ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета 29.12.2015 г. № 1

О присуждении Щемелинину Вадиму Леонидовичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 27 октября 2015, протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержденным приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Щемелинин Вадим Леонидович 1988 года рождения, в 2011 году окончил Санкт-Петербургский государственный университет информационных технологий, механики и оптики по специальности «Прикладная математика и информатика», присвоена квалификация «Магистр прикладной математики и информатики». Работает в настоящее время руководителем группы наукоёмкого тестирования в Обществе с ограниченной ответственностью «Центр речевых технологий».

Диссертация выполнена на кафедре речевых информационных систем Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» Министерства образования и науки Российской Федерации.

Научный руководитель – кандидат технических наук, СИМОНЧИК Константин Константинович, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» Министерства образования и науки Российской Федерации, кафедра речевых информационных систем, доцент.

Официальные оппоненты:

ПРИОРОВ Андрей Леонидович, доктор технических наук, доцент, Ярославский государственный университет им. П.Г. Демидова, кафедра динамики электронных систем, доцент;

ШОРОВ Андрей Владимирович, кандидат технических наук, Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина), кафедра вычислительной техники, ведущий научный сотрудник

дали положительные отзывы на диссертацию.

Ведущая организация – Государственное казенное образовательное учреждение высшего профессионального образования Академия Федеральной службы охраны Российской Федерации, г. Орёл в своем положительном заключении, подписанном Ивановым Борисом Рудольфовичем, доктором технических наук, профессором, Лисичкиным Владимиром Георгиевичем, доктором технических наук, доцентом, и утвержденном Козачком Василием Ивановичем, доктором социологических наук, профессором, заместителем начальника Академии ФСО России, указала, что в целом диссертационная работа В.Л. Щемелинина представляет собой завершенную научно-исследовательскую работу, выполненную на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая проблема 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 отвечает критериям «Положения о порядке присуждения ученых степеней» и соответствует требованиям ВАК Министерства науки и образования России к кандидатским диссертациям, а её автор, В.Л. Щемелинин заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 10 опубликованных работ, в том числе по теме диссертации- 10 работ, опубликованных в рецензируемых научных изданиях - 8 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ - 6, входящих в международную систему цитирования Scopus и/или «Сеть науки» - 5.

Основные научные результаты реализованы в одной научно-исследовательской работе Министерства образования и науки, 3 опытно-конструкторских работах, 10 научных трудов общим объемом 5,3 п.л., из которых 9 работ объемом 4,85 п.л., выполнены в соавторстве, а одна статья объемом 0,45 п.л. – лично. Наиболее значительные работы по теме диссертации:

1. **Щемелинин В.Л.**, Симончик К.К. Исследование устойчивости голосовой верификации к атакам, использующим систему синтеза // Известия высших учебных заведений. Приборостроение - 2014. - Т. 57. - № 2. - С. 84-88.
2. **Shchemelinin V.**, Topchina M., Simonchik K. Vulnerability of Voice Verification Systems to Spoofing Attacks with TTS Voices Based on Automatically Labeled Telephone Speech // Lecture Notes in Artificial Intelligence, 2014, Vol. 8773, C. 475–481.
3. **Shchemelinin V.**, Kozlov A., Lavrentyeva G., Novoselov S., Simonchik K. Vulnerability of Voice Verification System with STC Anti-spoofing Detector to Different Methods of Spoofing Attacks // Lecture Notes in Artificial Intelligence, 2015, Vol. 9319, C. 480-486.

4. Lavrentyeva G., Shchemelinin V., Kozlov A., Novoselov S., Simonchik K. Automatically Trained TTS for Effective Attacks to Anti-spoofing System // Lecture Notes in Artificial Intelligence, 2015, Vol. 9319, pp. 137-143.
5. Novoselov S., Kozlov A., Lavrentyeva G., Simonchik K. and Shchemelinin V. STC Anti-spoofing Systems for the ASVspoof 2015 Challenge [Электронный ресурс] - Режим доступа: http://www.spoofingchallenge.org/asvspoof2015/STC.pdf, свободный. Яз. Англ. (дата обращения 23.09.2015).

На автореферат диссертации поступило 7 отзывов, все отзывы положительны:

1) Белорусский государственный университет информатики и радиоэлектроники. Отзыв составил заведующий кафедрой электронных вычислительных средств, д.т.н., профессор Петровский А.А. Отзыв положительный. Замечания: Из материалов автореферата, остаётся не ясным, являются ли предложенные решения универсальными для иностранных языков, или их применимость ограничена голосовыми биометрическими системами, работающими с русским языком. В описании четвёртой главы диссертации (стр. 16-18 автореферата) следовало привести более подробное описание предлагаемого метода детектирования спуфинг атак за счёт сокращения обзорной информации в описании первой главы (стр. 8-9 автореферата).

2) Санкт-Петербургский государственный морской технический университет. Отзыв составил доцент кафедры морских информационных систем и технологий, к.т.н., Семёнов Н.Н. Отзыв положительный. Замечания: Одним из перспективных направлений в области голосовой биометрии является использование глубоких нейронных сетей (Deep Neural Net, DNN). В экспериментах, проведённых автором, используются голосовые биометрические системы, не содержащие данный подход. Остаётся не ясным, насколько серьёзную угрозу представляют описанные методы спуфинг атак для голосовых биометрических систем, опирающихся на DNN подход. В списке публикаций автора по теме диссертации, работы, опубликованные в международных изданиях, индексируемых в базе данных Scopus, не отделены от работ, опубликованных в изданиях, рекомендованных ВАК при МОиН РФ.

3) Национальный исследовательский университет «Высшая школа экономики». Отзыв составил доцент департамента анализа данных и искусственного интеллекта

факультета компьютерных наук, к.т.н., Игнатов Д.И. Отзыв положительный. Замечания: В автореферате не объяснён выбор довольно простого линейного ядра в SVM-классификаторе (нет сравнения с альтернативами, например ядром полиномиальном), а также не приведены сравнительные экспериментальные оценки эффективности аутентификации голосовой биометрической системы с другими методами детектирования спуфинг атак, представленными на международном конкурсе Automatic Speaker Verification Spoofing and Countermeasures.

4) ФГУП «НИИ «Квант». Отзыв составил заведующий лабораторией автоматического транскрибирования речи, к.т.н., профессор Воробьёв В.И. Отзыв положительный. Замечания: В автореферате довольно кратко представлено описание разработанного комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами и выполненного для него экспериментального анализа с оценкой получаемого практического эффекта. Скорее всего, это является недостатком формата автореферата. При оценке устойчивости аутентификации голосовыми биометрическими системами к спуфинг атакам, основанным на технологии синтеза, используется просто HMM синтез (стр. 12 автореферата), остаётся не ясным, какое воздействие на систему окажут атаки, основанные на более совершенных, гибридных методах синтеза. В тексте автореферата содержится несколько пунктуационных опечаток и стилистических неточностей.

5) Филиал корпорации «ЛГ Электроникс Инк». Отзыв составил научный сотрудник, к.т.н., Гусев М.Н. Отзыв положительный. Замечания: Материалы автореферата не позволяют судить о возможности применения предложенных решений в различных каналах связи, в частности телефонном и микрофонном. Указание на использованный в экспериментах канал связи также отсутствует в тексте автореферата. Из текста автореферата остаётся не ясным, какие именно признаки используются в предложенном методе детектирования спуфинг атаки.

6) ООО «А-ВИЖН». Отзыв составил руководитель группы связи и передачи данных проектного отдела, к.т.н. Савватин А.И. Отзыв положительный. Замечания: В описании первой главы, помимо методов спуфинг атак, основанных на технологиях синтеза и преобразования речи, упоминаются также методы, основанные на приёме

имперсонализации, а также записи и повторе биометрических характеристик (стр. 9 автореферата), однако далее по тексту они не используются. Остаётся не ясным, какую угрозу представляют данные методы атак для современных голосовых биометрических систем. В тексте автореферата не указано об исследованиях работы алгоритма в условиях аддитивных шумов.

7) ООО "Нетрикс Европа". Отзыв составил руководитель группы разработки программного обеспечения, к.т.н., Чистиков П.Г. Отзыв положительный. Замечания: Из текста автореферата остаётся неясным, почему выбран именно такой набор численных показателей эффективности. Рассматривая современные методы построения и сравнения голосовых моделей, автор приводит спектрально-формантный метод, метод основного тона и другие (стр. 8 автореферата). Однако в описании проведённых экспериментов упоминается только система на базе вероятностного линейного дискриминантного анализа (стр. 12 автореферата). Остаётся не ясным, как описанные методы спуфинг атак влияют на надёжность систем, основанных на других методах сравнения голосовых моделей.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент Приоров А.Л. является известным ученым в области цифровой обработки сигнала, защиты и передачи речевой информации; к.т.н. Шоров А.В. – ведущий ученый в области имитационного моделирования атак на компьютерные сети и механизмов защиты от них; ведущая организация,-Государственное казенное образовательное учреждение высшего профессионального образования Академия Федеральной службы охраны Российской Федерации, является известной как в России, так и за рубежом организацией в области разработки и создания систем обеспечения конфиденциальности, целостности и доступности информации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны методические основы оценки эффективности аутентификации голосовыми биометрическими системами, позволяющие разрабатывать решения по её совершенствованию за счёт учёта влияния спуфинг атак на модуль ввода биометрической информации при проведении технологических испытаний и на этапах разработки системы, повысить обоснованность принимаемых решений за счет

введения дополнительных численных и графических показателей эффективности системы и автоматизации процессов анализа;

предложен оригинальный подход к решению проблемы повышения эффективности аутентификации голосовыми биометрическими системами, отличительной особенностью которого является внедрение дополнительных численных показателей эффективности в методику оценки и комбинирование методов факторного анализа, сигнальной обработки и признакового описания сигнала в задаче детектирования спуфинг атаки в звуковом сигнале, обеспечивающее значительное повышение устойчивости голосовых биометрических систем к различным методам спуфинг атак на модуль ввода биометрической информации;

доказана перспективность использования разработанного специального методологического, методического и программного обеспечения решения проблемы повышения эффективности аутентификации голосовыми биометрическими системами, базирующегося на оригинальной реализации предложенного подхода по оценке эффективности аутентификации голосовыми биометрическими системами и противодействия угрозам за счёт детектирования спуфинг атак;

введены новые понятия, термины и определения, позволяющие раскрыть суть нового подхода и методологии решения проблемы оценки и повышения эффективности аутентификации голосовыми биометрическими системами и проводить исследования устойчивости голосовых биометрических систем к различным методам спуфинг атак более полно и с единых позиций.

Теоретическая значимость исследования обоснована тем, что:

доказаны возможность использования гибридного метода синтеза биометрических характеристик и методов автоматической разметки звукового сигнала в задаче имитационного моделирования спуфинг атаки на голосовые биометрические системы; возможность использования новых численных и графических показателей эффективности аутентификации голосовыми биометрическими системами, отражающих устойчивость к спуфинг атакам, при проведении технологических испытаний голосовой биометрической системы; возможность применения модуля имитации спуфинг атаки в комплексе программных средств оценки эффективности аутентификации голосовыми биометрическими системами; возможность применения

методов факторного анализа, амплитудных и фазовых признаков, используемых в задаче идентификации диктора для решения задачи детектирования фальсифицированного сигнала при незначительном увеличении ошибки ложного несовпадения голосовой биометрической системы;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы методологический аппарат общей теории вероятности и математической статистики, методы цифровой обработки сигнала, теории планирования эксперимента, методы экспертного оценивания, поисковой оптимизации, теории проектирования и разработки программного обеспечения;

изложены методологические и методические основы решения проблемы оценки и повышения эффективности аутентификации голосовыми биометрическими системами в условиях воздействия спуфинг атак на различные компоненты системы, включая модуль ввода биометрической информации;

раскрыты противоречия между существующими стандартами оценки эффективности аутентификации голосовыми биометрическими системами, в которых не учитываются активные воздействия злоумышленников, направленные на взлом системы и возросшей угрозой со стороны методов спуфинг атак на модуль ввода биометрической информации, основанных на значительно развившихся в последние годы технологиях синтеза и преобразования индивидуальных биометрических признаков человека;

изучены существующие концепции и подходы к имитации спуфинг атак на голосовые биометрические системы с использованием методов синтеза и преобразования индивидуальных биометрических характеристик человека, оценке эффективности аутентификации голосовыми биометрическими системами, решению задачи распознавания диктора в речевом сигнале, повышения эффективности аутентификации голосовыми биометрическими системами путём обнаружения следов спуфинг атаки во входном речевом сигнале;

проведена модернизация существующих методик и методов исследования оценки эффективности аутентификации голосовыми биометрическими системами, позволившая учитывать активные воздействия злоумышленников на модуль ввода

биометрической информации, выявлять уязвимость голосовых биометрических систем к различным методам спуфинг атак, разрабатывать методы повышения эффективности аутентификации голосовыми биометрическими системами путём детектирования следов фальсификации биометрических характеристик во входном звуковом сигнале, проводить анализ и сравнивать различные методы повышения эффективности аутентификации голосовыми биометрическими системами.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

1) методика и комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами, позволяющие оценивать эффективность аутентификации голосовыми биометрическими системами на этапе их разработки, а также предложенные методы по совершенствованию защиты голосовых биометрических систем, позволяющие повысить устойчивость голосовых биометрических систем к спуфинг атакам на модуль ввода биометрической информации в обществе с ограниченной ответственностью «Центр речевых технологий» в опытно–конструкторских разработках автоматических систем идентификации личности по голосу и производстве коммерческих продуктов: биометрическая платформа для подтверждения личности по голосу "VoiceKey", система поиска голосов мошенников в больших архивах аудиозаписей "VoiceGrid X", мультимодальная система биометрического поиска и криминалистического учёта "VoiceGrid";

определены возможности и перспективы практического использования полученных результатов диссертации при исследовании и разработке голосовых биометрических систем;

создан экспериментальный образец комплекса программных средств, успешно интегрированный в инфраструктуру разработки голосовых биометрических систем и позволяющий проводить оценку эффективности аутентификации голосовыми биометрическими системами с учётом влияния воздействия имитаций различных методов спуфинг атак;

представлены предложения и направления научных исследований для дальнейшего совершенствования эффективности аутентификации голосовыми биометрическими системами.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ воспроизводимость результатов многократных экспериментов, выполненных на сертифицированном современном оборудовании; достоверность полученных решений проблемы оценки и повышения эффективности аутентификации голосовыми биометрическими системами подтверждена обоснованным применением аналитических методов: теории вероятности, математической статистики, цифровой обработки сигнала, планирования эксперимента, экспертного оценивания, поисковой оптимизации, проектирования и разработки программного обеспечения; количественным и качественным согласованием с результатами, полученными на основе известных методов решения;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методах исследования, согласуется с опубликованными экспериментальными данными по теме диссертации;

идея базируется на анализе работ отечественных и зарубежных исследователей в области голосовых биометрических технологий; на обобщении передового опыта в этой области;

использованы полученные экспериментальные результаты для сравнения с данными, приведенными в современной научной литературе по голосовым биометрическим технологиям;

установлено качественное и количественное соответствие результатов решения задач оценки и повышения эффективности аутентификации голосовыми биометрическими системами с результатами, полученными с использованием стандартных методов оценки эффективности аутентификации; подтверждено преимущество решения задачи оценки эффективности аутентификации голосовыми биометрическими системами на основе предложенной методологии перед результатами, полученными другими авторами либо известными методами;

использованы сертифицированные оборудование и программные средства.

Личный вклад соискателя состоит в: постановке проблемы оценки эффективности аутентификации голосовыми биометрическими системами при воздействии спуфинг атак на модуль ввода биометрической информации, основанных на технологии синтеза биометрических характеристик, разработке методики и комплекса программных средств для её решения, анализе современного состояния объекта и предмета исследования, ведущем участии в проведении вычислительных экспериментов. Автору принадлежит решающая роль в апробации результатов исследования; разработке методов имитации атак на модуль ввода биометрической системы; разработке методики и комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами, обеспечивающих учёт влияния воздействия спуфинг атак на модуль ввода биометрической информации, как при технологических испытаниях системы, так и на этапах её разработки; подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Щемелинин В.Л. в своей диссертационной работе решил задачу повышения эффективности аутентификации голосовыми биометрическими системами, имеющую важное социально-экономическое и хозяйственное значение.

На заседании 29.12.2015 г. диссертационный совет принял решение присудить Щемелинину В.Л. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 24 человек, из них 8 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 24, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета Фаткиева Роза Равильевна

29.12.2015 г.