ОТЗЫВ НА АВТОРЕФЕРАТ ДИССЕРТАЦИИ

Сулавко Алексея Евгеньевича

на тему

«ВЫСОКОНАДЕЖНАЯ БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ЗАЩИЩЕННОГО ИСПОЛНЕНИЯ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ И АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»,

представленную на соискание ученой степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

С развитием технологий машинного обучения и искусственных нейронных сетей появляются новые угрозы информационной безопасности и риски от применения этих технологий на практике. Сегодня наиболее актуальные вопросы, касающиеся искусственного интеллекта, связаны с его способностью к бесперебойной работе в изменяющихся условиях, стойкостью и сопротивляемостью таким воздействиям, как состязательные атаки и манипуляции с данными, а также защищенностью данных, которые обрабатываются технологиями машинного обучения и находят отображение в памяти нейронных сетей. Диссертация Сулавко А.Е. как раз направлена на решение этих вопросов, которые рассматриваются в контексте проблемы повышения надёжности и защищенности биометрических систем аутентификации, которые являются частным случаем систем искусственного интеллекта.

В работе имеется 5 глав. В первой (обзорной) детально исследуется рассматриваемая проблема с разных точек зрения (наука, стандартизация и практика), во второй главе предлагается специальная концепция защиты знаний искусственного интеллекта, а также новый тип нейронов и нейронной сети, работающих в отличии от классических вариантов исполнения нейросетевых решений в так называемом «защищенном режиме». Защищенный режим создает повышенную устойчивость к анализу логики работы нейронной сети, данных нейронной сети и к атакам, направленным на дестабилизацию (формирование неверных решений). Третья глава посвящена борьбе с дрейфом – ухудшением работы искусственного интеллекта при изменении закономерностей в данных. Предложена модель искусственного интеллекта, сочетающая в себе признаки нейронной сети и иммунной системы, которая способна дообучаться, чтобы снизить негативное влияние дрейфа. Разработано два алгоритма обучения. Четвертая глава посвящена многофакторной биометрической аутентификации с помощью рукописных подписей и паролей, голосовых характеристик и параметров внутреннего строения уха. Достигнуты высокие показатели точности. Пятая глава описывает созданную технологию, а также национальный стандарт и программные продукты разработанные на базе этой технологии научной группой соискателя под его руководством. Описаны все внедрения соискателя.

Работа обладает высокой ценностью как с точки зрения теории машинного обучения и науки о данных, так и с точки зрения практики. Все положения диссертации являются новыми и опубликованы в научных работах в журналах из перечня ВАК, а также в журналах из баз цитирования Scopus и Web of Science.

К работе имеются следующие замечания:

1. В автореферате не описано, каким образом проверялась устойчивость модели искусственной иммунной сети к дрейфу?
2. Не продемонстрирована разница между концептуальным дрейфом и дрейфом данных, в связи с чем не ясно, какой из видов дрейфа будет учитываться при построении алгоритма обучения адаптивной нейро-иммунной модели.

Не смотря на данные замечания считаю, что диссертационное исследование Сулавко А.Е. является законченной научно-квалификационной работой, выполненной на высоком уровне. Тематика работы актуальна. Все положения и ключевые результаты работы научно обоснованы, обладают научной новизной и практической ценностью. Диссертация соответствует п. 9 «Положение о присуждении ученых степеней», а ее автор Сулавко Алексей Евгеньевич заслуживает присуждения ученой степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Доктор технических наук, профессор,

Почетный работник сферы образования РФ

Ажмухамедов Искандар Маратович

Декан факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева» тел.: +79276636007

Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный университет им. В.Н. Татищева»

ул. Татищева, 20а, г. Астрахань, 414056 тел. 8 (8512) 24-64-00; факс: 8 (8512) 24-68-64

Даю согласие на обработку персональных данных.

Докторская диссертация защищена по специальностям:

05.13.01 – Системный анализ, управление и обработка информации

05.13.19 – Методы и системы защиты информации, информационная безопасность