ОТЗЫВ

официального оппонента

о диссертационной работе Щемелинина Вадима Леонидовича, выполненной на тему «Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами» и представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

**Актуальность темы диссертации.** Развитие компьютерных технологий позволило мировому научному сообществу достигнуть значительных результатов в области обработки биометрических данных. Одним из биометрических признаков, наиболее удобных в использовании при решении задачи аутентификации пользователя, является речь. Последние десятилетия характеризуются бурным развитием, как голосовых биометрических технологий, так и технологий синтеза и преобразования речи. В настоящий момент, существующие открытые решения по синтезу и преобразованию речи позволяют злоумышленникам реализовывать спуфинг атаки на голосовые биометрические системы, что значительно снижает эффективность аутентификации голосовыми биометрическими системами. Очевидно, что решить данную проблему без стандартизованных методических основ по оценке эффективности аутентификации голосовыми биометрическими системами практически невозможно. Однако, принятые на сегодняшний день стандарты, регламентирующие методику испытаний голосовых биометрических систем, не включают в себя оценку надежности работы систем при активных попытках воздействия злоумышленника, в особенности на компоненты, специфичные для голосовых биометрических систем.

Вышеизложенное позволяет сделать вывод о том, что тема диссертационной работы Щемелинина В. Л. посвященная разработке

методики и комплекса средств оценки эффективности аутентификации голосовыми биометрическими системами с учетом воздействия спуфинг атак на модуль ввода биометрической информации, а также разработке метода повышения эффективности данного процесса за счет детектирования следов атаки во входящем сигнале, является актуальной и имеет важное научное и практическое значение.

**Научная новизна и основные результаты исследований.** Следующие результаты, представленные в диссертационной работе, являются наиболее значимыми:

1. В работе проведен анализ устойчивости современных голосовых биометрических систем к различным видам спуфинг атак. Разработан новый метод имитации спуфинг атаки на голосовые биометрические системы, позволяющий автоматизировать имитацию спуфинг атаки на голосовую биометрическую систему. Отличительной особенностью метода, предложенного автором работы, является применение автоматической разметки речевых данных для создания модели синтезированных индивидуальных биометрических характеристик человека.

2. В диссертации предложена обобщенная методика оценки эффективности аутентификации голосовыми биометрическими системами, дополненная показателями влияния спуфинг атаки, а также дополнительными шагами на этапе подготовке тестовой речевой базы данных. Предложенная методика позволят учесть воздействие различных видов спуфинг атак на модуль ввода биометрической информации при проведении испытаний, описанных в ГОСТ Р ИСО/МЭК 19795 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии.

3. Разработан комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами,

позволяющий учитывать воздействие спуфинг атак при оценке эффективности аутентификации голосовой биометрической системой на этапах разработки системы или ее внедрения. Отличительной особенностью разработанного комплекса программных средств является оригинальная схема, включающая модули имитации атаки и расчета показателей эффективности аутентификации с учетом воздействия спуфинг атаки.

4. Предложен перспективный метод противодействия спуфинг атакам позволяющий существенно повысить надежность аутентификации голосовыми биометрическими системами при воздействии различных методов спуфинг атак на модуль ввода биометрической информации. Полученный результат достигается оригинальным комбинированием методов факторного анализа, сигнальной обработки и признакового описания сигнала.

**Практическая значимость результатов исследований.** Практическая значимость полученных в диссертации результатов наглядно иллюстрируется в рамках рассмотрения проблемы повышения эффективности аутентификации голосовыми биометрическими системами. Результаты диссертационного исследования представляют реальный интерес для широкого круга организаций, исследователей и практикующих специалистов в области противодействия атакам на голосовые биометрические системы. Разработанные автором решения нашли свое применение в процессах разработки и проведения технологических испытаний, реально существующих голосовых биометрических систем. В частности, результаты исследований автора внедрены в коммерческих продуктах компании ООО “ЦРТ”, а также использованы при выполнении научно-исследовательских и опытно-конструкторских работ Министерства образования и науки, Федеральной службы безопасности, Министерства внутренних дел и Федеральной службы по контролю за оборотом наркотиков.

**Достоверность и обоснованность основных результатов исследований.** Обоснованность научных результатов диссертации обеспечивается:

обстоятельным сравнительным анализом достоинств и недостатков предшествующих научных разработок по исследуемой проблематике и преемственностью основных научных положений, сформулированных автором;

корректностью применения фундаментальных концепций, принципов и подходов, используемых в теории вероятности и математической статистики, теории цифровой обработки сигналов, теории проектирования и разработки программного обеспечения ЭВМ;

правильным определением ограничений и допущений при формировании исходных данных для решения задач исследования.

Достоверность результатов исследования подтверждается:

согласованностью результатов с известными публикациями отечественных и зарубежных авторов;

положительными экспертными оценками результатов диссертационного исследования в ходе их обсуждения на представительных международных научных семинарах и конференциях;

положительными результатами внедрения основных научных положений диссертации на производстве.

**Апробация и публикации.** Диссертационная работа написана хорошим научным языком, содержит 139 страниц, состоит из введения, четырех глав, заключения, списка литературы из 101 наименования и одного приложения. В заключениях по главам работы сделаны логичные, обоснованные и убедительные выводы. Результаты работы опубликованы в 6 статьях, изданных в научных изданиях рекомендованных ВАК и в зарубежных

изданиях, входящих в систему цитирования Web of Science и Scopus, в материалах 10 международных, всероссийских научно-практических конференциях и семинарах, подробно описаны в автореферате.

**Недостатки работы.** По существу диссертационной работы имеется ряд замечаний, основными из которых являются:

1. Приведенное в разделе 1.2.4 описание методов синтеза индивидуальных биометрических характеристик дано без соответствующих теоретических положений. Общее описание метода следовало бы дополнить примером.

2. Упоминаемый в разделе 2.4.1 детектор присутствия диктора не описан и может быть ошибочно интерпретирован читателем, как детектор речевой активности.

3. В работе отсутствуют оценка трудозатрат на реализацию предложенного комплекса программных средств и его дальнейшую поддержку при развитии биометрической системы.

4. В работе имеется ряд стилистических неточностей, а также опечатки.

Указанные недостатки не снижают общей научной и практической ценности работы, в которой содержится решение актуальной теоретической и прикладной проблемы, связанной с повышением эффективности аутентификации голосовыми биометрическими системами.

**Заключение**. Диссертация представляет собой целостную, завершенную научно-квалификационную работу, в которой содержится решение актуальной научной проблемы разработки методики и комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами. Содержание диссертации соответствует

профилю специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

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 ее автор, Щемелинин В.Л. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
Ведущий научный сотрудник, кафедры Вычислительной техники,
Федерального государственного автономного образовательного учреждения высшего образования Санкт-Петербургского государственного электротехнического университета "ЛЭТИ" им. В.И. Ульянова (Ленина)

кандидат технических наук Шоров Андрей Владимирович

«02» декабря 2015 г.

Рабочий адрес: 197376, Санкт-Петербург, ул. Профессора Попова, д. 5,
Телефон: (812) 234-25-03
e-mail: ashxz@mail.ru