Никифоров

«__» _____ 2015 г.

ЗАКЛЮЧЕНИЕ

Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО) Министерства образования и науки Российской Федерации.

Диссертация «Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами» выполнена на кафедре речевых информационных систем Университета ИТМО.

Работал в ООО "ЦРТ" руководителем группы наукоёмкого тестирования, научно исследовательского департамента.

В 2011 г. соискатель Щемелинин Вадим Леонидович окончил Санкт-Петербургский государственный университет информационных технологий механики и оптики по специальности 010500 «Прикладная математика и информатика».

В период подготовки диссертации проходил обучение в заочной аспирантуре Университета ИТМО Министерства образования и науки Российской Федерации,

Справка об обучении № 37/2015, выдана в 2015г Университетом ИТМО Министерства образования и науки Российской Федерации.

Научный руководитель – Симончик Константин Константинович, кандидат технических наук, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО) Министерства образования и науки Российской Федерации, доцент кафедры речевых информационных систем.

По итогам рассмотрения принято следующее заключение:

1. Личное участие соискателя в получении результатов, изложенных в диссертации.

Автором лично проведён анализ уязвимости современных голосовых биометрических систем к различным способам фальсификации индивидуальных голосовых биометрических характеристик человека. На основе проведённого анализа, разработана методика оценки эффективности аутентификации голосовыми биометрическими системами. Разработан комплекс программных средств, позволяющий применить предложенную методику на практике. С учётом проведённых исследований, разработан метод противодействия спуфинг атакам

на модуль ввода биометрической информации в голосовую биометрическую систему. Подготовка основных публикаций проводилась с соавторами, при этом вклад автора был основным.

2. Степень достоверности результатов проведенных исследований.

Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается результатами экспериментальных исследований, апробацией основных положений в ряде ведущих международных конференций, анализе состояния исследований в рассматриваемой области, а также результатами испытаний реальных систем, при оценке эффективности которых, были использованы предложенные методы, методика и комплекс программных средств. Практические рекомендации, сформулированные в диссертации, обоснованы проведенными исследованиями и могут служить руководством в работе.

3. Новизна и практическая значимость результатов исследования.

Главный результат представленной работы заключается в исследовании и разработке методики оценки эффективности аутентификации голосовыми биометрическими системами, позволяющей комплексно оценивать различные системы распознавания диктора по голосу и корректно сравнивать их между собой с учётом возможных атак на устройство ввода биометрической информации.

Практическая значимость работы заключается в реализации предложенных методик в виде комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами. Разработанные технические решения по совершенствованию защиты заняли второе место на международном конкурсе ASVspoof Challenge 2015 и могут быть встроены в коммерческие голосовые биометрические системы.

Приведенные решения были опубликованы в журналах ВАК и докладывались на известных международных конференциях по тематике речевых технологий.

4. Ценность научных работ соискателя.

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 “ЦРТ”.

5. Научная специальность, которой соответствует диссертация.

Диссертационная работа соответствует требованиям п. 9 Положения о присуждении ученой степени и п. 10 Паспорта специальностей ВАК, технические науки, по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

6. Полнота изложения материалов диссертации в работах, опубликованных соискателем.

Основное содержание диссертационного исследования достаточно полно отражено в автореферате и в 10 работах соискателя, в том числе в шести работах в журналах, рекомендованных ВАК Минобрнауки РФ, в том числе в пяти работах в изданиях, включенных в систему цитирования Scopus:

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. – статья – 0,5 п.л. / 0,28 п.л.

   В работе описаны результаты исследования устойчивости современных текстозависимых методов верификации диктора к атакам, основанным на технологии гибридного синтеза речи. Предложена модель нарушителя, использующего существующие системы гибридного синтеза на основе методов HMM и Unit Selection. Показана высокая уязвимость лучших (по результатам конкурса NIST SRE 2012) современных методов текстозависимой верификации диктора к предложенной модели нарушителя.

2. Shchemelinin V., Simonchik K.K. Examining vulnerability of voice verification systems to spoofing attacks by means of a TTS system // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2013, Vol. 8113, No. LNAI, pp. 132-137. – статья – 0,7 п.л. / 0,4 п.л.

   В данной статье рассматривается влияние размера обучающей базы при подготовке фальсифицированной парольной фразы гибридной системой синтеза. Обучающие данные размечаются экспертом и используются для подготовки голоса синтеза, используемого в дальнейшем для атаки на систему верификации. Как показали эксперименты, использование восьми минут речи человека для обучения системы синтеза, достаточно для снижения надёжности системы верификации с 96% до 56%, что является недопустимо низким показателем для подобных систем. При этом в случае увеличения объёма обучающих данных до четырёх часов речи, надёжность работы системы уменьшалась до 1,6%, что фактически гарантирует

успешность атаки на систему при отсутствии мер противодействия атаке и не наличии неограниченных ресурсов у злоумышленника. Сделано предположение, что причиной столь сильного воздействия данной модели атаки является ручная экспертная разметка обучающих данных.

3. Simonchik K., Shchemelinin V. "STC SPOOFING" DATABASE FOR TEXT-DEPENDENT SPEAKER RECOGNITION EVALUATION // Proc. 4th International Workshop on Spoken Language Technologies for Under-resourced Languages (SLTU) - 2014, pp. 221-224. – статья – 0,4 п.л. / 0,17 п.л.

   Приведено описание речевой базы, и нескольких метрик для проведения оценки уязвимости голосовой биометрической системы к спуфинг атакам. Речевая база содержала речь дикторов разного пола для подготовки эталонных моделей дикторов и фальсифицированную речь для имитации атаки на основе гибридного метода синтеза с различным объёмом обучающих данных. В качестве метрик предлагалось использовать численное значение ВЛС в двух точках, при пороге равном порогу в точке EER и при пороге равном порогу при котором ВЛС на калибровочной базе равнялось 0,01%

4. 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 Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2014, Vol. 8773, No. LNAI, pp. 475–481. – статья – 0,7 п.л. / 0,28 п.л.

   В данной работе приведены результаты исследования устойчивости современных систем текстозависимой верификации к спуфинг атакам, основанным на гибридном синтезе в условиях телефонного канала. Основным отличием данного исследования от предыдущих является не только использование телефонного канала связи, который намного более вероятен при проведении подобной атаки, но и применение технологии автоматической разметки для обучающей речевой базы данных. Таким образом, данный метод имитации атаки теоретически может быть полностью автоматизирован и потенциально представляет очень высокую угрозу для незащищённой системы. Результаты показали, что надёжность систем распознавания падает с 96% до 85,2%, что с учётом возможности полной автоматизации процесса атаки и отсутствием организационных и технических решений по противодействию подобным атакам у современных систем, делает данную угрозу существенной.

5. Sukhmel V., Aleinik S., Shchemelinin V. Voice Passphrase Variability Evaluation for Speaker Recognition // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2015, Vol. 8915, pp. 3-9. – статья – 0,7 п.л. / 0,1 п.л.

Предложен ряд организационных и технических решений по совершенствованию защиты систем текстозависимого распознавания диктора по голосу. Эксперименты показали, что при применении предложенных решений, основанных на анализе формант используемых в парольной фразе, можно существенно повысить надёжность работы системы верификации при "пассивных" транзакциях "самозванца".

6. Манукянц В.Э., Щемелинин В.Л. Тестирование наукоёмких SDK // Сборник тезисов XVI международной конференции по вопросам качества программного обеспечения SQA Days 16 - 2014. - С. 70. . – статья – 0,05 п.л. / 0,03 п.л.

   В произведённом докладе освещены существующие подходы к тестированию SDK содержащих вероятностные алгоритмы. Описаны основные проблемы, возникающие при решении задачи оценки эффективности различных биометрических алгоритмов и алгоритмов распознавания. Предложен ряд организационных и технических решений по решению данной задачи.

7. Щемелинин В.Л. Оценка эффективности биометрических систем // Альманах научных работ молодых ученых Университета ИТМО. – СПб: Университет ИТМО, 2015. - Т. 3. - С. 250-254. – статья – 0,45 п.л. / 0,4 п.л.

   В данной работе рассмотрены современные угрозы для систем распознавания диктора по голосу. Предложен вариант методики оценки эффективности процесса аутентификации в голосовой биометрической системе с учётом возможных угроз.

8. Novoselov S., Kozlov A., Lavrentyeva G., Simonchik K. and Shchemelinin V. STC Anti-spoofing Systems for the ASVspoof 2015 Challenge // arXiv:1507.08074 - 2015. – статья – 0,4 п.л. / 0,05 п.л.

   В статье описана система детектирования различных спуфинг атак, направленных на модуль ввода биометрической информации системы распознавания диктора по голосу. Разработанная и предложенная на конкурс Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015 система, заняла второе место среди более чем 16 участников из различных ведущих университетов и коммерческих компаний, таких как CRIM и SpeechLab.

9. Lavrentyeva G., Shchemelinin V., Kozlov A., Novoselov S., Simonchik K. Automatically Trained TTS for Effective Attacks to Anti-spoofing System // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2015, Vol. 9319, No. LNAI, pp. 137-143. – статья – 0,7 п.л. / 0,12 п.л.

В статье описаны результаты оценки надёжности детектора спуфинг атаки при имитации атаки на основе гибридного метода синтеза и ряда других методов использующих технологию синтеза и преобразования речи. Из результатов работы следует, что метод гибридного синтеза по прежнему остаётся наиболее опасным как для систем распознавания дикторов, так и для технических решений по совершенствованию защиты систем распознавания дикторов по голосу.

10. 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 Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2015, Vol. 9319, No. LNAI, pp. 480-486. – статья – 0,7 п.л. / 0,35 п.л.

В работе предложен метод объединения системы детектирования атаки с системой распознавания диктора по голосу. Сделан ряд ключевых выводов по необходимости комплексной оценки эффективности систем распознавания диктора по голосу, оборудованных подсистемами детектирования спуфинг атак. Проведённые эксперименты показали, что при применении разработанного решения по противодействию спуфинг атакам, вероятность успешной атаки снижается с 77,1% до 1,35%.

Диссертация «Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами» Щемелинина Вадима Леонидовича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заключение принято на заседании кафедры речевых информационных систем Университета ИТМО.

Присутствовало на заседании 7 чел.

Результаты голосования: «за» - 7 чел., «против» - нет, «воздержалось» - нет, протокол № 1 от «10» сентября 2015 г.