Отзыв на автореферат докторской диссертации

Сулавко Алексея Евгеньевича

«Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта»

Специальность: 2.3.6 – Методы и системы защиты информации, информационная безопасность

Диссертационная работа затрагивает две ключевые и актуальные на сегодняшний день тематики – многофакторная биометрическая аутентификация и доверенные системы искусственного интеллекта. Автор диссертационного исследования, Сулавко Алексей Евгеньевич, провел обширный анализ существующих методов биометрической аутентификации и выявил их недостатки, связанные с низкой надежностью и уязвимостью к атакам злоумышленников. В своей работе автор предлагает новый подход к биометрической аутентификации, основанный на защищенном выполнении нейросетевых моделей и алгоритмов искусственного интеллекта (ИИ).

Большой акцент в работе сделан на создание и обучение моделей доверенного ИИ, обладающего такими важными свойствами, как робастность обучения, безопасность использования, устойчивость к деструктивным воздействиям и дрейфу данных. Системы ИИ, обладающие в недостаточной мере указанными свойствами, не смогут считаться заслуживающими доверия в связи со значительными рисками от их внедрения в реальные бизнес-процессы.

Согласно автореферату, диссертационная работа включает в себя введение, пять глав, заключение, список сокращений, список литературы и приложения. Вводная часть работы подчеркивает рост числа научных работ и рынка биометрии и представляет новые вызовы, с которыми сталкиваются биометрические системы. Такие вызовы включают увеличение объемов данных пользователей в сети Интернет, использование искусственного интеллекта для атак и разработку систем аутентификации на базе биометрических образов, подверженных изменениям. В целом работа является весьма актуальной как с точки зрения информационной безопасности, так и с точки зрения теории машинного обучения.

Первая глава диссертации содержит обзор литературы, а также стандартов в области защиты искусственного интеллекта от компьютерных атак. Во второй и третьей главах работы предложены новые модели искусственных нейронов, нейронных и нейро-иммунных сетей, способных повысить длину ключа для специальных систем защиты, называемых преобразователями «биометрия-код», в соответствии с требованиями практики применения таких систем, а также предотвратить или снизить влияние концептуального дрейфа биометрических данных. Четвертая глава связана непосредственно с разработкой методов и алгоритмов высоконадежной биометрической аутентификации. В ходе исследования автор протестировал предложенные методы и алгоритм на реальных данных. Результаты тестирования показали низкий процент ошибочных решений по сравнению с другими методами распознавания биометрических образов. В целом полученные результаты обладают высокой теоритической значимостью, а также научной новизной.

Разработанные концепция, нейросетевые модели и алгоритмы их обучения, а также предложенная технология могут быть применены не только для усиления биометрических систем защиты, но и в других отраслях, в частности, в медицине. Это подтверждается

внедрением результатов диссертационной работы в бюджетном учреждении здравоохранения Омской области "Медико-санитарная часть № 4". Помимо использования результатов на практике (в программных продуктах) имеется внедрения в учебный процесс двух ВУЗов – ФГАОУ ВО ОмГТУ и ФГАОУ ВО СПбГЭТУ «ЛЭТИ».

Обозначим ряд замечаний к работе и автореферату:

1. Рисунок 2 построен не очень удачно и, возможно, нуждается в дополнительных пояснениях. В частности требуется разъяснить наименования осей и значения на них.
2. В автореферате не отражено, в каком формате подавились данные на вход экспериментальных автокодировщиков при процедуре извлечения признаков из усредненных спектров: изображения спектрограмм или их числовые характеристики.
3. В автореферате не расшифрована аббревиатура ПФС – психофизиологическое состояние человека.

Приведенные выше замечания не снижают общей положительной оценки работы.

Выполненное диссертационное исследование заслуживает высокой оценки, результаты обладают практической и теоритической значимостью, а также научной новизной. Диссертация соответствует требованиям пунктов 9-14 Положения о присуждении учёных степеней, а Сулавко Алексей Евгеньевич заслуживает присуждения учёной степени доктора технических наук по специальности 2.3.6.– Методы и системы защиты информации, информационная безопасность.

Доктор технических наук, доцент,
заведующий лабораторией медицинской кибернетики,
профессор кафедры цифровых технологий
факультета компьютерных наук Туровский Ярослав Александрович

федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет»
Адрес места основной работы: 394018, Россия, Воронежская область,
г. Воронеж, Университетская площадь, д. 1
Рабочий телефон: +7 (473) 220-83-84
Адрес эл. почты: yaroslav_turovsk@mail.ru

Докторская диссертация защищенапо специальности 05.13.01 - Системный анализ, управление и обработкаинформации (информационные технологии)

федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет» (ФГБОУ ВО «ВГУ»)
Подпись Туровского Я. А.
заверяю ведущий специалист
должность
Алексеева 30.08.23
подпись, расшифровка подписи