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)

В целях реализации Послания Главы государства народу Казахстана от 31 января 2017 года "**Третья модернизация Казахстана: глобальная конкурентоспособность**" Правительство Республики Казахстан 30 июня 2017 года утвердило Концепцию кибербезопасности ("Киберщит Казахстана"). Согласно данной Концепции, к основным угрозам в сфере кибербезопасности относятся:

– действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

– деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

Целями Концепции являются достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

К основным задачам Концепции относится формирование необходимых условий для развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищенного телекоммуникационного оборудования.

В современных условиях к основным недостаткам систем противодействия кибератакам относятся: недостаточная точность распознавания аномальной сетевой активности, сложная адаптация к вариативности условий использования, высокая стоимость.

Перспективным путем повышения эффективности средств распознавания сетевых кибератак является использование в них аппарата искусственных нейронных сетей.

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.

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

В диссертационной работе решена актуальная научно-прикладная задача разработки эффективных нейросетевых моделей, методов и средств распознавания кибератак, адаптированных к условиям эксплуатации и способных оперативно распознавать новые виды сетевых кибератак.

Проведенные исследования позволяют сформулировать следующие выводы:

– В результате анализа научно-практических работ посвященных разработке и эксплуатации систем распознавания кибератак на сетевые ресурсы информационных систем общего назначения показано, что одним из основных путей развития указанных систем является внедрение методов анализа сетевого трафика, базирующихся на современных решениях теории искусственных нейронных сетей. Для этого необходимо развить методологическую базу нейросетевого распознавания сетевых кибератак и разработать на этой базе метод создания обучающей выборки и метод создания, соответствующих нейросетевых средств. Для апробации предложенных решений целесообразно разработать нейросетевую систему и провести исследование ее эффективности.

– Получила дальнейшее развитие методологическая база нейросетевого распознавания кибератак на сетевые ресурсы информационных систем, которая за счет учета условий создания таких средств, обеспечила возможность создания эффективных нейросетевых моделей и методов распознавания.

– Получили дальнейшее развитие нейросетевые модели распознавания, которые за счет возможности обучения с помощью экспертных данных и использования комбинированной обучающей выборки, позволяют оперативно реагировать на новые типы сетевых кибератак.

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

Полученные и представленные в диссертационной работе научные результаты опираются на строгое изложение основных положений и

применяемых методов и подтверждаются результатами проведенного исследования. Основные положения достигнутых результатов опубликованы в открытой печати, обсуждены в ряде международных и научно-практических конференций, представлены актом внедрения результатов диссертационной работы.

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

Научная новизна 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.

Полученные в диссертационном исследовании научные результаты обладают внутренним единством, так как все они являются следствием решения одной единой задачи. Оценка внутреннего единства основана на логической связи последовательности элементов разработанного метода, выраженной в составе исследований и изложенной в диссертационной работе. Степень этого единства очень высока, так как каждый полученный результат является следствием предыдущего результата.

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;

– применение разработанного метода нейросетевого противодействия сетевым кибератакам позволяет приблизительно в 1,35 раз повысить эффективность нейросетевых систем противодействия сетевым кибератакам;

– разработанные программы, реализующие предложенные модели и методы, внедрены в учебный процесс на кафедре безопасности информационных технологий НАУ (Киев, Украина) и на кафедре информационные системы ЗКАТУ имени Жангир хана, а также в деятельность Научно-исследовательского центра «Тезис» КПИ им. И. Сикорского и ТОО «Безопасность информационных систем «Дельта».

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 её положения.

9. Недостатки по содержанию и оформлению диссертации.

– хотелось бы видеть более содержательный анализ современного состояния рассматриваемой проблемы с рассмотрением результатов теоретических и экспериментальных работ по изучению нейросетевых моделей и методов противодействия атакам, анализом известных подходов к решению данной задачи и обоснованным выбором цели диссертационной работы;

– в тексте диссертации встречаются орфографические ошибки, например, на стр. 25 и далее;

– некоторые указанные ссылки [8], [15], [23], [72] в тексте диссертации не совпадают с библиографическим списком.

Следует отметить, что приведённые выше замечания и рекомендации не снижают высокого качества выполненной работы и не влияют на полученные в диссертации теоритические и практические результаты.

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 сетей» 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).

Доктор PhD, РГП на ПХВ
"Институт информационных и
вычислительных технологий"
КН МОН РК Магзом М.М.

КАДР БӨЛІМІ

Инспектор по кадрам
Жунусова С.Ш.
28.11.2018