ОТЗЫВ

официального оппонента Приорова Андрея Леонидовича на диссертационную работу Щемелинина Вадима Леонидовича «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.

I. Актуальность темы диссертации

Диссертационная работа, посвященная решению проблемы оценки эффективности аутентификации голосовыми биометрическими системами при воздействии различных видов спуфинг атак, несомненно, является актуальной. Это обусловлено тем, что процессы глобализации и активного развития компьютерных технологий, включая технологии синтеза и преобразования голосовых биометрических характеристик, объективно порождают необходимость совершенствования аутентификации голосовыми биометрическими системами.

Вместе с тем, в последние годы значительно возросло доверие к биометрическим технологиям. Однако в принятых на сегодняшний день стандартах оценки эффективности аутентификации голосовыми биометрическими системами отсутствуют показатели устойчивости к различным видам спуфинг атак.

В этих условиях, становятся востребованными соответствующие решения, направленные на повышение надёжности голосовых биометрических систем, в том числе при воздействии различных видов спуфинг атак.

Поэтому разработанные в представленной диссертации методика и комплекс средств оценки эффективности аутентификации голосовыми

биометрическими системами с учётом влияния различных видов спуфинг атак имеют важное теоретическое и практическое значение.

II. Научная новизна результатов исследований

К новым научным результатам, полученным в представленной диссертационной работе, можно отнести.

1. Новый метод имитации атаки на голосовые биометрические системы, отличающийся применением автоматической разметки речевых данных для создания модели синтезированного голоса. Предложенный метод позволяет полностью автоматизировать процесс имитации спуфинг атаки на голосовую биометрическую систему.

2. Обобщённая методика оценки эффективности аутентификации голосовыми биометрическими системами, дополненная численными и графическими показателями влияния спуфинг атаки, а также дополнительными шагами на этапе подготовке тестовой речевой базы данных. Разработанные дополнения позволяют учесть воздействие различных видов спуфинг атак на модуль ввода биометрической информации при аутентификации голосовой биометрической системой.

3. Оригинальный комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами, отличающийся схемой, включающей модули имитации атаки и расчёта показателей эффективности аутентификации с учётом воздействия спуфинг атаки. Разработанный комплекс позволяет учитывать воздействие спуфинг атак при оценке эффективности аутентификации голосовой биометрической системой на этапах разработки системы или её внедрения.

4. Новый метод противодействия спуфинг атакам, отличающийся оригинальным комбинированием методов факторного анализа, сигнальной обработки и признакового описания сигнала. Применение данного метода позволяет значительно повысить устойчивость голосовых биометрических

систем к различным методам спуфинг атак на модуль ввода биометрической информации, что подтверждено результатами международного конкурса.

III. Практическая ценность результатов исследований

Практическая ценность результатов исследований диссертации состоит в том, что разработанные в ней методологические и методические основы оценки эффективности аутентификации голосовыми биометрическими системами нашли свою полную и всестороннюю реализацию при разработке и проведении технологических испытаний реально существующих голосовых биометрических систем. При этом предложенный в диссертации метод противодействия спуфинг атакам занял второе место на международном конкурсе ASVspoof Challenge 2015.

IV. Достоверность и обоснованность основных результатов исследований

Решение рассмотренных в диссертации задач выполнено с помощью корректного применения фундаментальных концепций, принципов и подходов, используемых в теории вероятностей и математической статистике, теории цифровой обработки сигналов, теории проектирования и разработки программного обеспечения ЭВМ. Полученные результаты хорошо согласуются с известными публикациями отечественных и зарубежных авторов. Результаты диссертации опубликованы и докладывались на представительных международных научных конференциях.

Достоверность результатов подтверждается их практическим использованием при решении задач, возникающих в ходе процесса разработки и технологических испытаний голосовых биометрических систем.

Степень обоснованности научных положений, основных выводов и рекомендаций диссертации соответствует общепринятой в рамках заявленной специальности.

V. Апробация и публикации

Диссертация написана чётким научным языком и хорошо структурирована. Каждая глава содержит принципиально важные результаты научных исследований автора и заканчивается содержательными выводами.

Полученные в диссертации результаты прошли апробацию на международных научно-практических конференциях. Основные результаты проведённого исследования, выводы и рекомендации отражены в автореферате и публикациях автора (10 научных работ, в том числе 6 работ в журналах, рекомендованных ВАК, 5 из которых в зарубежных изданиях, включенных в системы цитирования Web of Science и Scopus).

VI. Замечания по диссертационной работе

1. Приведено довольно краткое описание современных систем распознавания диктора, отсутствует обзор видов параметров, выделяемых из речевого сигнала.

2. В разделе 1.2.3 диссертации дано описание метода преобразования индивидуальных биометрических характеристик, основанного на моделях гауссовых смесей, но далее в тексте он не используется.

3. На стр. 42 указано, что детектор речи, использующийся в модуле предварительной обработки, основан на энергии сигнала. Чем обусловлен выбор именно такого детектора речевой активности? Известно, что такое решение обладает низкой помехоустойчивостью, и даже при незначительном уровне шумов возникают ошибки детектирования речевых фрагментов.

4. На с. 42 и с. 115 не пояснено, почему не отбрасывается первый мел-частотный кепстральный коэффициент, как это обычно делается в системах распознавания диктора.

5. Неясно, чем вызвано преобладание женских голосов в некоторых тестовых базах? Чаще для речевых баз характерна обратная ситуация.

6. Отсутствуют рекомендации по назначению весовых коэффициентов показателей, отражающих эффективность аутентификации.

7. В тексте диссертации детально описаны возможности применение разработанной методики при технологических испытаниях голосовых биометрических систем, однако остаётся не раскрытой возможность ее применения при проведении сценарных, оперативных испытаний и испытаний в режиме реального времени.

8. В недостаточной степени отражён возможный положительный эффект от внедрения разработанных методов, комплекса и методики.

9. Имеется ряд оформительских ошибок.

Указанные недостатки существенным образом не снижают научной и практической ценности проведённых исследований и не влияют на общий положительный вывод о качестве представленной к защите диссертации.

VII. Выводы

1. Выполненная диссертационная работа является законченной научно-квалификационной работой, в которой содержится решение важной научно-технической проблемы разработки методики и комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами, учитывающих влияние спуфинг атак, основанных на фальсификации индивидуальных голосовых биометрических характеристик. Содержание диссертации соответствует специальности 05.13.19 Методы и системы защиты информации, информационная

безопасность. Автореферат отражает основное содержание диссертационной работы.

2. Полученные в ходе исследования результаты обладают внутренним единством, аргументированы и оценены по сравнению с другими известными решениями, результаты достоверны, выводы и заключения обоснованы, что свидетельствует о новизне, теоретической и практической ценности работы, а также личном вкладе автора в науку.

3. Диссертационная работа отвечает требованиям п. 9 «Положения о порядке присуждения ученых степеней» и соответствует требованиям ВАК Министерства науки и образования России к кандидатским диссертациям, а её автор Щемелинин Вадим Леонидович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
доктор технических наук, доцент,
Ярославский государственный университет
им. П.Г.Демидова,
доцент кафедры динамики электронных систем