АННОТАЦИЯ

диссертации на соискание ученой степени доктора философии (PhD) по специальности 6D070300 – «Информационные системы»

БАПИЕВА ИДЕЯТА МЭЛСОВИЧА

Нейросетевые модели и методы противодействия атакам на сетевые ресурсы информационных систем

Актуальность темы. Согласно Концепции кибербезопасности «Киберщит Казахстана» [1], проявления компьютерной преступности и компьютерного терроризма относятся к основным угрозам, мешающим устойчивому и безопасному функционированию национальных информационных систем. В современных условиях системы противодействия кибератакам являются одним из основных средств защиты информации сетевых ресурсов информационных систем. Хотя используются такие системы уже не одно десятилетие, их разработкой занимается много высококвалифицированных специалистов, а созданию соответствующей научно-методической базы посвящено большое количество работ, однако практический опыт указывают на наличие в системах противодействия сетевым кибератакам ряда существенных недостатков. Основным из них является недостаточная точность распознавания всей номенклатуры сетевых кибератак, что подтверждается известными случаями успешного взлома систем защиты информации в ряде стран. Кроме этого, внедрение известных средств противодействия сетевым кибератакам в системы защиты информации отечественных информационных систем вызывает необходимость их сложной адаптации к вариативности условий использования. Также недостатками известных средств противодействия кибератакам на сетевые ресурсы информационных систем является высокая стоимость и отсутствие подробной научно-технической документации.

В такой постановке является актуальной задача разработки эффективных моделей, методов и систем противодействия сетевым кибератакам, которые бы были адаптированы к отечественным условиям применеия.

Научные исследования ученых Васильева В.И. [3], Гришина А.В. [4], Емельяновой Ю.Г. [5], Крыжановского А.В. [8], Мустафаева А.Г. [9], Слеповичева И.И. [10], Талалаева А.А. [12] и др. указывают на то, что перспективным путем повышения средств распознавания сетевых кибератак является использование в них аппарата искусственных нейронных сетей. Это объясняется доказанной эффективностью применения нейронных сетей для решения подобных задач ведущими разработчиками средств защиты информации (компании Cisco, Symantec) и доказанной адаптивностью нейросетевых средств к разнообразным условиям применения.

Методологическую и теоретическую основу для эффективного внедрения нейросетвых средств в системы противодействия атакам

составляют теоретические разработки и опыт создания систем защиты информации таких ученых как Ахметов Б.Б. [2], Корченко А.А. [6], Сухова В.Е. [11], Терейковского И.А. [13], Тимофеева А. [14], Тынынбаев С.Т. [7], Хафизова А.Ф. [15], Частиковой В.А. [16] и др.

Таким образом, задача разработки эффективных нейросетевых моделей, методов и средств противодействия кибератакам на сетевые ресурсы информационных систем обуславливает актуальность научных исследований и разработок, которым посвящена диссертационная работа.

Цель и задачи исследования. Цель работы состоит в разработке эффективных нейросетевых моделей, методов и средств противодействия кибератакам, адаптированных к условиям эксплуатации и способных оперативно распознавать новые виды сетевых кибератак.

В соответствии с поставленной целью определены следующие основные задачи исследования:

– провести анализ возможностей нейросетевых средств противодействия кибератакам на сетевые ресурсы информационных систем;

– развить методологическую базу нейросетевого противодействия кибератакам на сетевые ресурсы информационных систем;

– разработать нейросетевые модели и методы противодействия сетевым кибератакам;

– разработать нейросетевую систему противодействия сетевым кибератакам и провести экспериментальные исследования, направленные на верификацию предложенных решений.

Объект исследования – процессы противодействия кибератакам на сетевые ресурсы информационных систем.

Предмет исследования – нейросетевые модели, методы и средства противодействия кибератакам на сетевые ресурсы информационных систем.

Методы исследования – методы теории цифровой обработки сигналов, нейронных сетей, экспертного анализа, математической статистики и оптимизации.

Научная новизна полученных результатов состоит в том, что теоретические и практические исследования дозволили разработать и научно обосновать принципы, модели и методы нейросетевого противодействия кибератакам на сетевые ресурсы информационных систем.

Впервые:

– разработан метод создания обучающей выборки для нейросетевого противодействия сетевым кибератакам, который за счет определения параметров допустимых видов выборки и учета в выходном сигнале близости эталонов видов кибератак, позволяет определить круг допустимых видов нейросетевых моделей и обеспечить уменьшение количества учебных итераций;

– разработан метод нейросетевого противодействия кибератакам на сетевые ресурсы информационных систем, который за счет использования

разработанных нейросетевых моделей и разработанного метода создания обучающей выборки, позволяет расширить функциональные возможности и обеспечить достаточную точность распознавания.

Получили дальнейшее развитие:

− методологическая база нейросетевого противодействия кибератакам на сетевые ресурсы информационных систем, которая за счет учета условий создания таких средств, обеспечила возможность создания эффективных нейросетевых моделей и методов противодействия;

− нейросетевые модели противодействия, которые за счет возможности обучения с помощью экспертных данных и использования комбинированной обучающей выборки, позволяют оперативно реагировать на новые типы сетевых кибератак.

Практическое значение полученных результатов. Предложенные нейросетевые модели и методы позволили разработать архитектуру нейросетевой системы, которая адаптируясь к условиям создания и эксплуатации, позволяет с достаточной точностью распознавать основные виды сетевых кибератак, а также могут быть использованы для создания инструментальных средств.

Практическая ценность состоит в следующем:

− использование разработанного метода создания обучающей выборки позволяет приблизительно в 2,4 раза уменьшить количество учебных итераций нейросетевой модели, что подтверждается актом внедрения в деятельность Научно-исследовательского центра «Тезис» КПИ им. И. Сикорского (акт внедрения от 11.09.2017);

− применение разработанного метода нейросетевого распознавания сетевых кибератак позволяет приблизительно в 1,35 раз повысить эффективность нейросетевых средств распознавания сетевых кибератак, что подтверждается актом внедрения в деятельность ООО «Безопасность информационных систем «Дельта»» (акт внедрения от 09.10.2017);

− разработанные программы, реализующие предложенные модели и методы, внедрены в учебный процесс на кафедре безопасности информационных технологий Национального авиационного университета (Киев, Украина) (акт внедрения от 25.07.2017) и на кафедре информационные системы Западно-Казахстанского аграрно-технического университета имени Жангир хана (акт внедрения от 04.09.2017).

Личный вклад соискателя. В работах, опубликованных в соавторстве, соискателю принадлежат: разработка нового метода создания обучающей выборки для нейросетевого противодействия сетевым кибератакам, который за счет определения параметров допустимых видов выборки и учета в выходном сигнале близости эталонов видов кибератак, позволяет определить круг допустимых видов нейросетевых моделей и обеспечить уменьшение количества учебных итераций приблизительно в 2,4 раза; разработка метода нейросетевого противодействия кибератакам на сетевые ресурсы информационных систем, который за счет использования разработанных нейросетевых моделей и

разработанного метода создания обучающей выборки, позволяет расширить функциональные возможности и обеспечить достаточную точность распознавания кибератак. С использованием предложенных моделей и методов, разработана и исследована нейросетевая система противодействия кибератакам на сетевые ресурсы информационных систем. В отличии от известных нейросетевых средств, в данной системе предусмотрено использование подсистем определения условий создания нейросетевых средств, формирования адаптивной обучающей выборки и разработки нейросетевых моделей, что обеспечивает достаточную точность распознавания и адаптацию к условиям разработки и применения. Экспериментальным путем показано эффективность предложенной нейросетевой системы приблизительно в 1,35 раз выше по отношению к наилучшим подобным системам, а при ожидаемых условиях применения ее использование позволит обеспечить ошибку распознавания сетевых кибератак в пределах 0,05, что достаточно для практического использования.

Апробация результатов диссертации. Основные результаты диссертационной работы докладывались и обсуждались на семинарах кафедры «Информационные технологии» КазНИТУ имени К.И. Сатпаева и на международных научно-практических конференциях:

– II международная научно-практическая конференция «Актуальные вопросы обеспечения кибербезопасности и защиты информации», Европейский университет (Украина, г. Киев, 24-27 февраль 2016);

– III Международная научно-практическая конференция «Актуальные вопросы обеспечения кибербезопасности и защиты информации», Европейский университет (Украина, Киев, 22-25 февраль 2017);

– IV International scientific conference «Global and regional problems of informatizition in society and nature using'2016», National University of Life and Environmental Sciences of Ukraine (Ukraine, Kyiv, 23-24 of June 2016);

– V International scientific conference «Global and regional problems of informatizition in society and nature using'2017», NULES of Ukraine (Ukraine, Kyiv, 22-23 of June 2017);

– The 15th International Scientific Conference Information Technologies and Management, ISMA University – Satbayev University, (Latvia - Kazakhstan, Riga - Almaty, April 27-28, 2017);

– Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2017), Миколаїв – Коблево: МТУ «Миколаївська політехніка» (Украина, Николаево - Коблево, 20-23 июнь 2017г).

Публикации. Основные результаты, полученные при выполнении диссертационной работы опубликованы в 14 печатных работах, из которых 4 статьи опубликованы в издании, рекомендованном Комитетом по контролю в сфере образования и науки МОН РК, 1 статья опубликована в издании, индексируемой базой Scopus, 1 статья опубликована - в международном журнале (Академия Естествознания), 1 статья опубликована - в зарубежном журнале (Украина), 6 статей опубликованы в зарубежных сборниках

международных научно-практических конференций (Украина, Латвия), 1 статья опубликована в отечественном сборнике международной научно-практической конференции (Казахстан).

Объем и структура диссертации. Диссертация состоит из введения, четырех разделов, заключения, списка использованных источников из 106 наименований и 6 приложений. Общий объем работы 124 страниц. Работа содержит 25 рисунков, 7 таблиц.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Концепция кибербезопасности («Киберщит Казахстана»), утвержденная постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 [Электронный ресурс] - Режим доступа: http://mdai.gov.kz/ru/pages/ koncepciya-kiberbezopasnosti-kibershchit-kazahstana (дата обращения: 16.12.2017)
2. Ахметов Б.Б. Параметры оценки эффективности нейросетевых средств распознавания кибератак на сетевые ресурсы информационных систем / Б.Б. Ахметов, А.Г. Корченко, И.А. Терейковский, Ж.М. Алибиева // Reports of the national academy of sciences of the republic of Kazakhstan. ISSN 2224-5227. Volume 2, Number 312 (2017)
3. Васильев В.И. Нейронные сети при обнаружении атак в сети Internet (на примере атаки SYNFLOOD) / В.И. Васильев, А.Ф. Хафизов // Нейрокомпьютеры в информационных и экспертных системах. – М.: Радиотехника, 2007. – №6. – С. 34-38.
4. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак / А.В. Гришин // Информационные технологии и вычислительные системы – 2011. – №1. – С. 53 - 64.
5. Емельянова Ю. Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю. Г. Емельянова, А.А. Талалаев, И.П. Тищенко, В.П. Фраленко // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3-15.
6. Корченко А.Г. Определение эффективных видов нейросетевых моделей распознавания кибератак на сетевые ресурсы / А.Г. Корченко, И.А. Терейковский, Л.А. Терейковская, Б.Б. Ахметов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (32), 2016 р.
7. Корченко А.Г. Нейросетевые модели, методы и средства оценки параметров безопасности Интернет-ориентированных информационных систем: монография / А. Корченко, И. Терейковский, Н. Карпинский, С. Тынымбаев. – К. : ТОВ «Наш Формат». – 2016. – 275 с.
8. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак / А.В. Крыжановский // Доклады ТУСУРа. – 2008. – № 2 (18), часть 1. – С. 37-41. URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-v-sistemah-obnaruzheniya-atak

9. Мустафаев А.Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. – 2016. – № 2. – С.1-7. DOI: 10.7256/2409-7543.2016.2.18834. URL: http://e-notabene.ru/nb/article_18834.html.

10. Слеповичев И.И. Обнаружение DDoS-атак нечеткой нейронной сетью / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета. – 2009. – Т. 9, сер. Математика. Механика. Информатика, вып. 3. – С. 84-89.

11. Сухов В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов // Вестник РГРТУ. – 2015. – № 54. Ч.1. – С. 84-90.

12. Талалаев А.А.Разработка нейросетевого модуля мониторинга аномальной сетевой активности / А.А. Талалаев, И.П. Тищенко, В.П.Фраленко, В.М. Хачумов // Нейрокомпьютеры: разработка и применение. — 2011. — № 7. — С. 32-38.

13. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації: монографія / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

14. Тимофеев А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевіїх атак / А.Тимофеев, А. Браницкий // International Journal Information Technologies & Knowledge. – 2012. – Vol.6, Number 3. – P. 257-265

15. Хафизов А.Ф. Нейросетевая система обнаружения атак на WWW-сервер: дис. ... канд. техн. наук : 05.13.11 / А.Ф. Хафизов. – Уфа, 2004. –172 с.

16. Частикова В.А., Власов К.А., Картамышев Д.А. Обнаружение ddos-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения / В.А. Частикова, К.А. Власов, Д.А. Картамышев // Фундаментальные исследования. – 2014. – № 8-4. – С. 829-832.