ОТЗЫВ

на автореферат диссертации 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

Работа Сулавко А.Е. направлена на решение крайне актуальных задач в области информационной безопасности, связанных с необходимостью реализации защищенного исполнения алгоритмов доверенного искусственного интеллекта (ИИ), лежащих в основе процедуры биометрической аутентификации. В диссертации приведены результаты исследований нейросетевых моделей и алгоритмов машинного обучения на малых выборках, применяемых для высоконадежной биометрической аутентификации и защиты биометрических данных от компрометации. Решена актуальная научно-техническая проблема повышения надежности многофакторной биометрической аутентификации на основе защищенного исполнения нейросетевых моделей доверенного ИИ и алгоритмов их автоматического синтеза и обучения на малых выборках биометрических данных. Проблема защищенного исполнения нейросетевых алгоритмов ИИ и их автоматического обучения на малых выборках является частью общей проблематики для сквозных технологий доверенного взаимодействия субъектов информационного обмена, обеспечивающих корректную работу приложений и прикладных сервисов в недоверенном окружении.

Необходимость разработки предлагаемых в работе положений за последние годы значительно возросла, в связи с принятием федерального закона № 572 ("Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"), а также в связи с тем, что биометрические данные стали использоваться в целях аутентификации повсеместно. Особенно необходимым защищенное исполнение алгоритмов ИИ может стать на объектах критической информационной инфраструктуры, требующих повышенного внимания к персональным данным (в том числе, биометрическим).

Автореферат ясно отражает суть, цели и задачи диссертационного исследования. Все основные результаты работы обладают научной новизной и уникальностью. К наиболее значимым научным результатам работы следует отнести:

- концепцию защищенного исполнения нейросетевых алгоритмов ИИ, которая позволяет сформировать устойчивость модели к извлечению знаний;
- модель корреляционных нейронов и сформированную на их основе модель нейросетевого преобразователя биометрия-код, повышающего защищенность биометрических данных от компрометации и длину ключа;
- методы и алгоритм высоконадежной многофакторной аутентификации на основе рукописных и голосовых образов, а также акустических образов уха с обеспечением защиты биометрических данных от компрометации;
- технологию автоматического синтеза и обучения нейросетевых моделей доверенного ИИ для высоконадежной биометрической аутентификации и других ответственных приложений ИИ.

Результаты диссертационного исследования апробированы на всероссийских и международных научных конференциях, опубликованы и защищены патентом.

Замечания по тексту автореферата:

1. Один из ключевых аспектов работы связан с обеспечением защиты биометрических систем и данных от ряда угроз информационной безопасности. Однако в автореферате и общей характеристике работы не приводится описания актуальных угроз (даны только названия). Кроме того, понятие «атака» в работе часто подменяется понятием «угроза». Эти термины имеют разное значение, и соискателю следовало дать более конкретное формальное определение тех угроз и компьютерных атак, которые рассматриваются в представленной работе.

2. Не раскрыт ответ на вопрос - беспечивают ли полученные результаты полную защиту от рассматриваемых угроз (атак) или позволят лишь смягчить возникающие угрозы? Не приведены и основные экспериментальные данные.

3. В материалах работы не представлены основные данные о проведении экспериментов именно с биометрическими синтетическими образами, которые специально генерировались (или синтезировались) для проверки работоспособности методов и алгоритма аутентификации. Проводились ли такого рода состязательные атаки?

Указанные замечания, на мой взгляд, могут быть как перспективные направления дальнейших исследований и не снижают ценности диссертационной работы Сулавко А.Е.

Судя по автореферату, диссертационное исследование является законченной научно-исследовательской работой, обладающей научной новизной и практической значимостью и вносит значимый вклад развитие теории защиты информации. Работа соответствует требованиям п. 9-14 Положения ВАК «О присуждении учёных степеней», предъявляемым к диссертациям на соискание учёной степени доктора технических наук, а её автор — Сулавко Алексей Евгеньевич заслуживает присуждения учёной степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Президент ТУСУР,
директор Института системной интеграции и безопасности,
доктор технических наук, профессор

Шелупанов Александр Александрович
федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»
Адрес организации: 634050, г. Томск, пр. Ленина, 40
e-mail: prezident@tusur.ru
Телефон: +7 3822 907155

Докторская диссертация защищена в 1994 году по специальности 05.13.01- Системный анализ.

Подпись
УДОСТОВЕРЯЮ
Ученый секретарь
Е.В. Прокопчук