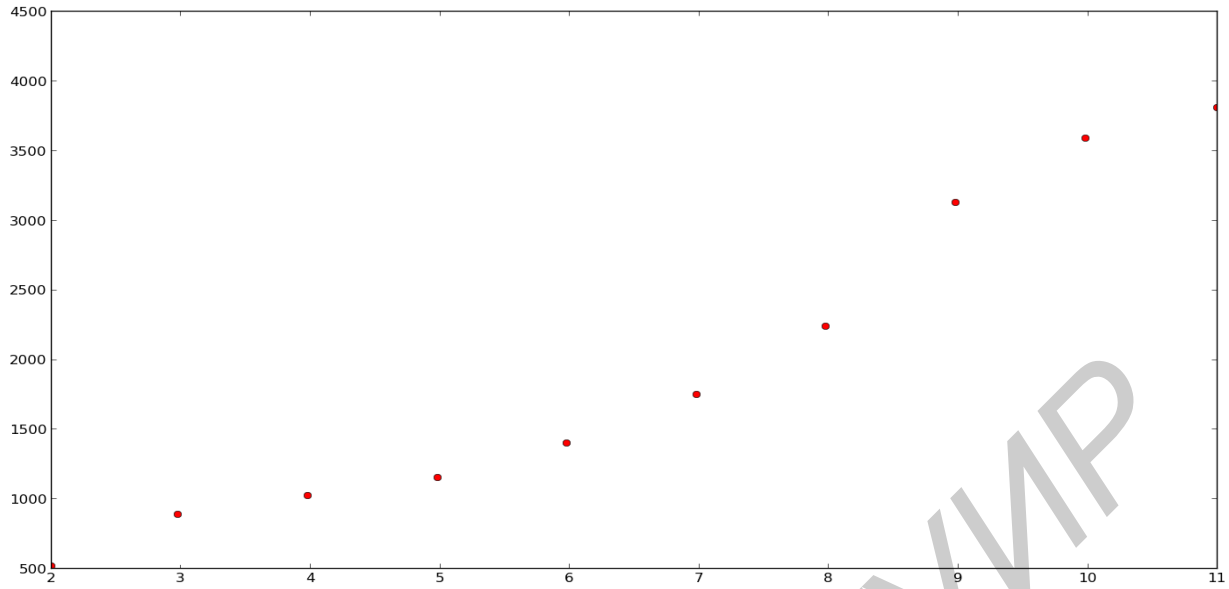

Рисунок 4 – График зависимости среднего количества сообщений от L при конфигурации сетис обратной связью при параметрах K=4, N=4

В разделе 3.4 приводятся результаты для синхронизации нейронных сетей RAAM.

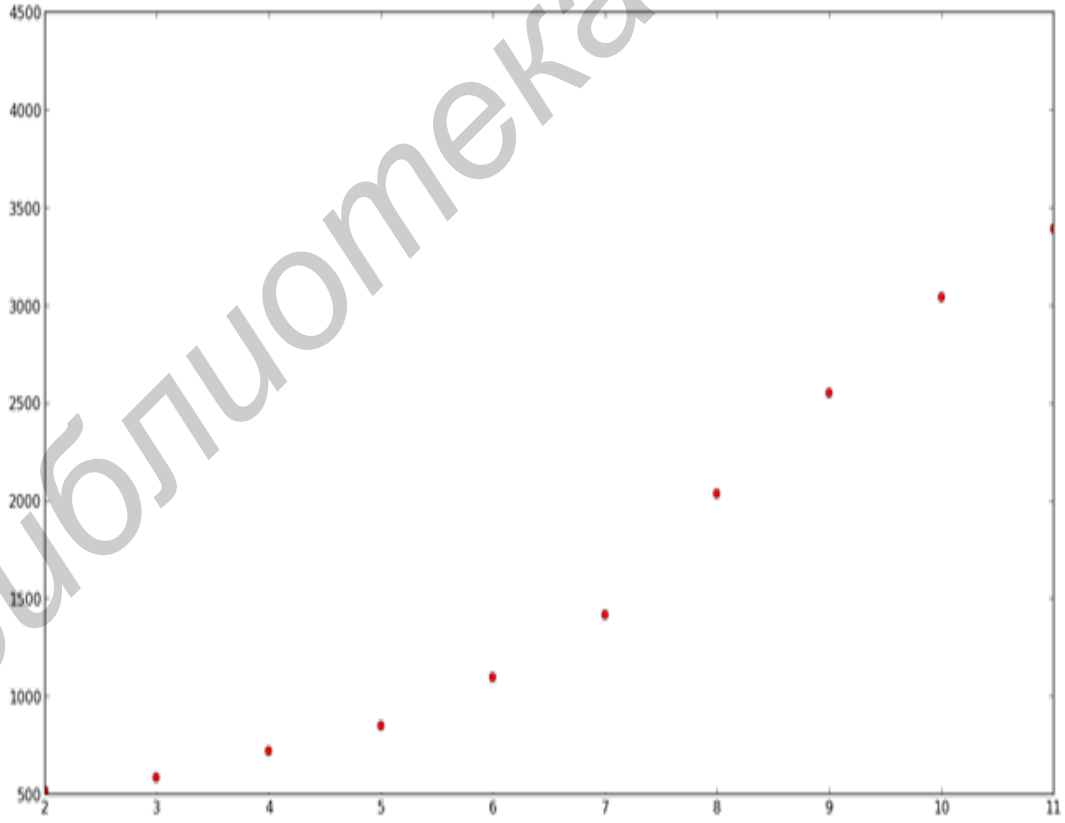

Рисунок 5 – График зависимости среднего количества сообщений от L при конфигурации сети RAMM с параметрами N=4

Также проводится оценка эффективности разработанных параллельных модификаций алгоритма вычисления нейронной сети на основе TPM.

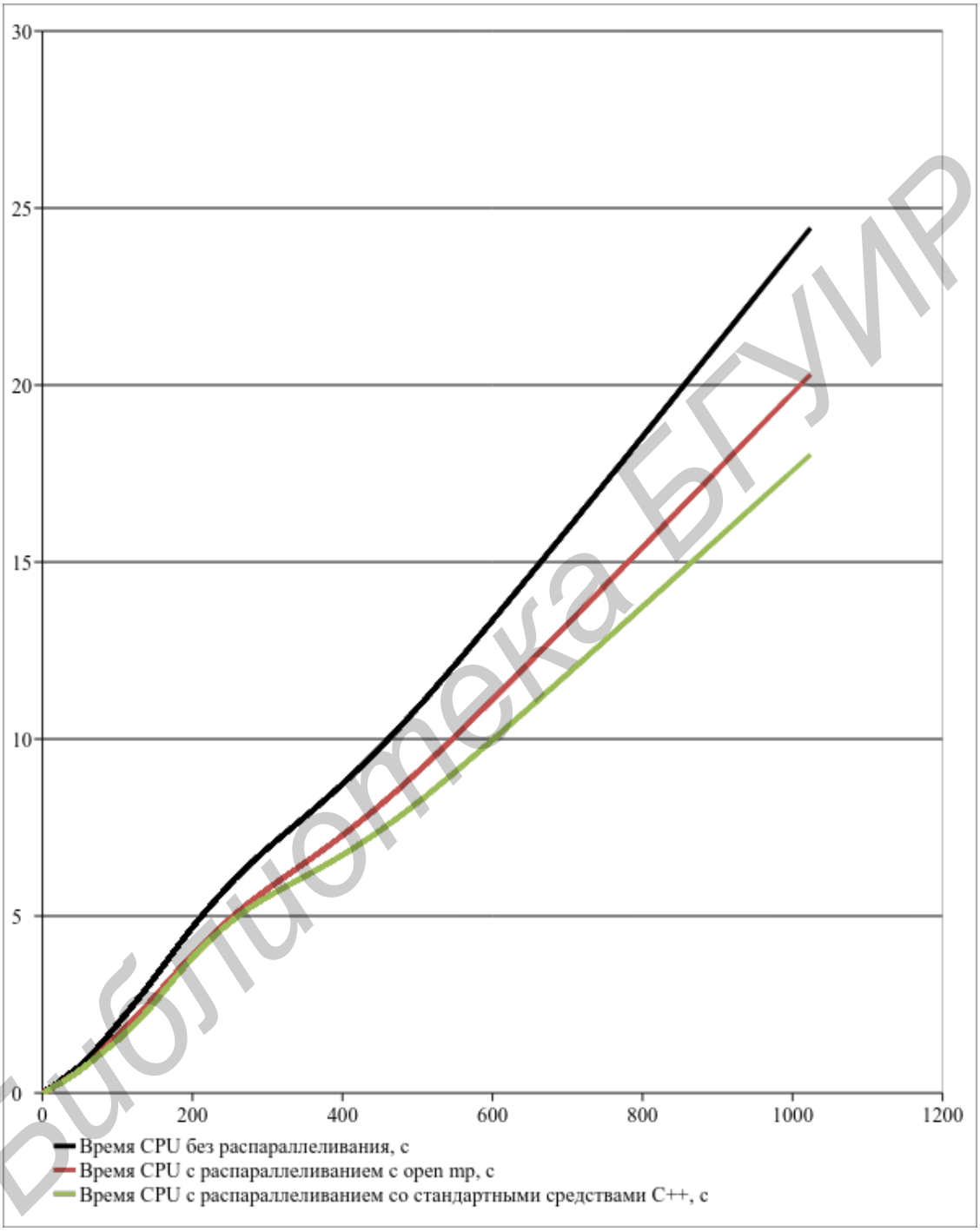

Рисунок 6 – График зависимостей среднего времени синхронизации при конфигурации сети K=4, L=3, количестве потоков p = 2 с использованием open mp и стандартных средств распараллеливания c++

Данные экспериментов показывают что во время проведения исследований было замечено, что можно ускорить синхронизацию, распараллелив некоторые логические части. В результате получился выигрыш в 1.2-1.5 раза по сравнению с запуском для одного потока при распараллеливании с помощью open mp, а при использовании распараллеливания с помощью стандартных средств c++ выигрыш получается еще больше .

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В результате написания работы над магистерской диссертацией были получены следующие результаты:

1. Проанализирован математический аппарат существующих подходов к построению криптографических систем на основе нейронных сетей. Предложены и реализованы модификации и новые методы построения криптосистем на базе нейронных сетей. Была математически обоснована и практически доказана эффективность применения данных методов в практических целях
2. Были рассмотрены математические модели процесса синхронизации нейронных систем, нейронных сетей с хаотичным отображением, а также модель нейронных сетей с обратным распространением. Был проведен анализ достоинств и недостатков каждого из методов
3. Показана возможность применения различных методов к построению криптографических систем на основе нейронных сетей.
4. Был разработан программный модуль для удобного проведения экспериментов с использованием различных нейронных сетей и использованием различных методов построения криптографических систем, а также добавления новых.
5. Экспериментальным путем была доказана эффективность построения криптографических систем на основе нейронных сетей. Результаты экспериментов показали быстрое время синхронизации нейронных сетей в построенной криптографической системе и, что скорость синхронизации сетей позволяет использовать такой подход к построению криптографических систем и их последующему применению.
6. Также показана перспектива дальнейшего ускорения работы систем за счет распараллеливания вычислений для некоторых нейронных сетей в 1.2-1.5 раза.
7. Реализована обертка для xmpp-протокола с использованием построенной криптографической системы на основе нейронных сетей, как пример практического применения.

Основные результаты проделанной в рамках магистерской диссертации работы были представлены на «51-ой научной конференции аспирантов, магистрантов и студентов БГУИР» по направлению компьютерные системы и сети [1-А], а также на III Международной научно-технической интернет конференции "Информационные

технологии в образовании, науке и производстве" (Международный институт дистанционного образования (МИДО) БНТУ, Минск, Беларусь, 2015) [2-А].

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют отличную теоретическую базу для изучения методов построения криптографических систем на основе нейронных сетей.

2. Разработанные методы могут быть применены в области построения криптографических систем.

3. Полученные экспериментальные данные могут послужить основой для дальнейших исследований в области построения криптографических систем на основе нейронных сетей, а также намечены пути развития и улучшения разработанных методов.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Плехова, Т.В. Методы построения и синхронизации криптографических систем на основе нейронных сетей / Т.В. Плехова, В.Н. Ярмолик // 51-я научная конференция аспирантов, магистрантов и студентов по направлению 4: Компьютерные системы и сети: Тезисы докл. – Минск : БГУИР, 2015. – с. 67-69.

2-А. Грицкевич, Т.В. Исследование построения криптографических систем на основе нейронных сетей / Т.В. Грицкевич, В.Н. Ярмолик // III Международная научно-техническая интернет конференция "Информационные технологии в образовании, науке и производстве" Тезисы докл. – Минск: Международный институт дистанционного образования (МИДО) БНТУ, Минск, Беларусь, 2015. – с. 250-254