УТВЕРЖДАЮ
Первый проректор –
проректор по научной работе
ФГБОУ ВО «Самарский
государственный технический
университет», д.т.н., профессор
_____ Ненашев М.В.
«9» июля 2024 г.

ЗАКЛЮЧЕНИЕ

федерального государственного бюджетного
образовательного учреждения высшего образования
«Самарский государственный технический университет»

Диссертация «Модели и алгоритмы нейросетевой биометрической аутентификации в защищенном режиме исполнения» выполнена на кафедре «Электронные системы и информационная безопасность» института автоматики и информационных технологий ФГБОУ ВО «Самарский государственный технический университет» Министерства науки и высшего образования Российской Федерации.

В период подготовки диссертации соискатель Панфилова Ирина Евгеньевна проходила обучение в очной аспирантуре ФГБОУ ВО «Самарский государственный технический университет», работала в должности преподавателя, а затем старшего преподавателя кафедры «Электронные системы и информационная безопасность» в ФГБОУ ВО «Самарский государственный технический университет».

В 2018 г. окончила с отличием бакалавриат ФГБОУ ВО «Самарский государственный технический университет» по направлению подготовки 10.03.01 «Информационная безопасность».

В 2020 г. окончила с отличием магистратуру ФГБОУ ВО «Самарский государственный технический университет» по направлению 09.04.01 «Информатика и вычислительная техника».

В 2024 г. окончила аспирантуру ФГБОУ ВО «Самарский государственный технический университет» по направлению 09.06.01 «Информатика и вычислительная техника».

Справки со сведениями о сданных кандидатских экзаменах выданы в 2024 г. в ФГБОУ ВО «Самарский государственный технический университет».

Научный руководитель – доктор технических наук, доцент Ложников Павел Сергеевич, проректор по научной и инновационной деятельности ФГАОУ ВО «Омский государственный технический университет».

По итогам обсуждения диссертации принято следующее заключение:

1. Диссертация Панфиловой Ирины Евгеньевны является законченной научно-квалификационной работой, соответствующей п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), в которой изложены научно обоснованные результаты решения задачи повышения защищенности процедуры биометрической

аутентификации на основе нейросетевых преобразователей «биометрия-код» по отношению к деструктивным воздействиям при работе с биометрическими образами лиц.

2. Соискателем лично получены все основные результаты, выносимые на защиту:

1) Концепция защищенной биометрической аутентификации по лицу.

2) Модель тригонометрического нейрона и основанная на ней модель нейросетевого преобразователя «биометрия-код».

3) Алгоритм настройки параметров нейросетевых преобразователей «биометрия-код» и алгоритм автоматического обучения НПБК на основе тригонометрических нейронов.

4) Система защищенной биометрической аутентификации по лицу и ее программная реализация.

В перечисленных в автореферате работах соискателем лично получены следующие результаты:

– в работах [5, 10] разработана концепция защищенной биометрической аутентификации по лицу, обеспечивающая устойчивость к атакам на биометрическое предъявление. За счет предложенной концепции решается не только задача противодействия спуфинг атакам, но также обеспечивается дополнительная защита параметров нейросетевого преобразователя «биометрия-код» (НПБК), осуществляющего аутентификацию;

– в работе [6] разработаны модель тригонометрического нейрона и основанная не ней модель НПБК, позволяющие работать со слабо коррелированными признаками лица человека и продуцировать длинный криптографический ключ на выходе преобразователя при высокой точности классификации биометрических образов;

– в работе [6] разработаны алгоритмы предварительной настройки параметров нейросетевого преобразователя «биометрия-код» и алгоритм автоматического обучения НПБК на основе тригонометрических нейронов на малых выборках, позволяющие предварительно оценить особенности распределений биометрических образов лиц, не компрометирующих легитимных пользователей, с целью последующей сборки и быстрого обучения НПБК, не требующего большого числа примеров «Свой»;

– в работах [2, 8] разработана структура системы защищенной биометрической аутентификации по лицу, обеспечивающая защищенность процедуры биометрической аутентификации личности по лицу на основе НПБК в отношении спуфинг атак и атак компрометации знаний НПБК и открытых биометрических образов лиц.

Опубликованные работы полностью отражают содержание диссертационной работы. Все основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [1, 3, 9]; по главе 2 – [5, 6, 10]; по главе 3 – [2, 4, 6, 7, 8]; по главе 4 – [2, 6, 8]. Две работы написаны автором единолично, другие – совместно с другими членами научного коллектива.

3. Достоверность полученных результатов и выводов основана на том, что предложенные в диссертационной работе решения подтверждаются:

1) корректной постановкой задач и выбором методов исследования;

2) результатами практического применения разработанных концепции, моделей и алгоритмов при решении прикладных задач;

3) апробацией в процессе проведения экспериментов и использованием разработанного программного комплекса;

4) апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях, в том числе из перечня ВАК, и в изданиях, индексируемых в международной базе Scopus.

4. Научную новизну работы составляют:

1) Концепция защищенной биометрической аутентификации по лицу, отличающаяся применением механизма защищенного нейросетевого контейнера (ЗНК) для безопасного взаимодействия блока аутентификации на основе пользовательского НПБК и блока обнаружения спуфинг атак на основе НПБК, представленного в виде классификатора реальных и поддельных изображений лиц, что позволяет обеспечивать устойчивость процедуры аутентификации к атакам на биометрическое предъявление (спуфинг атакам), а также дополнительную защиту таблиц нейросетевых функционалов пользовательского НПБК.

2) Модель тригонометрического нейрона, а также основанная на ней модель нейросетевого преобразователя «биометрия-код», отличающиеся применением новой тригонометрической меры оценки расстояния между образами субъектов в подпространстве пар признаков вместо исходных признаков, что дает возможность работы со слабо коррелированными признаками лица человека и защиту образов лиц от компрометации путем продуцирования длинного криптографического ключа при высокой точности классификации. Предложенные модели не используют параметры распределений и/или характеристики образов «Свой», что обеспечивает защиту знаний НПБК от компрометации.

3) Алгоритм предварительной настройки параметров нейросетевых преобразователей «биометрия-код» и алгоритм автоматического обучения НПБК на основе тригонометрических нейронов, отличающиеся использованием информации (порогов равного разделения подпространства пар признаков), полученной путем оценки не участвующего в обучении набора биометрических образов лиц, что дает возможность быстрого и робастного обучения пользовательских НПБК на малых выборках образов лиц.

4) Структура системы защищенной биометрической аутентификации по лицу, отличающаяся наличием независимых блоков извлечения признаков, обучения нейросетевых преобразователей и аутентификации, а также применением варианта исполнения ЗНК, при котором в режиме обучения ключом НПБК для обнаружения спуфинг атак осуществляется гаммирование структуры (порядка расположения синапсов в нейронах) пользовательского НПБК, а обратный описанному процесс осуществляется при аутентификации. Разработанная структура позволяет повысить защищенность процедуры биометрической аутентификации личности по лицу на основе НПБК в отношении спуфинг атак, а также атак извлечения знаний НПБК и компрометации биометрических образов лиц.

5. Практическая значимость и реализация результатов работы заключается в разработке системы защищенной биометрической аутентификации по лицу и ее программной реализации. Научные результаты получены при проведении работ в рамках государственного задания Минобрнауки России на 2023-2025 годы № FSGF-2023-0004 «Научные основы построения искусственного интеллекта на основе нейросетевых алгоритмов, исполняемых в защищенном режиме». Часть работы по теме диссертации проводилась в рамках гранта ИБ МТУСИ № 40469-18/23-К «Методы и алгоритмы повышения надежности нейросетевой биометрической аутентификации». Результаты диссертационного исследования приняты к внедрению в производственные и бизнес-процессы компаний ООО «Открытый код» г. Самары и ООО «АИ ЗИОН» г. Омска, а также в учебные процессы ФГБОУ ВО «Самарский государственный технический университет» и ФГАОУ ВО «Омский государственный технический университет».

6. Ценность научных работ соискателя заключается в том, что в результате выполненных исследований:

– предложена концепция защищенной биометрической аутентификации по лицу, устойчивая к спуфинг атакам;

– предложены модели тригонометрического нейрона и нейросетевого преобразователя «биометрия-код» (НПБК) для осуществления защищенной биометрической аутентификации по лицу;

– предложены алгоритм предварительной настройки параметров нейросетевого преобразователя «биометрия-код» на основе тригонометрических нейронов и алгоритм его автоматического обучения;

– предложена структура системы защищенной биометрической аутентификации по лицу.

7. Обоснование выбранной специальности и отрасли наук диссертации.

Диссертация «Модели и алгоритмы нейросетевой биометрической аутентификации в защищенном режиме исполнения» соответствует следующим пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность:

п.12. «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа»;

п.15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Отрасль науки – техническая, поскольку представленные результаты исследования в области защищенной нейросетевой аутентификации дают существенный технический эффект при их использовании и внедрении.

8. Полнота изложения материалов диссертации.

По материалам исследования лично и в соавторстве опубликовано 10 печатных работ, 6 из которых изданы в журналах, рекомендованных ВАК; 1 научная публикация индексирована в международной информационно-аналитической системе научного

цитирования Scopus. Получено 2 свидетельства о государственной регистрации программы для ЭВМ.

Статьи, опубликованные в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК

1. Панфилова И. Е., Сулавко А. Е. Методы определения живого присутствия пользователя перед видеокамерой в задачах биометрической аутентификации по лицу / Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2023. Вып. 2 (141). С. 17—26.

2. Васильев В.И., Панфилова И.Е., Сулавко А.Е., Серикова А.Е. Система верификации личности по изображению лица в защищенном режиме на основе искусственных нейронных сетей // Прикладная информатика. 2023. Т. 18. № 5. С. 33–47. DOI: 10.37791/2687-0649-2023-18-5-33-47

3. Панфилова И. Е. Глубокие нейронные сети в задачах идентификации и верификации лиц / Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2024. Вып. 2 (145). С. 33—41.

4. Жумажанова С. С., Панфилова И. Е., Сулавко А. Е., Ложников П. С., Серикова А. Е. Биометрическая аутентификация по тепловым изображениям лица на основе преобразователей "биометрия-код" / Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2023. Вып. 1 (140). С. 8—19.

5. Панфилова И.Е., Ложников П.С. Исследование применимости нейросетевых преобразователей «биометрия-код» для задачи обнаружения атак на биометрическое предъявление // Вестник УрФО № 2(52) / 2024, с. 106–121

6. Панфилова И. Е., Сулавко А. Е., Ложников П. С. Повышение защищенности процедуры биометрической аутентификации по лицу на основе нейросетевых преобразователей «биометрия-код» / Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2024. Вып. 3 (146). С. 3—11.

Статьи, индексируемые в международной базе Scopus

7. A. Sulavko, I. Panfilova, A. Samotuga and S. Zhumazanova, "Biometric Authentication Using Face Thermal Images Based on Neural Fuzzy Extractor," 2023 Intelligent Methods, Systems, and Applications (IMSA), Giza, Egypt, 2023, pp. 80-85, doi: 10.1109/IMSA58542.2023.10217752.

Другие публикации по теме диссертации

8. Сулавко А.Е., Панфилова И.Е. Верификация личности субъектов по лицу на основе методов глубокого обучения и нейросетевых преобразователей «биометрия-код» / Нанотехнологии. Информация. Радиотехника (НИР-23) : материалы Всерос. молодеж. науч.-практ. конф. (Омск, 18 апр. 2023 г.) / Минобрнауки России, Ом. гос. техн. ун-т, Радиотехн. фак., Каф. «Физика» ; редкол.: Н. О. Голубятникова [и др.]. – Омск : Изд-во ОмГТУ, 2023. с. 336-339

9. Панфилова И.Е., Иниватов Д.П. Обзор методов защиты данных биометрических шаблонов / Безопасность информационных технологий : сб. науч. ст. по материалам V

Всерос. науч.-техн. конф., посвящ. 70-летнему юбилею АО «НПП "Рубин"» (г. Пенза, 27 сентября 2023 г.) : в 2 т. – Пенза : Изд-во ПГУ, 2023. Т. 1. С. 135-145.

10. Панфилова И.Е. Методы и алгоритмы повышения надежности нейросетевой биометрической аутентификации / Сборник трудов III Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ, 25-237 октября 2023 г. – М., 2023. – с. 289-295

Свидетельства о государственной регистрации программы для ЭВМ

11. Свидетельство о государственной регистрации программы для ЭВМ: Реализация моделей и алгоритмов обучения нейросетевых преобразователей биометрия-код на основе тригонометрических нейронов, позволяющих симметризовать классы образов относительно пространства признаков: Свидетельство о государственной регистрации программы для ЭВМ № 2023684211: / И. Е. Панфилова, А. Е. Сулавко, А. Е. Серикова, Ю. Дорогов. – заявка № 2023682402 заявл. 27.10.2023: опубл. 14.11.2023

12. Свидетельство о государственной регистрации программ для ЭВМ: AIC ModelOps Platform: Свидетельство о государственной регистрации программы для ЭВМ № 2022680686/ А.Е. Сулавко, Д.Г. Стадников, А.Г. Чобан, А.Е. Самотуга, И.Е. Панфилова. – заявка № 2022668418; заявл. 10.10.2022; опубл. 3.11.2022.

Диссертация Панфиловой Ирины Евгеньевны соответствует п. 14 Положения о порядке присуждения ученых степеней:

– отсутствует недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации;

– соискатель ссылается на авторов и источники заимствования.

Диссертация на тему «Модели и алгоритмы нейросетевой биометрической аутентификации в защищенном режиме исполнения» Панфиловой Ирины Евгеньевны рекомендуется к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заключение принято на расширенном заседании кафедры «Электронные системы и информационная безопасность» ФГБОУ ВО «Самарский государственный технический университет» Министерства науки и высшего образования российской Федерации.

Присутствовало на заседании 23 человека, в том числе 5 докторов наук.

Результаты голосования: «за» – 23 человека, «против» – нет, «воздержалось» – нет.

Протокол № 11 от 28 июня 2024 года.

Подпись Карповой Н.Е.
удостоверяю, заместитель начальника управления по персоналу и делопроизводству Самарского государственного технического университета Саразова Н.И.

И.о. заведующего кафедрой
«Электронные системы и
информационная безопасность»,
к.т.н., доцент Н.Е. Карпова