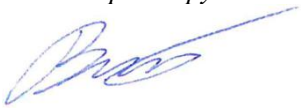
На правах рукописи



Щемелинин Вадим Леонидович

Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт - Петербург - 2015

Работа выполнена в Санкт-Петербургском национальном исследовательском университете информационных технологий, механики и оптики (НИУ ИТМО) на кафедре речевых информационных систем.

Научный руководитель: **Симончик Константин Константинович**
кандидат технических наук, доцент кафедры речевых информационных систем НИУ ИТМО

Официальные оппоненты: **Приоров Андрей Леонидович**
доктор технических наук, доцент
Ярославский государственный университет им. П.Г. Демидова, доцент кафедры динамики электронных систем

Шоров Андрей Владимирович
кандидат технических наук,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), ведущий научный сотрудник кафедры вычислительной техники

Ведущая организация: Государственное казенное образовательное учреждение высшего профессионального образования Академия Федеральной службы охраны Российской Федерации

Защита состоится «29» декабря 2015 г. в 11 часов 00 минут на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, г. Санкт-Петербург, В.О., 14 линия, д. 39.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук по адресу: 199178, г. Санкт-Петербург, 14 линия, д. 39 и на сайте http://www.spiiras.nw.ru/dissovet/.

Автореферат разослан «__» _____ 2015 г.

Ученый секретарь Диссертационного совета Д 002.199.01
кандидат технических наук Р.Р. Фаткиева

Общая характеристика работы

Актуальность темы исследования

Развитие компьютерных технологий в последние десятилетия дало возможность совершить прорыв в области обработки речевого сигнала. Современный мир уже сложно представить без повседневного использования речевых технологий. Системы распознавания речи позволяют не отвлекаться на управление мобильными устройствами во время движения за рулем, системы синтеза речи оповещают нас по телефону, в метро, на вокзалах и в офисах, голосовые биометрические системы обеспечивают решение задачи аутентификации при доступе к защищенным персональным данным или поиске нарушителей.

Исследования голосовых биометрических технологий занимают одно из ведущих мест в области обработки речевого сигнала. В первую очередь, следует отметить основополагающие работы авторов Douglas A. Reynolds, Patrick J. Kenny. Регулярные оценки эффективности аутентификации голосовыми биометрическими системами проводятся в виде конкурса Национальным Институтом Стандартов и Технологий США (NIST). Целью конкурса является определение доминирующих направлений в данной технологии. Однако, возникающие при обработке речевого сигнала задачи, в виду их комплексного характера и сложности, далеки от того, чтобы их можно было считать решенными как в практическом, так и в научном плане.

В последнее время все большее количество потребителей биометрических систем озабочено не только качеством непосредственно голосовой биометрии, но и противодействием различным видам спуфинг атак, проводимых с целью получения доступа к защищенной информации.

Большую работу в направлении исследования спуфинг атак на голосовые биометрические системы провела группа исследователей под руководством Tomi Kinnunen в Университете Восточной Финляндии. В 2015 году ими был организован первый в мире международный конкурс Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015 при крупнейшей конференции по речевым технологиям Interspeech. Результаты их исследований показали не только уязвимость голосовых

биометрических систем к простейшим атакам на основе записи речи на диктофон, но и к более сложным способам синтеза голоса, а также к преобразованию голоса злоумышленника к заданному голосу пользователя системы.

Таким образом, методы противодействия спуфинг атакам, позволяющие повысить степень защиты голосовых биометрических систем, являются на сегодняшний день крайне актуальными. Оценка эффективности аутентификации, используемой современными голосовыми системами безопасности, должна включать не только требования к надежности базовой технологии идентификации диктора, но и к защищенности такого рода систем от несанкционированных попыток доступа к ним.

Целью исследования является повышение эффективности аутентификации голосовыми биометрическими системами в условиях возможных спуфинг атак.

Для достижения поставленной цели были сформулированы и решены следующие основные **задачи:**

1. Анализ уязвимости современных голосовых биометрических систем к различным способам фальсификации индивидуальных голосовых биометрических характеристик человека.
2. Разработка методики оценки эффективности аутентификации голосовыми биометрическими системами с учетом возможного влияния различных видов спуфинг атак на модуль ввода биометрической информации.
3. Разработка комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами.
4. Разработка метода противодействия спуфинг атакам, позволяющего повысить устойчивость голосовых биометрических систем к спуфинг атакам различного вида на модуль ввода биометрической информации.

Объект исследования. Голосовые биометрические системы и способы фальсификации индивидуальных голосовых биометрических характеристик человека.

Предмет исследования. Методика и комплекс средств оценки эффективности аутентификации голосовыми биометрическими системами, оценка защищенности и выбор средств защиты персональных данных, обрабатываемых в голосовых биометрических системах.

Методы исследования. В работе использованы методы теории вероятности и математической статистики, цифровой обработки сигналов, методы проектирования и разработки программного обеспечения ЭВМ.

Научная новизна диссертационного исследования заключается в следующем:

1. Предложенный метод имитации атак на голосовые биометрические системы отличается применением автоматической разметки речевых данных для создания модели синтезированного голоса целевого диктора.
2. Предложенная методика оценки эффективности аутентификации голосовыми биометрическими системами отличается учетом воздействия различных видов спуфинг атак на модуль ввода биометрической информации.
3. Реализованный комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами отличается наличием модуля имитации атаки и модуля расчета показателей эффективности аутентификации с учетом воздействия спуфинг атак.
4. Разработанный метод противодействия спуфинг атакам отличается комбинированием методов факторного анализа, сигнальной обработки и признакового описания сигнала.

Основные положения, выносимые на защиту.

1. Метод имитации атак на голосовые биометрические системы, обеспечивающий автоматическое создание модели голоса для синтеза голосовых биометрических характеристик.
2. Методика оценки эффективности аутентификации голосовыми биометрическими системами, обеспечивающая учет воздействия различных видов спуфинг атак на модуль ввода биометрической информации.

3. Комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами, позволяющий оценивать устойчивость к различным видам атак при проведении технологических испытаний.

4. Метод противодействия спуфинг атакам, позволяющий значительно повысить устойчивость голосовых биометрических систем к различным методам спуфинг атак на модуль ввода биометрической информации.

Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается результатами экспериментальных исследований, успешным представлением основных положений в ряде докладов на ведущих международных конференциях, в том числе, на международном конкурсе Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015, а также результатами технологических испытаний реальных систем, при оценке которых были использованы предложенные методы, методика и комплекс программных средств. Практические рекомендации, сформулированные в диссертации, обоснованы проведенными исследованиями и могут служить руководством при решении практических задач.

Практическая значимость работы заключается в реализации предложенной методики 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.

Внедрение результатов работы. 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”.

Апробация результатов исследования. Результаты, полученные в рамках работы над диссертацией, представлялись и обсуждались на следующих научно-методических конференциях: «15th International Conference on Speech and Computer SPECOM 2013» (Пльзень, Чехия, 2013), «XLIII научная и учебно-методическая конференция НИУ ИТМО» (Санкт-Петербург, 2014), «III Всероссийский конгресс молодых ученых» (Санкт-Петербург, 2014) - диплом за лучший доклад на секции, «4th International Workshop on Spoken Language Technologies for Under-resourced Languages (SLTU'14)» (Санкт-Петербург, 2014), «16th International Conference on Speech and Computer SPECOM 2014» (Новый Сад, Сербия), «XVI Международная конференция по вопросам качества программного обеспечения SQA Days 16» (Санкт-Петербург, 2014), «XLIII научная и учебно-методическая конференция НИУ ИТМО» (Санкт-Петербург, 2014), «XLIV научная и учебно-методическая конференция НИУ ИТМО» (Санкт-Петербург, 2015), а также были представлены в виде системы детектирования атак, занявшей 2-ое место на международном конкурсе Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015.

Личный вклад автора. Автором лично проведен анализ уязвимости современных голосовых биометрических систем к различным способам фальсификации индивидуальных голосовых биометрических характеристик человека. На основе проведенного анализа разработана методика оценки эффективности аутентификации голосовыми биометрическими системами с учетом возможного влияния различных видов атак на модуль ввода биометрической информации. Проведены исследования, демонстрирующие преимущества предложенной методики в сравнении с существующими аналогами. Разработан комплекс программных средств, позволяющий применить предложенную методику на практике. С учетом проведенных исследований разработан метод противодействия спуфинг атакам, позволяющий повысить устойчивость голосовых биометрических систем к различным

методам спуфинг атак на модуль ввода биометрической информации. Подготовка основных публикаций проводилась с соавторами, при этом вклад автора был основным.

Публикации. По теме диссертации опубликовано десять печатных работ, шесть из которых - в изданиях из перечня рецензируемых научных журналов ВАК, в том числе, пять - в международных изданиях, индексируемых в базе данных Scopus.

Объем и структура диссертации

Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы. Материал изложен на 139 страницах, включает 8 таблиц, 29 рисунков и схем, а также одно приложение. Список использованной информации содержит 101 наименование.

Содержание работы

Во **введении** обосновывается актуальность выбранной темы диссертационного исследования, характеризуется степень ее разработанности, определяются цели и задачи, осуществляется выбор предмета и объекта исследования. Формулируются положения, выносимые на защиту.

В первой главе произведен обзор современных голосовых биометрических систем. Описаны особенности функций, выполняемых данными системами: регистрации, верификации и идентификации.

Рассмотрены современные методы построения и сравнения голосовых моделей, такие как: метод основного тона; спектрально-форматный метод; метод на базе применения смесей гауссовых распределения (СГР); метод факторного анализа в пространстве “полной изменчивости” (Total Variability Joint Factor Analysis, TV-JFA); метод на основе вероятностного линейного дискриминантного анализа (Probability Linear Discriminant Analysis, PLDA).

Приведена обобщенная структура голосовой биометрической системы, включающая такие компоненты, как: устройство ввода; подсистема обработки речевых данных; подсистема хранения шаблонов; подсистема сравнения и принятия решения; интерфейс

приложения; подсистема передачи данных. Основные компоненты системы показаны на рисунке 1. Отмечено, что многие голосовые биометрические системы основаны на одних и тех же биометрических комплектах средств разработки (Software Development Kit, SDK), являющихся ядром таких компонентов, как подсистема обработки данных и подсистема сравнения и принятия решения.

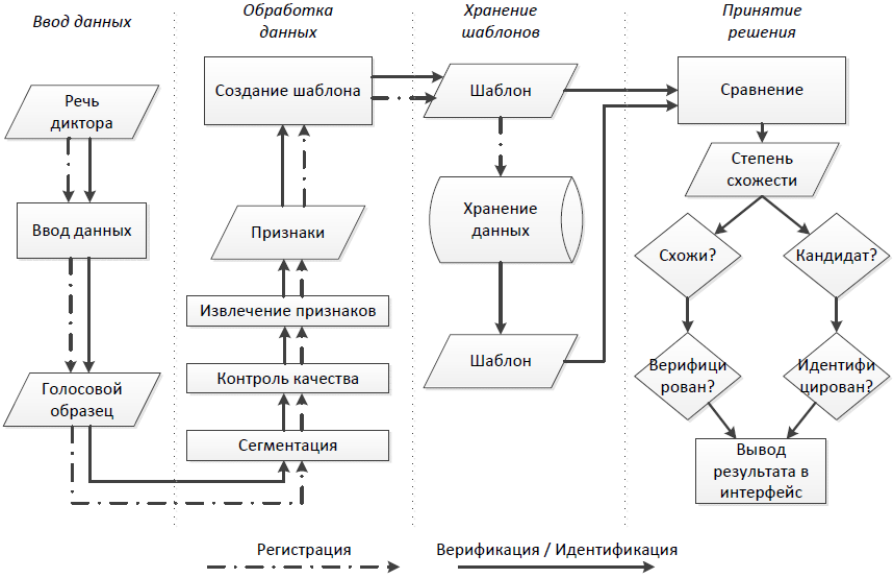


Рисунок 1 — Компоненты обобщенной голосовой биометрической системы

Описаны различные виды атак на устройство ввода данных голосовой биометрической системы с целью взлома (спуфинг атак):

– Методы, основанные на приеме имперсонализации.

– Методы, основанные на записи голосовых биометрических характеристик человека и их дальнейшем повторе.

– Методы, основанные на технологии преобразования речи злоумышленника в речь другого человека.

– Методы, основанные на технологии синтеза речи.

Приведены известные решения по увеличению защищенности голосовых биометрических систем к описанным видам атак.

Рассмотрены существующие подходы к оценке эффективности аутентификации голосовыми биометрическими системами. Отмечено

отсутствие в принятых стандартах численных показателей, отображающих устойчивость к различным видам спуфинг атак на голосовые биометрические системы.

В заключении отмечено, что за последнее десятилетие удалось достичь значительного прогресса в технологии голосовой биометрии, что делает использование голосовых биометрических систем для решения задачи аутентификации все более распространенным. Анализ известных методик оценки устойчивости голосовых биометрических систем к спуфинг атакам, использующим технологии синтеза и преобразования индивидуальных биометрических характеристик, не позволяет утверждать, что задача оценки эффективности аутентификации голосовыми биометрическими системами себя исчерпала. Требуется проанализировать уязвимость голосовых биометрических систем к спуфинг атакам, основанным на современных методах преобразования и синтеза индивидуальных биометрических характеристик. Необходимо разработать решения по совершенствованию защиты голосовых биометрических систем. Также при подготовке методики и комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами следует уделить внимание дальнейшему развитию и совершенствованию технологий преобразования и синтеза речи.

Во второй главе диссертации проведен анализ уязвимости компонентов обобщенной голосовой биометрической системы. Проведена типизация нарушителей, воздействующих на систему. Определены и классифицированы типовые сценарии атак на различные компоненты обобщенной голосовой биометрической системы. На рисунке 2 отображена общая схема системы с обозначенными атаками. Отмечено, что только атака на устройство ввода биометрической информации не является общей для всех биометрических систем и требует уникальных методов противодействия. Для оценки устойчивости аутентификации голосовыми биометрическими системами к спуфинг атакам на устройство ввода смоделированы сценарии атак, основанные на методах преобразования и синтеза индивидуальных биометрических характеристик.

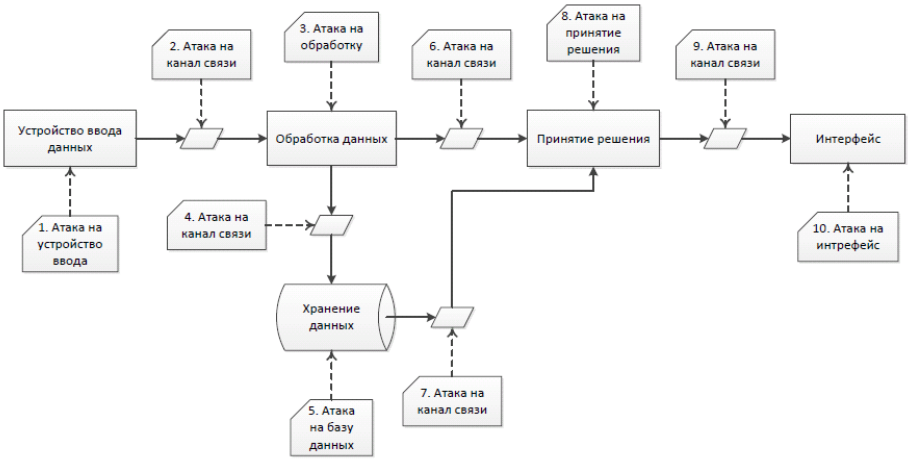


Рисунок 2 — Компоненты обобщенной голосовой биометрической системы с обозначенными атаками

Эксперимент проводится на 3497 записях 35 дикторов (15 мужчин и 20 женщин). Для моделирования атак используются 49875 фальсифицированных записей, полученных пятью методами (*S1-S5*):

1. *S1* - Метод преобразования речи, основанный на простой реализации алгоритма замены фреймов речи "самозванца" на соответствующий фрейм речи зарегистрированного пользователя.
2. *S2* - Простой метод преобразования речи, заключающийся в замене первого мел-кепстрального коэффициента, которая направлена на уменьшение различий в спектрах целевой и исходной речи.
3. *S3* - Метод синтеза речи, основанный на применении статистических моделей (HMM-синтез) и адаптацией на 20 фразах целевого диктора.
4. *S4* - Совпадает с *S3*, но для адаптации используются 40 записей целевого диктора.
5. *S5* - Опирается на Festvox систему, открытый инструмент по преобразованию речи.

В качестве графического показателя уязвимости системы выбраны кривые КОО (компромиссного определения ошибки, DET curve). Результаты эксперимента с голосовой биометрической системой на базе вероятностного линейного дискриминантного

анализа (Probability Linear Discriminant Analysis, PLDA) показаны на рисунке 3.

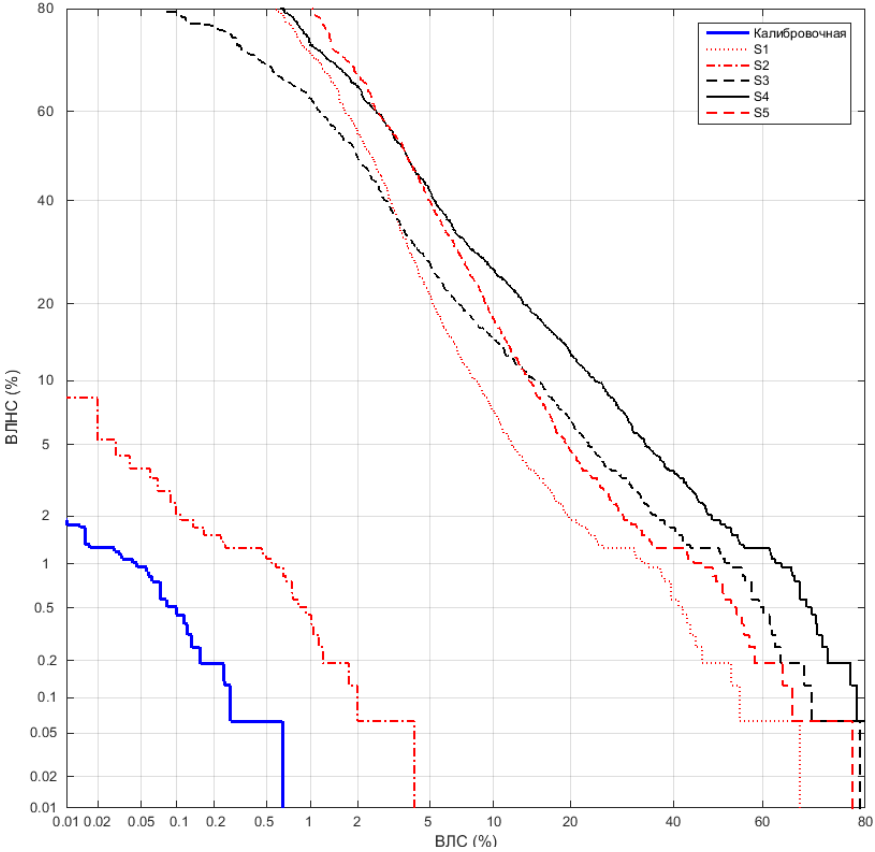


Рисунок 3 — Кривые КОО для системы верификации диктора при воздействии пяти методов атак на устройство ввода

Из результатов эксперимента видно, что методы спуфинг атак, основанные на технологии синтеза, значительно увеличивают ошибки системы. Необходимо также отметить, что атаки, основанные на технологии синтеза речи, в отличие от атак, основанных на технологии преобразования речи, не требуют участия нарушителя и могут быть полностью автоматизированы.

Предложен метод имитации спуфинг атаки, основанный на гибридном методе синтеза (гибрид методов выбора речевых

элементов и статистических моделей) и автоматической разметке на основе аллофонной сегментации и разметки периодов основного тона. Схема работы предложенного метода имитации спуфинг атаки изображена на рисунке 4. Проведена оценка влияния объема обучающих данных системы синтеза и качества их предварительной обработки на устойчивость текстозависимой системы верификации, использующей сценарий динамической парольной фразы. Подготовленная в рамках экспериментов тестовая речевая база данных описана и выложена в общий доступ.

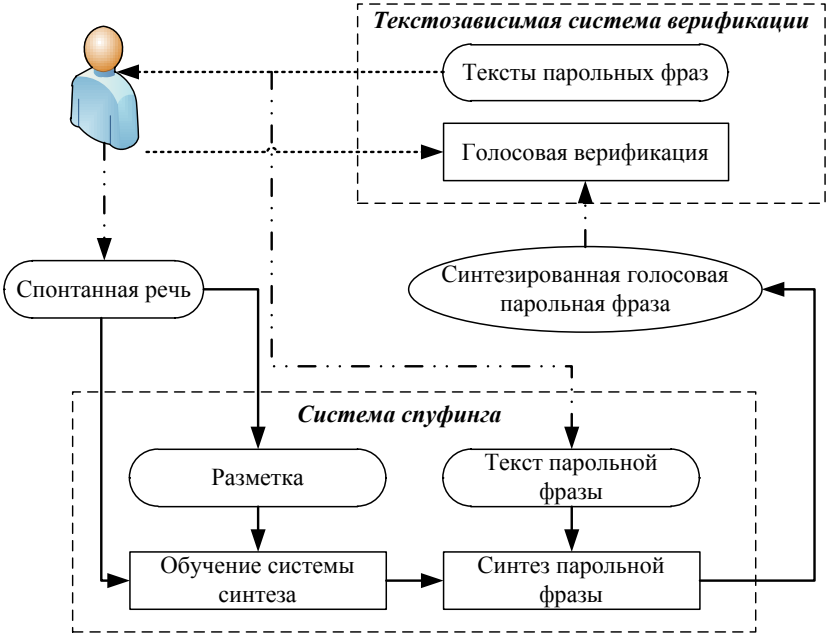


Рисунок 4 — Схема имитации спуфинг атаки на текстозависимую систему верификации с динамической парольной фразой

Результаты проведенного анализа показывают, что методы спуфинг атак на устройство ввода голосовой биометрической системы, основанные на технологии синтеза, представляют угрозу большую, чем аналогичные методы на базе технологии преобразования речи. При этом, несмотря на значительную редукцию вероятности успешной атаки при полной автоматизации процесса,

уровень надежности биометрической аутентификации требует дополнительных методов противодействия спуфинг атакам.

Третья глава диссертации описывает методику и комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами.

Предлагаемая методика включает испытания, соответствующие российским стандартам, с добавлением шагов, проверяющих устойчивость к возможным спуфинг атакам на систему. Методика состоит из следующих основных этапов:

1. Планирование испытаний в соответствии с ГОСТ Р ИСО/МЭК 19795-1-2007.
2. Расчет показателей эффективности аутентификации голосовой биометрической системы в соответствии с ГОСТ Р ИСО/МЭК 19795-2-2008, ГОСТ Р ИСО/МЭК ТО 19795-3-2009, ГОСТ Р ИСО/МЭК ТО 19795-4-2010, ГОСТ Р ИСО 9000-2011.
3. Имитация спуфинг атаки на голосовую биометрическую систему. Сбор и протоколирование результатов.

На втором этапе методики, в дополнение к указанным в стандарте ГОСТ Р ИСО-МЭК 19795-1-2007 “Эксплуатационные испытания и протоколы испытаний в биометрии. Ч1. Принципы и структура” численным показателям, предлагается вносить в протокол испытаний следующую информацию:

– Значение равновероятной ошибки пропуска-отклонения РВО (equal error rate, EER) равное значениям ВЛС (вероятность ложного совпадения, FAR) и ВЛНС (вероятность ложного несовпадения, FRR) при пороге, в котором их значения равны. Данный показатель выделяет основную значимую информацию из кривых КОО (компромиссного определения ошибки, DET curve) или РХ (рабочей характеристики, ROC curve).

– Графическое представление зависимости значений ВЛС и ВЛНС от порога принятия решения. В отличие от кривых КОО или РХ, не отображающих влияние порога принятия решения на ошибку биометрического сравнения, предлагаемое графическое представление наглядно показывает не только зависимость ВЛС и ВЛНС друг от друга, но и устойчивость системы к возможному колебанию порога принятия решения.

– Для систем идентификации на замкнутом множестве при построении кривой ХСС (характеристики совокупной схожести, CMC curve) рассчитывать значения вероятности истинно положительной идентификации ранга r при значениях ранга r относительно размера базы, в процентном отношении.

На третьем этапе методики в качестве численных показателей предлагается использовать значения ВЛСФ (вероятность ложного совпадения фальсифицированного образца).

$$\text{ВЛСФ}(\theta) = \frac{N_{target\ (error\ )}(\theta)}{N_{spoofing}} \cdot 100\%$$

где $N_{spoofing}$ - количество сравнений вида "свой–чужой" при применении методов фальсификации БХЧ;

$N_{target\ (error\ )}(\theta)$ - количество сравнений вида "свой–чужой" при применении методов фальсификации БХЧ, идентифицированных как "свой–свой", в зависимости от порога.

В качестве порога θ рекомендуется выбирать следующие значения, полученные на втором этапе методики:

– порог принятия решения в точке РВО;
– порог, соответствующий значению ВЛС меньшему или равному 0,01%.

Для графического представления результатов второго шага испытаний и их занесения в протокол предлагается строить кривые КОО системы под воздействием нескольких видов атак. Кривые строят, отображая ВЛСФ по абсциссе и ВЛНС по ординате. При сравнении полученных кривых с кривыми, полученными на предыдущем этапе методики, легко оценить степень устойчивости голосовой биометрической системы к спуфинг атакам. Чем ближе кривые друг к другу, тем надежнее система работает под воздействием атаки.

Комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами реализован с использованием языков программирования C++ и Python с обеспечением поддержки операционных систем Linux CentOS 6.1 и MS Windows 7 с архитектурой процессора x86 и x64.

Основными модулями комплекса программных средств оценки эффективности аутентификации голосовыми биометрическими системами являются:

- модуль сопряжения с голосовой биометрической системой;
- модуль формирования протоколов по тестовой речевой базе данных;
- модуль имитации спуфинг атаки на голосовую биометрическую систему;
- модуль тестирования голосовой биометрической системы;
- модуль расчета показателей эффективности аутентификации;
- модуль генерации протоколов испытаний.

В качестве основных достоинств разработанного комплекса программных средств следует отметить следующие функциональные возможности. Во-первых, возможность сопряжения с различными голосовыми биометрическими системами для проведения технологических испытаний. Во-вторых, применение инструментов модульного тестирования, обеспечивающее возможность легкой интеграции в существующие инфраструктуры разработки программных средств, возможность распараллеливания вычислений, а также применение стандартной формы протоколирования результатов. В-третьих, наличие легко расширяемого модуля имитации атаки, позволяющего оценивать устойчивость голосовой биометрической системы при воздействии различных методов спуфинг атаки.

Помимо этого, опыт практического внедрения показал, что при соответствующих доработках в модуле сопряжения и модуле расчета показателей эффективности данный комплекс программных средств может быть внедрен при проведении технологических испытаний или на этапе разработки таких систем, как: системы распознавания по изображению; системы автоматического распознавания речи; системы синтеза речи; системы шумоочистки; системы преобразования сигнала.

В **четвертой главе** представлен метод противодействия спуфинг атакам на устройство ввода голосовой биометрической системы.

Дано детальное описание метода детектирования спуфинг атак, основанного на TV-JFA подходе с использованием SVM классификатора с линейным ядром. Общая схема предложенного метода изображена на рисунке 5.

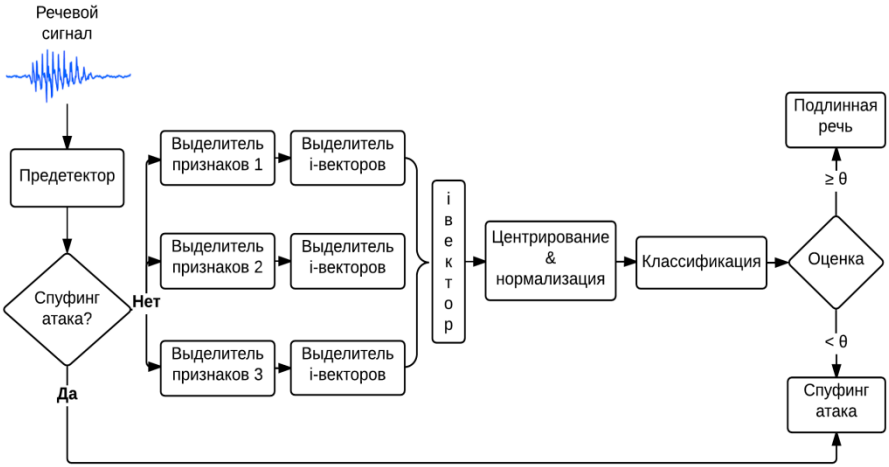


Рисунок 5 — Общая схема метода автоматического детектирования спуфинг атак

Предложенный детектор занял второе место на международном конкурсе Automatic Speaker Verification Spoofing and Countermeasures (ASVspoof) Challenge 2015 [10].

Для объединения результатов детектора с модулем принятия решения предлагается использовать следующую формулу:

$$P_{system} = P_{speaker} \cdot (1 - P_{spoofing})$$

где:

P_{system} - результат голосовой биометрической системы;

$P_{speaker}$ - вероятность того, что диктор в записи совпадает с зарегистрированным в системе шаблоном;

$P_{spoofing}$ - вероятность того, что запись содержит фальсифицированную речь.

Приведены результаты экспериментальной оценки эффективности аутентификации голосовой биометрической системой, включающей предложенный метод противодействия спуфинг атакам. Как видно из таблицы 1, предложенная методика позволяет учесть влияние спуфинг атак различных видов и корректно оценить эффективность аутентификации голосовой биометрической системой обладающей методом противодействия.

Таблица 1 — Численные показатели эффективности аутентификации TV-PLDA системой без предложенного детектора и с ним

Показатель	TV-PLDA	TV-PLDA + ASD
ВОР	0,00%	0,00%
ВОСД	0,00%	0,00%
ВЛС(50)	12,94%	10,60%
ВЛНС(50)	0,00%	0,00%
РВО	0,19%	0,57%
ВЛСФ(РВО)	51,29%	0,81%
ВЛСФ(ВЛС<0,01%)	44,98%	0,04%

Из полученных в таблице 1 значений ВЛСФ видно, что применение предложенного метода противодействия обеспечивает значительное повышение защищенности голосовой биометрической системы от атак, основанных на методах синтеза и преобразования индивидуальных голосовых биометрических характеристик.

В **заключении** подведены итоги диссертационного исследования, изложены его основные выводы и обобщающие результаты.

Заключение

Главный результат представленной работы заключается в исследовании и разработке методики оценки эффективности аутентификации голосовыми биометрическими системами, позволяющей комплексно оценивать различные голосовые биометрические системы и корректно их сравнивать с учетом возможных атак на устройство ввода биометрической информации.

Наряду с этим, в работе были получены следующие основные результаты:

1. Проведен анализ уязвимости современных голосовых биометрических систем к различным способам фальсификации индивидуальных голосовых биометрических характеристик человека. Показана необходимость совершенствования защиты модуля ввода биометрической информации от атак, использующих фальсификацию голосовых биометрических характеристик.

2. Разработан метод имитации атаки на устройство ввода биометрической информации, обеспечивающий автоматическое

создание модели голоса для синтеза голосовых биометрических характеристик. Проведен численный эксперимент, показывающий необходимость дополнения существующих стандартов оценки эффективности аутентификации голосовыми биометрическими системами, оценкой устойчивости к спуфинг атакам.

3. В соответствии со сделанными выводами, разработана методика оценки эффективности аутентификации голосовыми биометрическими системами, учитывающая воздействие различных видов спуфинг атак на модуль ввода биометрической информации. Проведены численные эксперименты, показывающие преимущества разработанной методики в сравнении с существующими аналогами.

4. На основе предложенной методики разработан комплекс программных средств оценки эффективности аутентификации голосовыми биометрическими системами, позволяющий оценивать устойчивость к различным видам атак при проведении технологических испытаний или на этапе разработки системы.

5. Разработан метод противодействия спуфинг атакам, позволяющий значительно повысить устойчивость голосовых биометрических систем к различным методам спуфинг атак на модуль ввода биометрической информации. Проведены численные эксперименты, показывающие значительную редукцию уровня ошибки распознавания диктора при воздействии атаки на модуль ввода. Разработанный метод детектирования спуфинг атак занял второе место на международном конкурсе ASVspoof Challenge 2015.

Работы, опубликованные автором по теме диссертации

В изданиях, рекомендованных ВАК при МОиН РФ:

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., 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, C. 132-137.

3. 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, C. 475–481.

4. 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, C. 3-9.

5. 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, C. 480-486.

6. 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, C. 137-143.

В других изданиях:

7. Манукянц В.Э., Щемелинин В.Л. Тестирование наукоемких SDK // Сборник тезисов XVI международной конференции по вопросам качества программного обеспечения SQA Days 16 - 2014. - С. 70.

8. Щемелинин В.Л. Оценка эффективности биометрических систем // Альманах научных работ молодых ученых Университета ИТМО. – СПб: Университет ИТМО, 2015. - Т. 3. - С. 250-254.

9. 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, C. 221-224.

10.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) .