«УТВЕРЖДАЮ»

Проректор по научной и
исследовательской деятельности
ФГАОУ ВО «Южный федеральный
университет»
доктор химических наук, с.н.с.
_____ А. В. Метелица
«13» _____ 2023 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» на диссертационную работу Сулавко Алексея Евгеньевича «Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта»,
представленной на соискание учёной степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность работы

В диссертации Сулавко А.Е. рассматривается важная научно-техническая проблема в сфере информационной безопасности: повышение надежности многофакторной биометрической аутентификации и защищенности биометрических систем от компьютерных атак на основе технологии защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта.

Биометрические системы позволяют достичь высокого уровня безопасности процедур аутентификации и идентификации на основе физиологических и поведенческих характеристик человека, таких как отпечаток пальца, голос, лицо или сетчатка глаза. Однако, несмотря на повсеместность использования и уникальность биометрических характеристик, биометрические системы уже сегодня оказываются подвержены множеству потенциальных атак и разрушительных факторов.

Последние годы серьезно возрастают риски нарушения приватности биометрических данных и несанкционированного доступа к такой «чувствительной» информации. Чтобы обеспечить безопасность

биометрической системы, а также циркулирующих в ней конфиденциальных данных недостаточно просто использовать современные криптографические алгоритмы. Сегодня ряд стандартов предъявляет требования не только к алгоритмам шифрования биометрических данных, но и к самой архитектуре искусственного интеллекта, которая лежит в основе биометрической системы и позволяет ей функционировать бесперебойно. В связи с этим, диссертационная работа Сулавко А.Е. является особенно актуальной.

Предметом исследования представленной диссертационной работы являются нейросетевые модели и алгоритмы машинного обучения на малых выборках для высоконадежной биометрической аутентификации и защиты биометрических данных от компрометации. В диссертации Сулавко А.Е. проведено комплексное исследование, нацеленное не только на повышение надежности и снижение количества ошибок аутентификации, но и на построение моделей искусственного интеллекта специально для таких задач, устойчивых к состязательным атакам и другим деструктивным воздействиям, а также позволяющим хранить биометрические шаблоны, не компрометируя их даже без применения средств шифрования.

Структура и содержание диссертационной работы и автореферата

Работа состоит из введения, пяти глав, заключения, списка сокращений, списка литературы и приложений. Общее количество страниц – 391, включая 108 рисунков и 28 таблиц. Библиографический список насчитывает 362 источника.

Во введении сформулированы цель и задачи диссертационного исследования, обозначена его актуальность, перечислены элементы научной новизны работы и практической значимости результатов.

В первой главе даны определения ключевых понятий, а также описаны основные критерии доверенного искусственного интеллекта. Определены недостатки существующих решений в области высоконадежной биометрической аутентификации. Проведен анализ существующих стандартов по защите искусственного интеллекта от угроз информационной безопасности.

Во второй главе разработана концепция защищенного исполнения нейросетевых алгоритмов искусственного интеллекта и модель корреляционных нейронов для высоконадежной биометрической аутентификации – нового класса нейронов, анализирующих корреляционные связи между признаками вместо признаков. Предложена модель нейросетевого преобразователя биометрия-код на основе корреляционных

нейронов и алгоритм ее автоматического обучения на малых выборках биометрических данных.

В третьей главе проведён анализ подходов к построению адаптивных моделей искусственного интеллекта (моделей, способных к онлайн-обучению), включая методы глубокого обучения с подкреплением, эволюционный и иммунный подходы. В результате проведенного анализа выделен класс нейро-иммунных моделей, соединяющих в себе элементы аппаратов искусственных нейронных сетей (ИНС) и искусственных иммунных систем (ИИС). Разработан алгоритм обучения с учителем указанного класса моделей.

Четвёртая глава посвящена высоконадежной многофакторной аутентификации и безопасному комплексированию независимых биометрических признаков. Представлены комплексный метод и алгоритм высоконадежной трехфакторной аутентификации на основе биометрических признаков (акустический образ уха и два других дополнительных образа – рукописный почерк и голосовой фрагмент). Особое внимание уделено новому типу биометрических данных – эхограммам ушного канала, которые характеризуют внутреннее строение уха.

В пятой главе описываются разработанная технология автоматического синтеза и обучения нейросетевых моделей доверенного искусственного интеллекта. Обозначены ключевые положения первой редакции разработанного национального стандарта, основанного на данной технологии. Приведено описание внедрений результатов работы на примере ряда организаций, в том числе на базе образовательных учреждений.

В заключении приведены основные результаты диссертационного исследования.

В целом, диссертационная работа имеет четкую структуру, последовательные и взаимосвязанные разделы.

Автореферат достаточно полно раскрывает основное содержание диссертации. Полученные результаты соответствуют паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Новизна исследований и полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертационной работе, состоят в разработке научно-обоснованного концептуального подхода, методов, моделей и алгоритмов решения

поставленных в диссертации задач. К новым научным результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Концепция защищенного исполнения нейросетевых алгоритмов искусственного интеллекта (ИИ), позволяющая обеспечить устойчивость моделей и алгоритмов ИИ к извлечению знаний в задачах классификации образов, которая в отличие от существовавших ранее концепций основана на преобразовании корреляционных связей между признаками в высокоинформативные мета-признаки с помощью предложенного для этой цели отображения. Отображение позволяет перейти из исходного пространства признаков в пространство мета-признаков Байеса-Минковского.

2. Модель корреляционных нейронов и модель нейросетевого преобразователя биометрия-код (НПБК) на их основе, отличающиеся тем, что новые нейроны анализируют корреляционные связи между признаками вместо признаков. Предложен устойчивый алгоритм автоматического синтеза и обучения этих моделей на малых выборках, что позволяет повысить защищенность биометрических данных от компрометации, длину ключа, связываемого с биометрическими образами субъектов, и сопротивляемость систем биометрической аутентификации к состязательным атакам.

3. Адаптивная нейро-иммунная модель ИИ, отличающаяся от существовавших ранее использованием предложенной гибкой архитектуры искусственных антител и клеток памяти (иммунных детекторов), базирующихся на ядерных функциях, сочетанием ансамблевых методов машинного обучения и метода обучения с подкреплением, что позволяет модели устойчиво обучаться на малых выборках и адаптироваться к изменению биометрических данных в процессе функционирования.

4. Методы и алгоритм высоконадежной многофакторной биометрической аутентификации, отличающиеся использованием новых акустических биометрических параметров, характеризующих внутреннее строение ушного канала, комплексированием динамических и статических признаков с учетом их приоритезации, информативности и стабильности, а также совместным использованием НПБК и нейро-иммунной модели, что позволяет обеспечить более высокую надежность аутентификации, робастность дрейфующих характеристик, защиту биометрических образов от компрометации, а также снизить вероятность ошибок «ложного допуска» и «ложного отказа» по сравнению с известными аналогами.

5. Технология синтеза нейросетевых моделей доверенного ИИ, которая позволяет снизить объем тренировочной выборки, повысить

надежность и защищенность биометрических систем аутентификации и других приложений ИИ, отличающаяся наличием режимов автоматического обучения нейросетевых моделей ИИ, защищенного исполнения нейросетевых алгоритмов классификации образов и применением процедур автоматической оценки информативности признаков.

Значимость полученных результатов для науки и практики

Теоретическая значимость результатов диссертационной работы заключается в предложенных концепции, моделях нейронов и ИИ, а также алгоритмах обучения этих моделей. Полученный математический аппарат позволяет комплексно подойти к решению проблемы повышения надёжности многофакторной биометрической аутентификации, а также может быть экстраполирован на решение других актуальных проблем и задач, связанных с обеспечением защиты приложений ИИ от компьютерных атак.

Практическая значимость полученных автором диссертации результатов состоит в разработке первой редакции государственного национального стандарта ГОСТ Р «Искусственный интеллект. Нейросетевые алгоритмы в защищённом исполнении. Автоматическое обучение нейросетевых моделей на малых выборках в задачах классификации», а также интеграции полученных результатов в ряд программных продуктов. Отдельной значимостью обладают разработанные методы высоконадежной многофакторной биометрической аутентификации по особенностям ушного канала.

Полученные результаты прошли практическую апробацию, подтвержденную актами внедрения. Значение полученных результатов исследования для практики дополнительно подтверждается тем, что имеется патент на изобретение, автором которого является соискатель.

Обоснованность и достоверность основных выводов и положений

Достоверность защищаемых положений и выводов диссертационной работы подтверждается соответствием результатов вычислительного моделирования и натурных экспериментов, апробацией разработанных концепции, моделей, методов и алгоритмов при решении практических задач, а также экспертной оценкой, проведенной при публикации результатов и их внедрении на практике. Достоверность результатов, представленных соискателем в диссертации, не вызывают сомнения.

Все положения, выносимые на защиту, подтверждаются теоретическими обоснованиями и не противоречат известным положениям теории и практики

информационной безопасности. Результаты математически обоснованы и получены на основе численного и компьютерного моделирования, при этом применялись общепризнанные методики статистической обработки данных, что свидетельствует об их достоверности.

Публикации по теме диссертации

Результаты диссертационной работы опубликованы в 80 научных работах, в том числе опубликовано 38 статей в журналах из Перечня, рекомендуемых ВАК, либо в научных изданиях, индексируемых базой RSCI. 21 научная работа опубликована в изданиях, включенных в базы Web of Science и Scopus. Получен 1 патент на изобретение и 8 свидетельств о регистрации программ для ЭВМ.

Рекомендации по использованию результатов и выводов диссертации

Полученные в диссертационной работе результаты могут быть использованы различными предприятиями и организациями для повышения надежности биометрической аутентификации, защиты биометрических персональных данных и систем от компьютерных атак. Также разработанные модели ИИ и алгоритмы их обучения могут быть адаптированы для использования в других задачах, которые сводятся к классификации образов. Созданные на базе предлагаемой соискателем технологии программные модули могут применяться при разработке различных интеллектуальных приложений и в рамках исследований, связанных с машинным обучением. В частности, корпоративная среда управления жизненным циклом ИИ AICPlatform позволяет контролировать рабочие процессы на всех этапах цифровой трансформации: от исследования и разработки моделей машинного обучения до их внедрения в бизнес-среду и контроля их эффективности. Пользователями данной системы могут быть ИТ-подразделения организаций, отвечающие за процесс цифровой трансформации бизнес-процессов, ВУЗы, а также организации, занимающиеся заказной разработкой искусственного интеллекта. Область применения технологии и программного комплекса не ограничивается только сферой информационной безопасности, но и затрагивает финансовую сферу, телемедицину, дистанционное образование и другие отрасли, где требуется создавать и обучать на малых выборках в автоматическом режиме модели доверенного ИИ.

Отдельно стоит отметить, что на базе результатов может быть основана серия национальных стандартов, проект первого из них уже разработан под

руководством соискателя ГОСТ Р «Искусственный интеллект. Нейросетевые алгоритмы в защищённом исполнении. Автоматическое обучение нейросетевых моделей на малых выборках в задачах классификации». Данный стандарт может быть дополнен другими при необходимости (например, стандартами с описанием терминологии в области защищенного исполнения нейросетевых алгоритмов, а также регламентирующими процесс тестирования сетей корреляционных нейронов).

Учитывая, что представленные в диссертации материалы хорошо методологически проработаны и внедрены в учебный процесс ФГАОУ ВО СПбГЭТУ «ЛЭТИ» и ФГАОУ ВО «ОмГТУ», целесообразно использование полученных результатов в высших учебных заведениях для подготовки студентов по направлениям, связанным с информационной безопасностью и искусственным интеллектом.

Замечания по работе

1. В работе говорится, что для усиления защитных свойств корреляционных нейронов может быть применен механизм защищенного нейросетевого контейнера с использованием криптографических преобразований. В работе нет обстоятельного объяснения того, насколько защитные свойства нейронов повысятся и для чего это может быть необходимо.

2. Выбор некоторых гиперпараметров нейросетевых моделей недостаточно четко обоснован. Например, возможно, стоило более явно обосновать, почему использовалась именно трехуровневая пороговая функция активации, а не одноуровневая или какая-либо иная (например, ReLU, синусоидальная и т.д.). Каким образом количество уровней квантования влияет на эффективность работы нейрона и нейронной сети?

3. В работе активно используются методы ансамблирования классификаторов. Однако есть некоторые неточности в формулировках. Не совсем понятно, что именно подразумевалось под бустингом, когда речь шла об алгоритме создания врожденного иммунитета (обучения иммунной сети с учителем)? Также при разработке алгоритмов обучения предложенной в третьей главе нейро-иммунной модели используются два популярных ансамблевых метода: бэггинг и бустинг. В исследовании не отражено, почему для процедуры обучения детекторов не подходит метод стекинга.

4. В работе не приведено явного обоснования выбора базовых мер близости для создания на их основе детекторов иммунной сети, кроме мер

близости Минковского и Байеса-Минковского, которые используются, исходя из соображений равновесия – первая обрабатывает слабо коррелированные группы признаков, вторая – сильно коррелированные. Однако подобных обоснований нет для классификатора Байеса и для мер близости на базе статистических критериев.

5. Указано, что для извлечения признаков, поступающих на вход нейросетевого преобразователя «биометрия-код», основанного на корреляционных нейронах, следует применять архитектуры типа «автокодировщик». Не ясно, возможно ли применять иные архитектуры.

6. Не указано, из каких соображений применяется именно трёхфакторная аутентификация, а также не описаны ее преимущества перед другими возможными процедурами аутентификации, например, двухфакторной. Интуитивно понятно, что чем больше факторов, тем надежнее процедура. Однако следовало описать какие-либо рекомендации по выбору количества факторов, необходимых для конкретных условий применения.

Заключение

Приведенные замечания в целом не меняют общего положительного впечатления о выполненной диссертационной работе, которая выполнена на актуальную тему, обладает научной новизной, практической ценностью, является самостоятельной и законченной научно-исследовательской работой.

Диссертация Сулавко Алексея Евгеньевича на соискание ученой степени доктора технических наук является законченной научно-квалификационной работой, в которой изложены научно обоснованные технические решения и разработки в области повышения надежности систем биометрической аутентификации, работа соответствует требованиям п. 9 «Положение о присуждении ученых степеней», а ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Отзыв подготовлен Бабенко Людмилой Климентьевной – доктором технических наук, профессором, профессором кафедры Безопасности информационных технологий имени профессора О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета. Диссертация защищена по специальностям 05.13.15 – Вычислительные машины, комплексы и компьютерные сети, 05.13.18 – Математическое моделирование, численные методы и комплексы

программ.

Отзыв заслушан и одобрен на заседании кафедры безопасности информационных технологий имени профессора О. Б. Макаревича (протокол № 17 от «11» июля 2023 г.).

Профессор кафедры безопасности
информационных технологий
имени профессора О. Б. Макаревича,
д.т.н., профессор — Бабенко Людмила Климентьевна

Диссертация защищена по специальностям:
05.13.15 – Вычислительные машины, комплексы и компьютерные сети,
05.13.18 – Математическое моделирование, численные методы и комплексы программ.

Зав. кафедрой безопасности
информационных технологий
имени профессора О. Б. Макаревича,
к.т.н., доцент — Абрамов Евгений Сергеевич

Диссертация защищена по специальности:
05.13.19 – Методы и системы защиты информации, информационная безопасность.

Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет»
Адрес: 344006, Ростовская обл., г. Ростов-на-Дону, ул. Большая Садовая, 105/42
Телефон: +7 (863) 218-40-00
e-mail: info@sfedu.ru
Официальный сайт: https://sfedu.ru/

Федеральное государственное автономное
образовательное учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Личную подпись Бабенко Л.К.
ЗАВЕРЯЮ:
Начальник сектора
«13» 07 2023 г.
УПРАВЛЕНИЕ ДЕЛАМИ И КАДРОВОЙ РАБОТЫ
ОГРН 1026103165241
14