Отзыв на автореферат диссертации Сулавко Алексея Евгеньевича
«Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта»,
представленной на соискание ученой степени доктора технических наук
по специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность.

Представленная диссертация посвящена проблеме высоконадежной биометрической аутентификации и обеспечению конфиденциальности биометрических шаблонов на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта. На сегодняшний день данное научное направление представляет интерес для науки и практики, что находит отражение в рамках таких национальных программ, как «Цифровая экономика Российской Федерации» и Национальная технологическая инициатива (НТИ).

Актуальность исследования Сулавко А. Е. как с академической, так и с прикладной, точки зрения не вызывает сомнений – это качественное и значимое исследование систем биометрической аутентификации на основе защищенного исполнения нейросетевых моделей доверенного ИИ и алгоритмов их автоматического синтеза и обучения на малых выборках биометрических данных. Объект, предмет, новизна, цели и задачи исследования грамотно сформулированы. Структура работы логична и обоснована. Комплексный теоретический подход в сочетании с экспериментальными результатами показывает перспективность выбранных методов и реализуемых на их основе программных продуктов. Исследования в области мета-признаков могут найти своё применение не только в области биометрии, но и в других приложения искусственного интеллекта, например, для создания кросс-рыночных решений которые могут служить основой для продуктов таких рынков НТИ как беспилотные автомобили, водный и воздушный транспорт, средства человеко-машинных коммуникаций. Технология автоматического синтеза и обучения на малых выборках доверенного искусственного интеллекта, предложенная Сулавко А.Е., является сквозной и может быть применена (при определенной адаптации) в различных приложениях, хотя обозначенная автором научно-техническая проблема относится непосредственно к средствам высоконадежной биометрии.

Наибольший вклад работы можно отнести к сегменту прикладных систем связанных с защитой таких компьютерных технологий как защищенная передача данных и/или безопасность информационных и киберфизических систем. Автор в своей работе усиливает безопасность, надежность и функциональность систем биометрического контроля и аутентификации. Новации, которые предложены в диссертации Сулавко А.Е., позволяют создавать средства высоконадежной, в том числе многофакторной, биометрической аутентификации, электронной подписи с биометрической активацией и других защищенных приложений доверенного искусственного интеллекта.

Результаты обладают практической и теоритической значимостью. Научной новизной обладают следующие результаты:

1. Концепция защищенного исполнения нейросетевых алгоритмов искусственного интеллекта, основанная на преобразовании корреляционных связей между признаками в мета-признаки.
2. Модель корреляционных нейронов и модель нейросетевого преобразователя биометрия-код на их основе, а также алгоритм их автоматического синтеза и обучения на малых выборках.
3. Адаптивная нейро-иммунная модель ИИ и алгоритмы ее обучения с учителем и с подкреплением.
4. Методы и алгоритм высоконадежной многофакторной аутентификации на основе рукописных и голосовых образов, а также акустических образов уха с обеспечением защиты биометрических данных от компрометации.
5. Технология автоматического синтеза и обучения нейросетевых моделей доверенного ИИ на малых выборках.

Работа является актуальной и соответствует заявленной специальности и.

К диссертации у имеются следующие вопросы и замечания:

1. Автор часто приводит понятие “дрейфа”, в том числе для описания задач, научной новизны, положений на защиту и теоретической значимости - “концептуальный дрейф”, “дрейфующие характеристики”, “дрейф биометрических данных”, “дрейф концепций и данных”. В автореферате дано лишь одно пояснение к понятию в самом начале - “изменчивость”. Однако явно, применительно ко всем употреблениям, смысл понятия более сложный, чем просто изменчивость или изменение чего-либо в контексте биометрии и ИИ. Соответственно вкладываемый в понятие смысл сложно уловим для неподготовленного читателя.
2. На странице 23 сказано, что пользователям рекомендуется проходить аутентификацию не менее одного раза в полгода. В процессе эксплуатации на реальной системе необходимо ли также вносить новые биометрические данные в выборку “Чужих”? Или этот набор данных может быть собран только единожды? Так как на странице 22 указано, что этот набор также собирался на основании данных от некоторых субъектов.
3. Применительно к реальной эксплуатации системы аутентификации, описанной в главе 4. Набор данных “Все свои” на странице 22 - это набор пользователей системы, проходящих аутентификацию? Каким образом будет происходить добавление новых пользователей в систему? Нужно ли будет заново пересчитывать все признаки и наборы, если допустим есть схожесть между новым пользователем и каким-то субъектов из набора “Чужие”? Учитывая размер выборки “Все свои”, значит ли это что система может быть внедрена только в тех организациях, где число пользователей достаточно значимо (~260)?

4. На странице 13 указывается, что ключ, формируемый НПБК может использоваться как подпись или пароль. На странице 22 говорится о том, что длина ключа была увеличена более чем в 10 раз. Влияет ли это на эксплуатационные характеристики системы? В качестве чего и в какой прикладной области может использоваться такой ключ от НПБК?
5. Из материалов автореферата не ясно, почему нейросетевые преобразователи, обученные с помощью ГОСТ Р 52633.5-2011 дают меньшую длину ключа по сравнению с преобразователями, построенными с применением корреляционных нейронов.

Указанные замечания не являются принципиальными и не снижают высокой оценки диссертационного исследования которое является законченной научной работой на актуальную тему. Решение научной проблемы повышения надежности многофакторной биометрической аутентификации и защищенности биометрических систем от компьютерных атак на основе технологии защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта имеет важное хозяйственное значение. Результаты работы безусловно обладают научной новизной и имеют высокую значимость для науки и практики. Диссертация соответствует требованиям пунктов 9-14 Положения «О присуждении учёных степеней», которые предъявляются к диссертациям, а ее автор – 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, профессор,
Заведующий базовой кафедрой
«Безопасные информационные
технологии умного города»,

25.08.2023

Захаров Александр Анатольевич

Федеральное государственное автономное образовательное учреждение высшего образования «Тюменский государственный университет»
625003, г. Тюмень, ул. Володарского, 10
+7(3452)59-77-55

a.a.zakharov@utmn.ru
Докторская диссертация защищена по специальности 05.13.18 в 2002 году

Первый проректор А.В. Толстиков