РЕЦЕНЗИЯ

официального рецензента на диссертационную работу Бапиева Идеята Мэлсовича на тему: «Нейросетевые модели и методы противодействия атакам на сетевые ресурсы информационных систем», представленной на соискание ученой степени доктора философии (PhD) по специальности 6D070900 – «Информационные системы»

1. Актуальность темы исследования и ее связь с общенаучными и общегосударственными программами (запросами практики и развития науки и техники)

Согласно государственной программе «Цифровой Казахстан» на 2017-2020 года, новые реалии диктуют необходимость постоянного увеличения скоростных параметров сетей и мощности объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним.

Вместе с тем, развитие телекоммуникационных сетей и технологий передачи данных требует принятия мер по обеспечению конфиденциальности и целостности информации. Для повышения безопасности информационных систем государственных органов Казахстана проводятся обязательные испытания объектов информатизации на соответствие требованиям информационной безопасности.

Особенности развития современного общества таковы, что вслед за обеспечением повсеместной доступности глобальной сети Интернет, наблюдается рост инцидентов информационной безопасности. По данным Kaspersky Security Network, Казахстан стал объектом 85% интернет атак в Центральной Азии, по сравнению с 8% в Узбекистане, 4% в Кыргызстане, 2% в Туркменистане и 1% в Таджикистане. До недавнего времени крупные кибератаки, главным образом, были нацелены на правительственные сайты. Эти атаки росли пропорционально развитию цифровой инфраструктуры, и Казахстан стал главным объектом атак в Центральной Азии.

Согласно исследованиям Международного союза электросвязи (ITU) «Глобальный индекс кибербезопасности (GCI)» Казахстана в 2017 г. составил 0,352, что соответствует 83 месту из 193 исследованных стран.

Таким образом, обеспечение конфиденциальности, целостности и доступности государственных информационных ресурсов априори является базовой задачей для правительств всех стран.

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

Теоретические разработки и опыт создания систем защиты информации как зарубежных, так и отечественных ученых указывают на

то, что перспективным путем повышения эффективности средств распознавания сетевых кибератак является использование в них аппарата искусственных нейронных сетей.

2. Научные результаты в рамках требований к диссертациям (пп. 2, 5, 6 «Правил присуждения ученых степеней»)

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

– разработаны: концептуальная модель обеспечения эффективности нейросетевого противодействия кибератакам, принципы использования нейронных сетей, модель правил определения эффективных видов нейросетевых моделей, модель формирования параметров учебных примеров;

– на основе применения аппарата искусственных нейронных сетей разработана нейросетевая модель противодействия сетевым кибератакам с помощью экспертных знаний и модель глубокой нейронной сети;

– разработаны: метод создания обучающей выборки и метод нейросетевого противодействия сетевым кибератакам;

– на основе указанных моделей и методов разработана нейросетевая система противодействия сетевым кибератакам и проведены экспериментальные исследования, направленные на верификацию предложенных решений;

– указанные результаты внедрены в учебный процесс на кафедре безопасности информационных технологий Национального авиационного университета (Киев, Украина) и на кафедре информационные системы Западно-Казахстанского аграрно-технического университета имени Жангир хана (акт внедрения от 04.09.2017)

3. Степень обоснованности и достоверности каждого научного результата (положения), выводов и заключения соискателя, сформулированных в диссертации.

Полученные результаты и сформулированные выводы являются обоснованными и достоверными, т.к. диссертант в работе использовал целый комплекс достаточно точных классических и современных методов исследования (методы теории цифровой обработки сигналов, нейронных сетей, экспертного анализа, математической статистики и оптимизации и др.)

4. Степень новизны каждого научного результата (положения), выводов и заключения соискателя, сформулированных в диссертации.

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.

5. Оценка внутреннего единства полученных результатов.

Диссертационная работа обладает внутренним единством, обусловленным общей целенаправленностью работы на достижение прикладной цели, логической взаимосвязью теоритических положений и практических результатов. Все её разделы объединены основной задачей. Логическим завершением работы является испытание разработанной системы противодействия сетевым кибератакам на экспериментальной установке.

6. Направленность полученных соискателем результатов на решение соответствующей актуальной проблемы, теоритической или прикладной задачи.

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 противодействия сетевым кибератакам позволяет приблизительно в 1,35 раз повысить эффективность нейросетевых систем противодействия сетевым кибератакам, 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).

7. Подтверждение достаточной полноты публикации основных положений, результатов и заключения диссертации.

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).

8. Соответствие аннотации содержанию диссертации.

Аннотация полностью соответствует содержанию диссертации и отражает все основные ее положения.

9. Недостатки по содержанию и оформлению диссертации.

По оформлению и содержанию работы имеются следующие замечания:

1. Необходимо более четко выделить постановку задачи или конкретизировать актуальность темы.
2. Усилить методику эксперимента за счет учета других факторов.
3. В работе недостаточно внимания уделено вопросам применения нейросетевых моделей типа карты Кохонена, звезды Гросберга, что потенциально сужает полученные научно-практические результаты.

Вместе с тем, следует отметить, что данные замечания не умаляют достоинство диссертационной работы, которая представляет собой квалифицированный научный труд, который содержит результаты и положения, важные как с теоретической, так и с практической точки зрения.

10. Соответствие диссертации предъявляемым требованиям раздела 2 «Правил присуждения ученых степеней» Комитета по надзору и аттестации в сфере образования МОН РК.

Диссертационная работа Бапиева И.М. «Нейросетевые модели и методы противодействия атакам на сетевые ресурсы информационных систем» по

научной новизне, объему, значимости полученных результатов соответствует требованиям п.п. 2, 6, 7 «Правил присуждения степеней» Комитета по контролю в сфере образования и науки МОН РК, предъявляемым к работам, представленным на соискание степени доктора философии (PhD), а ее автор заслуживает присуждения искомой степени доктора философии (PhD) по специальности 6D070300 – Информационные системы.

Профессор кафедры «Инженерная
кибернетика» Алматинского университета
энергетики и связи,
доктор технических наук Утепбергенов И.Т.

ДҰРЫС
ВЕРНО
"30" 11 2018 ж.
(қолы/подпись)