


УТВЕРЖДАЮ
Заместитель начальника
Академии ФСО России
доктор социологических наук,
профессор
В.И. Козачок
30.11.2015



ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу Щемелинина Вадима Леонидовича на тему:
"Методика и комплекс средств оценки эффективности аутентификации
голосовыми биометрическими системами",
представленную на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – "Методы и системы защиты информации,
информационная безопасность"

1. Актуальность темы диссертации

В связи с бурным ростом компьютерных технологий в последние два десятилетия произошел прорыв в области автоматической обработки биометрических признаков. Вместе с ростом доверия к голосовым биометрическим технологиям, возросла и ценность защищаемой ими информации. Следовательно, возросли и требования к эффективности работы голосовых биометрических систем, в том числе при воздействии на них различных видов спуфинг атак. В диссертационной работе Щемелинина В.Л. рассматривается проблема отсутствия в принятых на сегодняшний день

стандартах оценки эффективности аутентификации голосовыми биометрическими системами этапов, позволяющих корректно учесть влияние спуфинг атаки. Анализ состояния проблемы, проведённый соискателем, показывает, что в отличие от методов имперсонализации или записи и повтора голосовых биометрических характеристик, методы синтеза и преобразования голосовых биометрических характеристик значительно развились и представляют высокую угрозу для надёжности современных голосовых биометрических систем.

Таким образом, диссертационная работа Щемелинина В.Л., посвящённая разработке методики и комплекса средств оценки эффективности аутентификации голосовыми биометрическими системами с учётом влияния различных видов спуфинг атак, посвящена решению актуальной научно-технической задачи, имеющей существенное значение для развития науки и практики.

II. Научная новизна и основные результаты исследований

Научную новизну диссертации характеризуют следующие положения.

1. *Метод имитации атаки на голосовые биометрические системы*, отличающийся применением автоматической разметки речевых данных для создания модели синтезированного голоса целевого диктора. Это обеспечивает автоматизацию процесса синтеза индивидуальных биометрических характеристик при имитации спуфинг атаки на голосовую биометрическую систему.

2. *Методика оценки эффективности аутентификации голосовыми биометрическими системами*, обладающая уникальными численными и графическими показателями, а также дополнительными шагами на этапе подготовке тестовой речевой базы данных. Это позволяет учесть воздействие

различных видов спуфинг атак на модуль ввода биометрической информации при аутентификации голосовой биометрической системой. Проведены численные эксперименты, показывающие преимущество разработанной методики по сравнению с существующими аналогами.

3. *Комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами*, отличающийся оригинальной схемой, включающей модули имитации атаки и расчёта показателей эффективности аутентификации с учётом воздействия спуфинг атаки. Применение разработанного комплекса позволяет учитывать воздействие спуфинг атак как на этапе разработки голосовых биометрических систем применяемых для аутентификации, так и на этапе проведения технологических испытаний.

4. *Метод противодействия спуфинг атакам* отличающийся оригинальным комбинированием методов факторного анализа, сигнальной обработки и признакового описания сигнала и позволяющий значительно повысить устойчивость голосовых биометрических систем к различным методам спуфинг атак на модуль ввода биометрической информации.

III. Практическая ценность результатов исследований

Практическая ценность диссертационного исследования состоит в том, что теоретические результаты доведены до комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами, внедрённого на этапах разработки голосовых биометрических систем и проведения технологических испытаний. Разработанные технические решения по совершенствованию защиты заняли второе место на международном конкурсе ASVspoof Challenge 2015 и могут быть интегрированы в коммерческие голосовые биометрические системы.

Результаты диссертации использованы при выполнении следующих научно-исследовательских и опытно-конструкторских работ: НИР Министерства образования и науки «Исследование методов и алгоритмов многомодальных биометрических и речевых систем» (грант 074-U01); ОКР Федеральной службы безопасности, шифр «Ярмарка-ТМС»; ОКР Министерства внутренних дел, шифр «Кристалл-М (Флот)»; ОКР Федеральной службы по контролю за оборотом наркотиков, шифр «Этнос». Также результаты работы были внедрены в различные коммерческие продукты компаний ООО «Центр речевых технологий».

IV. Достоверность и обоснованность результатов исследований

Основные положения, выводы и рекомендации, полученные в диссертации, достаточно обоснованы и аргументированы. Сформулированная в диссертации задача исследована и решена на основе корректного использования фундаментальных концепций, принципов и подходов, используемых в теории вероятности и математической статистики, теории цифровой обработки сигналов, теории проектирования и разработки программного обеспечения ЭВМ.

Достоверность основных выводов и результатов диссертации подтверждается:

– обстоятельным сравнительным анализом достоинств и недостатков предшествующих научных разработок по исследуемой проблематике и преимуществом основных научных положений;

– корректностью предложенных методов и апробацией основных положений диссертации в печатных трудах, докладах на конференциях и научно-технических семинарах, в том числе, на международном конкурсе

Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015;

– согласованностью основных результатов диссертации с данными, полученными как самим автором, так и другими исследователями в ходе экспериментов, внедрении и эксплуатации голосовых биометрических систем;

– положительными результатами внедрения основных научных положений диссертации в процесс разработки голосовых биометрических систем и технологических испытаний реальных систем.

V. Апробация и публикации

Результаты исследований автора прошли всестороннюю апробацию на 8 международных, всероссийских, региональных научно-практических конференциях. По тематике диссертации автором опубликовано 10 научных работ, в том числе 6 работ в журналах, входящих в перечень рецензируемых научных журналов и изданий, 5 – в зарубежных изданиях, включенных в систему цитирования Web of Science и Scopus.

VI. Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационной работы Щемелинина В.Л. целесообразно использовать в организациях, занимающихся исследованием и разработкой технических систем обработки речи, например, в Санкт-Петербургском государственном университете, Институте проблем передачи информации Российской академии наук, Московском государственном лингвистическом университете, Московском государственном университете им. М.В.

Ломоносова, Университете Восточной Финляндии, ООО «Центр речевых технологий».

VII. Замечания по диссертации

1. Проведённый анализ устойчивости современных голосовых биометрических систем к различным видам спуфинг атак не включает в себя оценку устойчивости к методам имперсонализации, реализуемым профессиональными актёрами.

2. В диссертационной работе и автореферате отсутствуют оценки затрат вычислительных ресурсов на реализацию разработанных автором методик.

3. В экспериментах, проведённых соискателем, отсутствуют результаты оценки надёжности предложенного метода противодействия спуфинг атакам при использовании злоумышленником методов фальсификации голосовых биометрических характеристик для маскировки.

4. Предварительный детектор спуфинг атаки, основан на простом анализе сигнала. Подобное, довольно грубое оценивание приведёт к увеличению ошибки ложного пропуска предварительным детектором спуфинг атаки в условиях наличия дополнительных помех в сигнале.

5. Следовало привести более полные комментарии к рисункам. Например, рисунок 5 автореферата (в диссертации рисунок 4.2) не содержит расшифровки компонентов схемы. Если в диссертации их суть становится ясна из дополнительных рисунков 4.3-4.5, то в автореферате следовало, хотя бы их расшифровать в подрисуночной надписи.

Перечисленные замечания не снижают высокий научный уровень проведённых исследований и не влияют на общий положительный вывод о качестве представленной к защите диссертации. Замечания носят

рекомендательный характер и могут быть учтены автором в дальнейших публикациях по теме исследования.

VIII. Общая оценка диссертационной работы

В целом диссертационная работа Щемелинина В.Л. представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов.

Автором диссертации сформулирована и решена важная научно-техническая задача разработки методики и комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами учитывающих влияние спуфинг атак, основанных на фальсификации индивидуальных голосовых биометрических характеристик.

Соискателем разработана совокупность технических и методических решений, внедрение которых можно рассматривать как вклад в развитие научного направления, связанного с повышением защищённости персональных данных, доступ к которым обеспечивается голосовыми биометрическими системами.

Основные этапы работы, выводы и результаты представлены в автореферате, который достаточно полно отражает содержание диссертации.

Диссертационная работа «Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами» соответствует паспорту научной специальности и отвечает критериям, установленным Положением о присуждении ученых степеней, утвержденным постановлением Правительства РФ № 842 от 24.09.2013 г., предъявляемым к кандидатским диссертациям, а ее автор – Щемелинин Вадим Леонидович по уровню профессиональных, специальных и

общенаучных знаний заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв рассмотрен и одобрен на заседании кафедры Академии ФСО России. Протокол № 15 от 25.11.2015 г.

Доктор технических наук,
профессор

Иванов Борис Рудольфович

Доктор технических наук,
доцент

Лисичкин Владимир Георгиевич

«-» ноября 2015 г.

Государственное казенное образовательное учреждение высшего профессионального образования Академия Федеральной службы охраны Российской Федерации (Академия ФСО России)

Адрес: 302034, г. Орел, ул. Приборостроительная, д. 35

Телефон: 8(4862)549763

Эл. адрес: <http://academ.msk.rsnet.ru>

5 | 4 | 29 | 3 - 4621