Отзыв

на автореферат диссертации на соискание степени доктора технических наук

Сулавко Алексея Евгеньевича,

Тема: Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта

Научная специальность: 2.3.6. Методы и системы защиты информации, информационная безопасность.

Сегодня мы наблюдаем процесс внедрения и применения технологий искусственного интеллекта (ИИ) на практике, который сопровождается устойчивой тенденцией к демократизации ИИ. Функции ИИ внедрены во множество программных продуктов. Однако с каждым годом выявляется все больше уязвимостей искусственного интеллекта, которые несут потенциальные и даже реальные риски для его использования на практике.

В диссертационном исследовании соискателя получены результаты, касающиеся обеспечения защиты искусственного интеллекта от ряда угроз информационной безопасности и компьютерных атак (декодирование знаний, состязательные атаки, зондирование искусственных нейронных сетей с целью извлечения знаний и другие). Однако целью работы является повышение надежности многофакторной биометрической аутентификации на основе защищенного исполнения нейросетевых моделей доверенного ИИ и алгоритмов их автоматического синтеза и обучения на малых выборках биометрических данных. Биометрические системы рассматриваются соискателем как частный случай систем искусственного интеллекта, что является вполне обоснованным. В работе предлагается концепция, модели искусственного интеллекта и искусственных нейронов, алгоритмы их обучения, методы и алгоритмы биометрической аутентификации с высокой точностью, технология и программный комплекс. Хотя основной акцент работы делается на биометрию, результаты вполне могут быть адаптированы и расширены для других областей применения. Это подтверждается тем, что соискателем разработан проект национального стандарта в области защиты искусственного интеллекта и его обучения на малых выборках. В связи со всем вышеуказанным, считаю, что тематика работы является актуальной, а результаты обладают высокой научной и практической значимостью, а также новизной.

Соискателем опубликованы научные статьи, коллективная монография, патент и восемь свидетельств о регистрации программ. Также Сулавко А.Е. активно принимал участие в научных конференциях, международного и всероссийского уровня.

Текст автореферата изложен грамотно, структура работы классическая – пять глав (включая обзорную, три теоритических и экспериментальных и одну практическую), список литературы из 362 источников, несколько приложений, присутствие которых в работе вполне оправдано, так как они содержат значимые для работы дополнения, акты внедрений и другую важную информацию.

Также считаю необходимым указать на замечания и недостатки работы:

1. соискатель не представил строгого математического доказательства работоспособности корреляционных нейронов с точки зрения защиты от извлечения параметров обучающей выборки (хотя в работе приводятся достаточные доводы, подкрепленные большим количеством экспериментальных данных и результатов имитационного моделирования).
2. в автореферате не уделено внимания архитектуре разработанных программных продуктов.

Указанные замечания не снижают высокой оценки диссертационного исследования. Диссертация Сулавко Алексея Евгеньевича обладает всеми необходимыми качествами и новизной, соответствует требованиям «Положения о присуждении ученых степеней», а ее автор Сулавко А.Е. заслуживает присуждения ученой степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заведующая кафедрой информатики и информационной безопасности
ФГБОУ ВО «Магнитогорский
государственный технический
университет им. Г.И. Носова»
Доктор технических наук, доцент И.И. Баранкова

Сведения об авторе отзыва:
Баранкова Инна Ильинична
Д.т.н., профессор
ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»
Адрес: 455000 Россия, Челябинская область, г. Магнитогорск, пр. Ленина, 38
Телефон:+7 (3519) 23-27-51
E-mail: Inna_Barankova@mail.ru
Докторская диссертация защищена в 2010 г. по специальности: 05.09.10 «Электротехнология».

Даю согласие на обработку персональных данных.