УТВЕРЖДАЮ
Проректор
Государственное бюджетное образовательное учреждение высшего образования «Донецкий институт железнодорожного транспорта»
к. т. н., доцент
_____ Ю. В. Тимохин
«28» марта 2023 г.

ОТЗЫВ

ведущей организации о диссертации Бабичевой Маргариты Вадимовны на тему «Автоматизированные системы научных исследований угроз безопасности личности», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.3. «Автоматизация и управление технологическими процессами и производствами» (технические науки).

Актуальность для науки и практики

Создание автоматизированных систем научных исследований безопасности личности на основе искусственных нейронных сетей является научно-технической задачей, решение которой позволит повысить быстродействие, степень достоверности принятия решений такого рода систем. В настоящее время многие предприятия начинают использовать нейронные сети для прогнозирования, планирования, и управления качеством продукции. Причиной роста их популярности служит гибкость – возможность подстраиваться под конкретные нужды. Нейронные сети используются и в защите информации, где активно применяются для борьбы с различными угрозами как физическими, так и информационными. Это и системы аутентификации по биометрическим признакам, системы выявления киберугроз и технических каналов утечки информации, системы видеонаблюдения с распознаванием лиц или опасных предметов. При этом применение нейросетевых алгоритмов в подобных системах накладывает ряд ограничений, таких как значительная ресурсоемкость, затраты на время, необходимое для обучения, необходимость разработки нейронной сети для

конкретной задачи, предварительная обработка данных и т. д. Для применения в автономных автоматизированных системах необходимо помещать нейросетевые программные решения в ограниченный объем постоянной и оперативной памяти. При этом актуален вопрос уязвимостей, которыми обладают подобные системы, поскольку при получении доступа к управлению технологическим процессом или к системе аутентификации злоумышленник может нанести ощутимый вред.

Таким образом создание автоматизированных систем научных исследований на основе искусственных нейронных сетей для совершенствования систем предотвращения угроз безопасности личности, позволяющих повысить компактность, быстродействие и степень достоверности принятия решений, а также снизить уровень уязвимости нейросетевых алгоритмов на сегодняшний день является крайне актуальной научно-технической задачей, и избранная тема диссертационного исследования имеет научное и практическое значение.

Основные научные результаты и их значимость для науки и производства

Основные научные результаты диссертации, полученные соискателем:

– разработан метод сокращения количества параметров нейросетевых алгоритмов редукцией проигравших нейронов, который позволяет снизить количество параметров нейронных сетей до 30 %, повышает скорость работы и снижает ресурсоемкость программных решений;

– разработаны архитектурные решения и программная реализация двух систем обработки формализованных данных и четырех систем обработки изображений;

– исследованы уязвимости автоматизированных систем научных исследований безопасности личности на основе нейросетевых алгоритмов путем создания состязательных примеров и проведения 9-ти типов атак на классификаторы изображений и предложены методы защиты от подобных атак;

– обоснована возможность внедрения нейросетевых технологий в автономные автоматизированные системы другого назначения, например, промышленного и широкого назначения за счет уменьшения ресурсоемкости разработанных решений без понижения эффективности и качества.

Теоретическая значимость результатов диссертационной работы для науки состоит в развитии методов усовершенствования нейросетевых алгоритмов, для применения в системах предотвращения угроз безопасности личности. Практическая значимость заключается в предложенных принципах

построения компактных нейросетевых решений, которые можно использовать для прошивки микроконтроллерных устройств в автономных автоматизированных системах, разработке алгоритмов для обработки изображений в автоматизированных системах аутентификации и классификации и способов защиты автоматизированных систем безопасность личности на нейросетевых алгоритмах от атак генерацией состязательных примеров.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационных исследований имеют широкий спектр применения в разработке автоматизированных систем общего назначения и предотвращения угроз безопасности личности. Практическая ценность работы заключается в целесообразности использования результатов исследования в практической, научно-исследовательской и преподавательской деятельности. Метод, позволяющий на 70% сокращать количество параметров нейронных сетей, с сохранением и даже увеличением точности и скорости работы нейросетевых алгоритмов рекомендуется для внедрения в автоматизированных системах с ресурсными ограничениями, в частности автономными на микроконтроллерах. Алгоритмы для обработки изображений в автоматизированных системах аутентификации и классификации, а также способы защиты от атак генерацией состязательных примеров для усовершенствования систем аутентификации и видеонаблюдения. Результаты исследования могут быть использованы при чтении лекций и проведения лабораторных занятий в учебном процессе.

Общие замечания

1. В списке работ, опубликованных по теме диссертации соискатель ограничился лишь научными изданиями, рекомендуемыми ВАК ДНР. Хотелось бы видеть в этом списке работы, опубликованные и в изданиях: рекомендуемых ВАК РФ.
2. В подразделе диссертации 3.2.2.2 описан метод эйквализации гистограммы, однако ранее, в разделе 3.2.1 он был упомянут, таким образом нарушена последовательность изложения.
3. В автореферате диссертации не совсем понятно, что подразумевается под направленными и ненаправленными атаками на нейросетевые классификаторы и системы распознавания лиц.
4. В работе отсутствует обоснование использования некоторых сред разработки и библиотек.

Заключение

Диссертация представляет собой завершенную научно-исследовательскую работу, содержащую новые теоретические и практические результаты, обладает научной новизной и имеет практическую значимость. Полученные результаты диссертации соответствуют областям исследования паспорта научной специальности 2.3.3. Автоматизация и управление технологическими процессами и производствами в частности: п.3 «Методология, научные основы, средства и технологии построения автоматизированных систем управления технологическими процессами (АСУТП) и производствами (АСУП), а также технической подготовкой производства (АСТПП) и т. д», п. 16 «Средства и методы проектирования технического, математического, лингвистического и других видов обеспечения АСУ», п. 18 «Разработка автоматизированных систем научных исследований». Работа соответствует требованиям п. 2.2 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а ее автор, Бабичева Маргарита Вадимовна, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.3 - Автоматизация и управление технологическими процессами и производствами (технические науки).

Отзыв обсужден и одобрен на заседании кафедры «Автоматика, телемеханика, связь и вычислительная техника» Государственной образовательной организации высшего профессионального образования «Донецкий институт железнодорожного транспорта»

«24» 03 2023 г., протокол № 8.

Кандидат технических наук, доцент,
заведующий кафедрой «Автоматика,
телемеханика, связь и вычислительная техника»

ГБОУ ВО «ДОНИЖТ» _____ Радковский Сергей Александрович

Подпись Радковского С. А. удостоверяю.
Начальник отдела кадров
ГБОУ ВО «ДОНИЖТ» _____ Гончарук Елена Николаевна

Адрес: 283122, г. Донецк, ул. Артема, д. 184.
Тел: +7(856) 319-08-31
Email: institute-transporta@mail.ru

Я, Радковский Сергей Александрович, согласен на автоматизированную обработку персональных данных, приведенных в этом документе.

_____ Радковский С. А.

Подпись Радковского С. А. удостоверяю.
Начальник отдела кадров
ГБОУ ВО «ДОНИЖТ» _____ Гончарук Елена Николаевна

Я, Тимохин Юрий Витальевич, согласен на автоматизированную обработку персональных данных, приведенных в этом документе.

_____ Тимохин Ю. В.

Подпись Тимохина Ю. В. удостоверяю.
Начальник отдела кадров
ГБОУ ВО «ДОНИЖТ» _____ Гончарук Елена Николаевна