

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.934

ЗЕЛЬМАНСКИЙ
Олег Борисович

**СИНТЕЗ РЕЧЕПОДОБНЫХ ПОМЕХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ
ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ**

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации,
информационная безопасность

Минск 2012

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Давыдов Андрей Геннадьевич, кандидат технических наук, старший научный сотрудник ООО «Речевые технологии»

Липницкий Станислав Феликсович, доктор технических наук, доцент, главный научный сотрудник ГНУ «Объединенный институт проблем информатики НАН Беларуси»

Борискевич Анатолий Антонович, кандидат технических наук, доцент, доцент кафедры сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Оппонирующая организация

Учреждение образования «Военная академия Республики Беларусь»

Защита состоится «20» сентября 2012 года в 14:00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп.1, ауд. 232, тел. (8-017) 293-89-89, e-mail 7650772@ Rambler.ru.

КРАТКОЕ ВВЕДЕНИЕ

Задача защиты информации от утечки по акустическим каналам занимает одно из главных мест в области безопасности ввиду того, что она является ключевым элементом в жизни современного мира и именно через нее реализуется значительная часть угроз. Наиболее важным в этом направлении представляется защита речевой информации, поскольку речь является для человека самой естественной формой взаимодействия.

Одним из подходов к решению данной задачи является маскировка разговора, которая состоит в создании маскирующего акустического шума по периметру защищаемого помещения или непосредственно в самом помещении. Анализ существующих на настоящий момент систем активной акустической маскировки выявил тот факт, что в большинстве систем в качестве маскирующего используется «белый» или «окрашенный» шум, при использовании которого уровень сигнала, необходимый для надежной защиты помещения, может превышать комфортный уровень, а иногда и допустимые санитарные нормы.

Исходя из вышеизложенного, можно сделать вывод о целесообразности усовершенствования систем активной акустической маскировки путем формирования новых видов речевых помех.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» в период с 2009 по 2012 г. в рамках:

– ГБЦ НИР № 11-3132 № ГР 20112037 по теме «Разработка программных модулей детектирования и сегментации речи» в период с 03.01.2011 по 31.12.2011 г. на основании гранта Министерства образования Республики Беларусь для аспирантов;

– ОКР «Доработать и подготовить к запуску в производство детектор речи для устройств защиты речевой информации типа «Прибой», систем аудиозаписей и систем связи», УДК 681.84/85, главный конструктор Г.В. Давыдов, х/д 10-1064, № ГР 20113150.

Тема диссертационной работы соответствует приоритетным направлениям фундаментальных и прикладных исследований Республики Беларусь в области

информационной и инженерно-технической безопасности, создания современных систем защиты информации.

Цель и задачи исследования

Целью диссертационной работы является синтез речеподобных помех для защиты переговоров на нескольких языках и создание на его основе многофункционального устройства защиты речевой информации от утечки по техническим каналам.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать существующие методы и средства защиты речевой информации, аппаратно-программные средства активной акустической маскировки, способы и устройства формирования речеподобных помех для систем защиты информации.

2. Провести синтез речеподобных помех для защиты переговоров одновременно на нескольких языках, основанный на компиляции участков записей речи дикторов, выделяемых непосредственно из их речи.

3. Разработать способ детектирования речи, основанный на сравнении классификационных параметров сигнала с их пороговыми значениями, позволяющий обнаружить наличие речи в сигнале при отношении уровня сигнала к уровню шума не менее 40 дБ, и реализовать его в виде модуля детектирования речи для определения моментов начала переговоров с целью запуска синтеза речеподобных помех.

4. Обосновать выбор методики сегментации речи на фонетические единицы, используемой в качестве основы для разработки модуля сегментации речи; методики классификации выделенных фонетических единиц, используемой в качестве основы для разработки модуля классификации речи; методики компиляции участков записей речи дикторов для синтеза речеподобных помех, используемой в качестве основы для разработки модуля синтеза речи.

5. Разработать генератор речеподобных помех для защиты переговоров на разных языках с подстройкой характеристик помехи к голосу диктора, состоящий из модулей детектирования, сегментации, классификации и синтеза речи, а также модернизировать устройство защиты информации серии «Прибой» введением в его структуру многофункционального генератора речеподобных помех.

В качестве объекта исследования выбраны устройства и системы активной акустической маскировки. Предметом исследования являются алгоритмы

анализа и синтеза речи, обеспечивающие формирование речеподобных помех с целью маскирования речевой информации.

Положения, выносимые на защиту

1. Синтез речеподобных помех для защиты информации от утечки по акустическим каналам, базирующийся на компиляции участков записей речи дикторов на разных языках по формируемому с учетом статистических особенностей языков фонемному тексту, применении верификации речи для определения моментов смены голосов дикторов, сегментации и классификации речи для подстройки характеристик помехи к голосу диктора, что позволяет снизить вероятность обнаружения и выделения речевой информации средствами ее перехвата.

2. Способ детектирования речевого сигнала для синтеза речеподобных помех, основанный на изменении режимов буферизации аудиосигнала, совместной оценке параметров мощности, среднего количества переходов через нуль, отклонения распределения спектральной плотности мощности от оценки спектральной плотности мощности шума и их классификации, что позволяет выделять и записывать речевые участки аудиосигнала, при этом частота ложных срабатываний снизилась до 19,6 %, а частота пропуска речевых участков – до 14,9 %.

3. Алгоритм формирования баз аллофонов непосредственно из речи разноязычных участников переговоров для синтеза речеподобных помех, заключающийся в сегментации речи, обнаруженной в ходе детектирования, на фонетические единицы и их аллофонной классификации по критерию минимума расстояния, характеризующийся относительной точностью обнаружения границ фонем до 98 %, количеством лишних границ до 17,5 %, количеством обнаруживаемых границ до 72 %, что позволило предложить устройство формирования баз аллофонов разноязычных дикторов.

Личный вклад соискателя

Содержание диссертационной работы отражает личный вклад автора. Основные научные и практические результаты работы, а также положения, выносимые на защиту, получены лично автором.

В совместно опубликованных работах автору принадлежат: синтез речеподобных помех непосредственно из речи разноязычных участников переговоров, алгоритм формирования баз аллофонов из речи дикторов, способ детектирования речи, исследование частоты употребления букв арабского

алфавита, разработка модулей детектирования, сегментации, классификации речи, верификации диктора по голосу, устройства пассивной защиты информации от утечки по средствам связи, системы синтеза речеподобных помех.

Соавторами основных публикаций являются научный руководитель, канд. техн. наук, ст. науч. сотр. А. Г. Давыдов, который осуществлял определение целей и постановку задач исследования, выбор методов исследований, принимал участие в планировании работ и обсуждении результатов, а также д-р техн. наук, проф. Л. М. Лыньков, который осуществлял интерпретацию и обобщение полученных результатов, научное редактирование материалов монографии.

Апробация результатов диссертации

Основные положения и результаты, изложенные в диссертационной работе, докладывались и обсуждались на VI, VII, VIII, IX и X Белорусско-российских научно-технических конференциях «Технические средства защиты информации» (Минск, 2008, 2009, 2010, 2011, 2012 гг.), V Международной научной конференции по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения «МИЛЕКС 2011» (Минск, 2011 г.), XII, XIII, XIV и XV Международных научно-технических конференциях «Современные средства связи» (Минск, 2008, 2009, 2010, 2011 гг.), Международной научно-технической конференции, посвященной 45-летию МРТИ – БГУИР (Минск, 2009 г.), VIII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2011г.), V и VI Международных конференциях-форумах «Информационные системы и технологии (IST'2009, 2010)», (Минск, 2009, 2010 гг.), Международном научно-техническом семинаре «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных» (Браслав, 2010 г.), II Международной научно-практической молодежной конференции «Научные стремления» (Минск, 2011 г.), 4-й Международной специализированной выставке «Человек и безопасность» (Минск, 2010 г.), слете молодых ученых и преподавателей, посвященном дню белорусской науки (Минск, 2011 г.).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 42 работы, в том числе 1 монография, 6 статей в научных

журналах, 10 статей в сборниках материалов научных конференций, 16 тезисов докладов, 1 отчет об ОКР, 1 отчет о НИР. Получен 1 патент Республики Беларусь на изобретение и 6 патентов Республики Беларусь на полезные модели. Общий объем опубликованных работ по теме диссертации составляет 15,8 авторских листов.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе проведен анализ существующих методов и средств защиты речевой информации, приведено обоснование выбора речеподобных помех для маскирования речевой информации и рассмотрены их основные особенности. Дано описание методов детектирования, сегментации и классификации речи, выполнен их сравнительный анализ.

Во второй главе приведено обоснование синтеза речеподобных помех по фонемному тексту. Предложен синтез речеподобных помех для защиты переговоров одновременно на нескольких языках путем компиляции участков записей речи дикторов на разных языках. Предложен алгоритм формирования баз аллофонов дикторов на основе детектирования, сегментации и классификации речи.

В третьей главе содержится описание реализации предложенного синтеза речеподобных помех в виде системы синтеза речеподобных помех для защиты переговоров на разных языках, состоящей из разработанных модулей детектирования, сегментации, классификации и синтеза речи. Приведено описание данных модулей и результаты их тестирования. Предложен способ детектирования речи.

В четвертой главе содержится описание и результаты модификации устройства защиты речевой информации «Прибой» путем введения в его состав разработанной системы синтеза речеподобных помех непосредственно из русской, арабской и английской речи. Приведена его структура и принципы работы. Даны рекомендации по его эксплуатации.

В приложениях представлены исходные тексты программной реализации модулей детектирования, сегментации и классификации речи, а также акты внедрения результатов научно-исследовательской работы в практику НИЛ 5.3 и учебный процесс учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Общий объем диссертационной работы составляет 185 страниц, из них 98 страниц текста, 40 рисунков на 25 страницах, 23 таблицы на 16 страницах, 2 приложения на 30 страницах, библиография из 166 источников на 16 страницах, включая список из 42 собственных публикаций автора на 6 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Первая глава посвящена рассмотрению активной защиты речевой информации, заключающейся в формировании маскирующих шумовых помех с целью снижения отношения уровня сигнала к уровню шума в местах возможного нахождения средств перехвата информации путем увеличения уровня шума. Это позволяет уменьшить разборчивость речи и тем самым затруднить ее перехват.

В состав аппаратуры акустической маскировки входят генераторы шума. Наиболее эффективным для защиты речевой информации является использование речеподобных помех в качестве маскирующих шумов, поскольку позволяет защитить речевую информацию от большинства способов ее перехвата благодаря тому, что речеподобные помехи наиболее подобны реальным речевым сигналам не только по временным и спектральным характеристикам, но и по восприятию на слух. При этом уровень речеподобной помехи, необходимый для защиты помещения, ниже уровня «белого» и «окрашенного» шума, необходимого для обеспечения такого же результата.

Проанализированы методы обнаружения речи в сигнале. Наиболее рациональным, совмещающим эффективность и компактность вычислений, является метод сравнения классификационных параметров сигнала с пороговыми значениями, при этом для определения порога целесообразно применить метод минимума статистики. Обнаружение речи в сигнале позволяет выделять из него все речевые участки для использования при синтезе речеподобных помех.

Рассмотрены подходы к сегментации речи. Достаточно высокой точностью характеризуются системы сегментации речи, основанные на анализе функции изменения спектра, которая определяется исходя из расстояния между параметрическими векторами, описывающими фреймы речевого сигнала. По средствам сегментации речи осуществляется разделение речевых сигналов на аллофоны, из которых синтезируются речеподобные помехи.

Проведен обзор подробной классификации звуков русской речи. Классификация речи в реальном времени с помощью современных методов требует больших вычислительных ресурсов, объем которых часто бывает

ограничен. Невозможность широкого применения многих алгоритмов в невысокопроизводительных мобильных устройствах обуславливает необходимость в разработке модуля классификации речи, реализующего эффективный и оптимизированный алгоритм с целью классификации применяемых для синтеза речеподобных помех аллофонов.

Проанализированы основные особенности речевых сигналов. Наиболее приемлемой формулировкой речеподобной помехи является «синтезируемый по случайному закону акустический сигнал, который по своим основным характеристикам соответствует речевому сигналу, но не содержит смысловой информации».

На основе результатов анализа литературных источников показано, что необходимый для надежной защиты помещения уровень «белого» или «окрашенного» шума может превышать комфортный уровень, а иногда и допустимые санитарные нормы, а формирование речеподобных помех в существующих системах защиты информации осуществляется в большей степени на основе интуитивных принципов. Таким образом, обоснована необходимость разработки синтеза речеподобных помех непосредственно из речи участников переговоров на основе ее верификации, сегментации и классификации для защиты произнесенной на разных языках речевой информации от утечки по техническим каналам.

Во **второй** главе проанализированы методы синтеза речи. Установлено, что для синтеза речеподобных помех следует использовать аллофонную модель синтезатора речи по фонемному тексту с целью компиляции отрезков естественной речевой волны дикторов в речеподобные помехи.

Разработан синтез речеподобных помех, основанный на компиляции участков записей речи дикторов на разных языках по формируемому с учетом статистических особенностей языков фонемному тексту. Предложенный синтез включает верификацию речи для определения моментов смены голосов дикторов, сегментацию и классификацию речи для подстройки характеристик помехи к голосу диктора (рисунок 1).

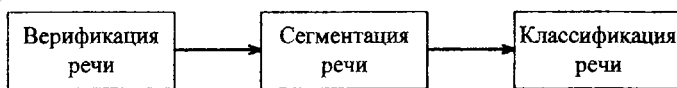


Рисунок 1 – Схема синтеза речеподобных помех

Синтез речеподобных помех обеспечивает защиту переговоров на разных языках как с использованием заранее сформированных баз аллофонов, так и непосредственно из речи участников разговора, или с использованием заранее

сформированных баз аллофонов с одновременным подмешиванием речеподобной помехи, которая формируется непосредственно из речи участников переговоров.

Составлены базы аллофонов дикторов на русском, арабском и английском языках путем сопоставления сегментированных на фонемы текстов с результатами временного и спектрального анализа аудиозаписей этих текстов (рисунок 2). Для формирования баз аллофонов использовались аудиозаписи с речью дикторов, которые являются носителями русского, арабского и английского языков. Запись речи производилась с использованием аппаратуры для акустических измерений производства RFT с линейной частотной характеристикой в диапазоне 20 Гц – 10 кГц и персонального компьютера с установленной программной средой Sound Forge 9.0 в акустически заглушенной комнате.

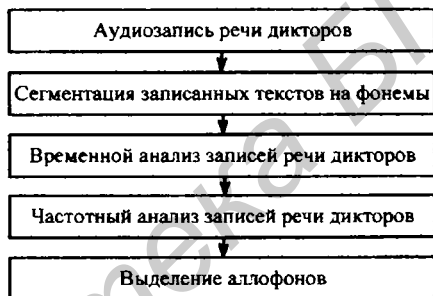


Рисунок 2 – Методика составления баз аллофонов дикторов

Разработан алгоритм автоматического формирования баз аллофонов непосредственно из речи разноязычных участников переговоров для синтеза речеподобных помех, заключающийся в сегментации речи, обнаруженной в ходе детектирования, на фонетические единицы и их аллофонной классификации по критерию минимума расстояния.

Третья глава посвящена разработке системы синтеза речеподобных помех. Функционирование предлагаемой системы включает в себя следующее: обнаружение речи, верификацию диктора по его речи с целью загрузки ранее сформированной базы аллофонов, выделенных из его речи, сегментацию обнаруженного речевого сигнала на фонетические единицы, их классификацию на соответствующие фонемы и озвучивание с помощью аллофонов. Структура разработанной системы (рисунок 3) включает разработанные модули детектирования, сегментации, классификации речи, обозначенные на рисунке пунктиром, а также верификации диктора по голосу и синтеза речи.

Система выполняет формирование речеподобных помех по случайному закону и по своим спектральным и временным характеристикам, а также восприятно на слух, максимально похожих на речевые сигналы, но не несущих при этом никакой смысловой нагрузки.

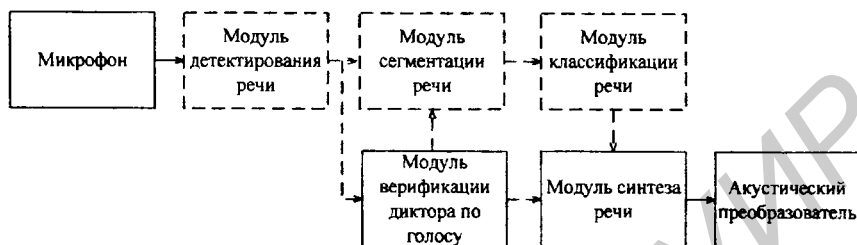


Рисунок 3 – Структурная схема системы синтеза речеподобных помех

Разработан способ детектирования речи, основанный на совместном сравнении таких классификационных параметров сигнала, как кратковременное среднеквадратичное значение сигнала, кратковременная функция среднего числа переходов сигнала через нуль и спектральная оценка сигнала, с их пороговыми значениями, что позволяет выделять и записывать речевые участки аудиосигнала, при этом частота ложных срабатываний снизилась до 19,6 %, а частота пропуска речевых участков – до 14,9 %.

Для расчета среднеквадратичного значения сигнала (RMS) применяется следующая формула:

$$RMS = \sqrt{\frac{1}{N} \sum_{n=0}^{N-1} |x(n)|^2}, \quad (1)$$

где N – число временных отсчетов окна анализа;
 $x(n)$ – n -й временной отсчет входного сигнала.

Функция среднего числа переходов сигнала через нуль имеет вид:

$$Z_n = \frac{1}{N} \sum_{n=0}^{N-1} |\text{sgn}[x(n)] - \text{sgn}[x(n-1)]|, \quad (2)$$

где

$$\text{sgn}[x(n)] = \begin{cases} 1, & x(n) \geq 0, \\ -1, & x(n) < 0. \end{cases} \quad (3)$$

На рисунке 4 приведена блок-схема алгоритма детектирования речи во временной области. Структурная схема программного модуля детектирования речи представлена на рисунке 5.

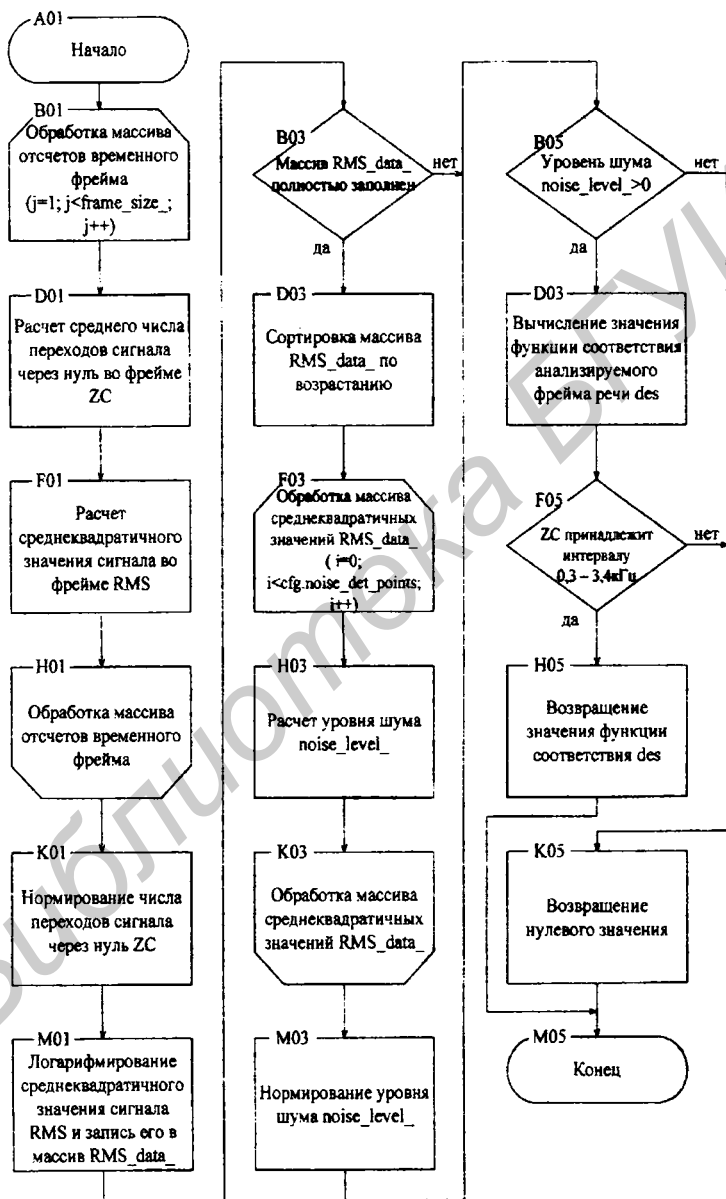


Рисунок 4 – Блок-схема алгоритма детектирования речи

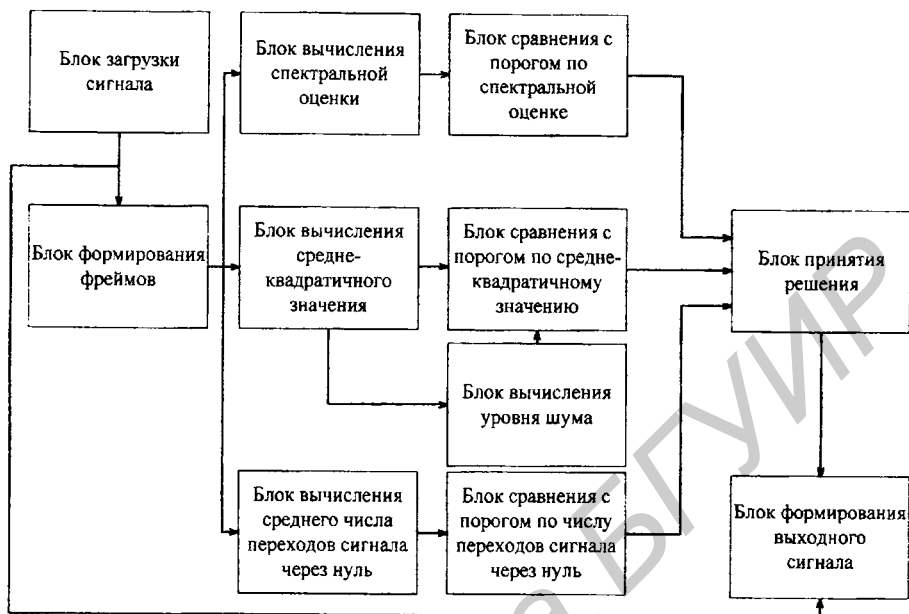


Рисунок 5 – Структурная схема модуля детектирования речи

Предложен программный модуль сегментации речи на фонетические единицы. В основу данного модуля положен анализ функции изменения спектра сигнала, рассчитываемой исходя из расстояния между векторами линейных спектральных частот. В качестве расстояния использовано расстояние Минковского с метрикой, равной четырем, поскольку согласно результатам проведенных исследований (таблица 1) применение этого расстояния совместно с таким параметром сигнала, как линейные спектральные частоты, обеспечивает наиболее оптимальное соотношение между количеством лишних границ, пропущенных границ и точностью их обнаружения, определяемое по следующей формуле:

$$F = -m_1 - m_2 + m_3, \quad (4)$$

где m_1, m_2, m_3 – количество лишних границ, пропущенных границ и точность обнаружения границ соответственно.

Показано, что относительная точность обнаружения границ фонем данным модулем сегментации речи составляет до 98 %, при этом количество лишних границ – до 17,5 %, количество обнаруживаемых границ – до 72 %.

Таблица 1 – Критерии оценки использования метрик при сегментации речи

Критерий	Метрика							
	Евклидово расстояние	Нормированное евклидово расстояние	Расстояние Махаланобиса	Расстояние «городских квадратов»	Косинусное расстояние	Корреляционное расстояние	Расстояние Минковского с метрикой 3	Расстояние Минковского с метрикой 4
Количество лишних границ, %	18,2	16,8	21,8	18,8	20,9	22,9	18,1	17,5
Количество пропущенных границ, %	30,9	31,0	33,9	32,5	35,2	35,9	31,3	27,9
Точность обнаружения границ, %	98,6	98,9	98,7	99,0	98,9	98,7	98,8	98,7
Обобщенный критерий, %	49,5	51,1	43	47,7	42,8	39,9	49,4	53,3

Разработан модуль классификации фонетических единиц на фонемы, реализующий алгоритм, заключающийся в нахождении минимума расстояния между кепстрами анализируемой фонетической единицы и базы образцов. Показано, что модуль классификации речи позволяет определить, к какой группе фонем относится анализируемая фонетическая единица и, кроме того, какой фонеме она соответствует в большей степени. Например, согласно таблице 2, классифицируемая предложенным модулем фонетическая единица, представленная фонемой [а] длительностью 95 мс, может быть отнесена к группе гласных и наиболее коррелирует с фонемой [а] русского языка.

Таблица 2 – Коэффициенты различия для фонемы [а] русского языка

Образец фонемы	Длительность фонемы, мс	Коэффициент различия	Образец фонемы	Длительность фонемы, мс	Коэффициент различия
Гласные			Шумные согласные глухие		
а	98	1,8404	п	30	4,6759
о	105	4,2761	т	25	3,345
и	101	10,3144	к	56	1,939
ы	151	7,3202	ф	164	5,8501
у	136	5,8366	с	181	11,7766
э	136	2,1971	ш	113	9,0782
Шумные согласные звонкие			щ	200	18,0396
			х	155	6,8726
б	111	6,8718	ц	97	4,1811
д	127	8,2736	Соворные согласные		
г	102	7,3062	л	67	4,2038
в	136	10,5866	м	108	8,2211
з	125	8,4564	р	68	3,2072
ж	131	8,9914	н	87	6,8219

Проведен анализ статистических характеристик различных элементов речи, формируемых пауз, распределения вероятности длин слова и положения ударений в слове на примере русской, арабской и английской речи. Таблица 3 содержит статистические закономерности количества слогов в слове для русского, арабского и английского языков.

На основе аллофонной модели синтеза речи по фонемному тексту, формируемому с учетом статистических особенностей языка, разработан модуль синтеза речи.

Таблица 3 – Распределение вероятности длины слова русского, арабского и английского языков

Вероятность появления	Число слогов в слове								
	1	2	3	4	5	6	7	8	9
Для русского языка, %	16,31	36,67	25,52	13,60	5,16	1,40	0,29	0,034	0,004
Для арабского языка, %	31,63	42,75	19,82	4,87	-	-	-	-	-
Для английского языка, %	71,52	19,40	6,80	1,60	0,56	0,12	-	-	-

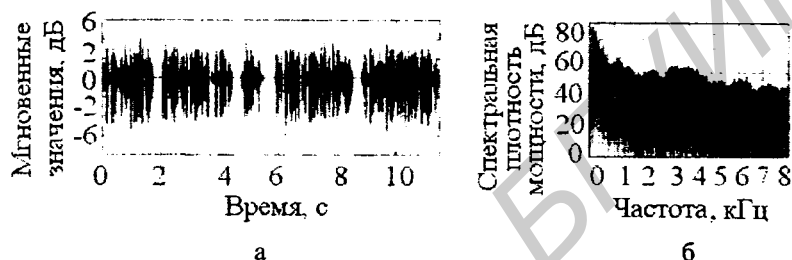
Таким образом, предложенный синтез речеподобных помех реализован в системе защиты речевой информации от утечки по акустическим каналам с подстройкой характеристик помехи к голосу диктора. Показано, что система может быть легко адаптирована с целью синтеза речеподобных помех для защиты переговоров на любом языке путем добавления базы статистических закономерностей требуемого языка.

В четвертой главе рассмотрены структура, принцип действия и условия эксплуатации усовершенствованного устройства защиты речевой информации «Прибой-РМ» на разных языках. Показано, что генератор речеподобных помех со встроенным управляемым усилителем, входящий в его состав, содержит базы русского, арабского и английского языков, блок формирования фонемного текста, блок компиляции аллофонов, управляемый усилитель, устройство управления, блок детектирования речи, блок сегментации речи, блок классификации речи, блок верификации диктора по голосу, базу аллофонов дикторов и обеспечивает формирование речеподобных помех путем озвучивания фонемного текста, генерируемого с учетом статистики.

Усовершенствованное устройство «Прибой-РМ» позволяет генерировать речеподобные помехи для защиты русской, арабской и английской речи, а также разговора одновременно на двух или трех языках с использованием заранее выделенных аллофонов произвольных дикторов; аллофонов, выделяемых непосредственно из речи участников переговоров, или

одновременно из заранее выделенных аллофонов и выделяемых непосредственно из речи участников переговоров. Пример временной реализации фразы, синтезированной с помощью устройства «Прибой-РМ» на русском языке, и ее спектральная плотность мощности приведены на рисунке 6.

Установлено, что устройство «Прибой-РМ» позволяет защитить речевую информацию, произнесенную на разных языках, от утечки по техническим каналам по средствам синтеза речеподобных помех с подстройкой их характеристик к голосу диктора.



а – временная реализация; б – спектральная плотность мощности

Рисунок 6 – Временная реализация и спектральная плотность мощности синтезированной речеподобной помехи

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложен синтез маскирующих речеподобных помех, которые по своим основным характеристикам соответствует речевым сигналам, но не содержат смысловой информации и позволяют существенно затруднить перехват речевой информации [4–А, 21–А, 27–А]. В основу синтеза положена аллофонная модель компиляции участков записей речи дикторов по формируемому с учетом статистических особенностей языка [6–А] фонемному тексту, верификация речи для определения моментов смены голосов дикторов, сегментации и классификации речи для подстройки характеристик помехи к голосу диктора. Предложенный синтез обеспечивает формирование речеподобных помех для защиты переговоров на разных языках как с использованием заранее сформированных баз аллофонов произвольных дикторов, так и непосредственно из речи участников разговора, или с использованием заранее сформированных баз аллофонов с одновременным подмешиванием речеподобной помехи, которая формируется непосредственно из речи участников переговоров [1–А, 7–А, 15–А, 31–А].

2. Разработан алгоритм формирования баз аллофонов непосредственно из речи разноязычных участников переговоров для синтеза речеподобных помех, заключающийся в сегментации речи, обнаруженной в ходе детектирования, на фонетические единицы и их аллофонной классификации по критерию минимума расстояния [1-А, 7-А].

3. Разработана система синтеза речеподобных помех для защиты переговоров на разных языках (русском, арабском и английском), реализующая алгоритм синтеза речеподобных помех, а также предложенный алгоритм автоматического формирования баз аллофонов непосредственно из речи разноязычных участников переговоров [1-А, 7-А]. В соответствии с данными алгоритмами структура разработанной системы включает разработанные модули детектирования, сегментации и классификации речи, а также верификации диктора по голосу и синтеза речи. Система выполняет формирование речеподобных помех для защиты переговоров на разных языках или одновременно на нескольких языках по случайному закону, и по своим спектральным и временным характеристикам, а также восприятию на слух, максимально похожих на речевые сигналы, но не несущих при этом никакой смысловой нагрузки [3-А, 8-А, 9-А, 10-А, 11-А, 16-А, 17-А, 22-А, 25-А, 26-А, 28-А].

4. Разработан способ и программный модуль детектирования речи для синтеза речеподобных помех, основанный на совместной оценке параметров мощности, среднего количества переходов через нуль, отклонения распределения спектральной плотности мощности от оценки спектральной плотности мощности шума и их классификации, при этом частота ложных срабатываний снизилась до 19,6 %, а частота пропуска речевых участков – до 14,9 % [2-А, 18-А, 19-А, 20-А, 23-А, 34-А, 42-А].

5. Предложен программный модуль сегментации речи на фонетические единицы для синтеза речеподобных помех на основе анализа функции изменения спектра сигнала, рассчитываемой исходя из расстояния между векторами линейных спектральных частот (расстояние Минковского с метрикой, равной четырем). Показано, что относительная точность обнаружения границ фонем данным модулем составляет до 98 %, при этом количество лишних границ – до 17,5 %, количество обнаруживаемых границ – до 72 % [5-А, 12-А, 14-А, 24-А, 29-А, 30-А, 42-А].

6. Разработан программный модуль классификации фонетических единиц на фонемы, основанный на критерии минимума расстояния между кепстрадами анализируемой фонетической единицы и базы образцов. Показано, что модуль классификации речи позволяет определить, к какой группе фонем относится

анализируемая фонетическая единица и, кроме того, какой фонеме она соответствует в большей степени [7-А, 13-А, 32-А, 33-А].

Рекомендации по практическому использованию результатов

1. Проведен анализ статистических характеристик различных элементов русской речи, формируемых пауз, распределения вероятности длин слова и положения ударений в слове. На основе аллофонной модели синтеза речи по фонемному тексту разработан модуль синтеза речи. Показано, что в задачи данного модуля входит преобразование в акустические колебания звукового диапазона частот генерируемого фонемного текста, соответствующего статистическим закономерностям языка [1-А, 6-А].

2. Разработан модуль детектирования речи, осуществляющий обнаружение и выделение речевых участков из аудиосигнала. Данный модуль может быть использован как самостоятельно, так и в составе систем с голосовым управлением, систем с биометрическим контролем доступа, систем кодирования и распознавания речи, систем повышения качества речи, систем передачи речевых сигналов, систем прослушивания, систем маскирования речи [34-А, 41-А].

3. Разработано устройство автоматического распознавания диктора по речи. Данное устройство может применяться для контроля и ограничения несанкционированного доступа к материальным и информационным ресурсам, а также для обеспечения удаленного распознавания пользователей на основе биометрических параметров в телекоммуникационных системах [35-А, 36-А].

4. Разработано устройство анализа речи, позволяющее осуществлять сегментацию речевого сигнала на квазистационарные участки, соответствующие фонетическим единицам, и последующую их классификацию. Данное устройство включает модули сегментации и классификации речи и может использоваться самостоятельно или в качестве модуля в системах распознавания и синтеза речи [39-А].

5. Разработано устройство синтеза речеподобных помех для защиты речевой информации на разных языках от утечки по акустическим каналам [40-А], позволяющее существенно затруднить ее перехват. Речеподобные помехи синтезируются как на основе заранее сформированных баз аллофонов произвольных дикторов, так непосредственно из речи участников переговоров. Показано, что данное устройство может быть легко адаптировано для синтеза помех на любом языке путем добавления базы статистических закономерностей требуемого языка. Разработанное устройство может быть использовано для защиты международных переговоров на разных языках [37-А, 38-А].

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Монографии

1—А. Активные и пассивные методы и средства защиты информации от утечки по техническим каналам : моногр. / М.О. Аль-Хатми, О.Б. Зельманский, Л.М. Лыньков, С.Н. Петров ; под ред. Л.М. Лынькова. – Минск : Бестпринт, 2011. – 275 с.

Статьи в научных журналах

2—А. Зельманский, О.Б. Построение программного модуля детектирования речи на основе классификационных параметров аудиосигнала / О.Б. Зельманский // Доклады БГУИР. – 2008. – № 7 (37). – С. 72–76.

3—А. Зельманский, О.Б. Программные средства текстозависимой верификации диктора по голосу / О.Б. Зельманский // Доклады БГУИР. – 2009. – № 4 (42). – С. 37–41.

4—А. Методика оценки снижения разборчивости речи конструкциями для средств защиты информации / О.Б. Зельманский, И.С. Худолей, А.М. Прудник, Л.М. Лыньков, С.Н. Петров // Вестн. Воен. акад. Респ. Беларусь. – 2010. – № 2 (27). – С. 153–157.

5—А. Зельманский, О.Б. Построение программного модуля сегментации речи на основе анализа изменения спектра / О.Б. Зельманский, А.Г. Давыдов // Безопасность информационных технологий. – 2011. – № 3. – С. 127–133.

6—А. Зельманский, О.Б. Исследование частоты употребления букв арабского алфавита и слов арабского языка для систем синтеза речеподобных сигналов / О.Б. Зельманский, А.Г. Давыдов // Вестник компьютерных и информационных технологий. – 2012. – № 2 (92). – С. 20–23.

7—А. Зельманский, О.Б. Методика синтеза речеподобных сигналов на разных языках для систем защиты информации / О.Б. Зельманский // Информационные системы и технологии. – 2012. – № 4 (72). – С. 122–131.

Статьи в материалах научных конференций

8—А. Зельманский, О.Б. Использование речевой информации для биометрической верификации личности / О.Б. Зельманский // Комплексная защита информации: материалы XIV Междунар. конф., Могилев, 19–22 мая 2009 г. / Белорус.-Российск. ун-т ; редкол.: А.П. Леонов [и др.]. – Могилев, 2009. – С. 107–108.

9—А. Зельманский, О.Б. Программный модуль верификации пользователя по голосу: вопросы надежности и качества / О.Б. Зельманский // Информационные системы и технологии (IST'2009) : материалы V междунар. конф.-форума, Минск, 16–17 нояб. 2009 г. / Науч.-технол. ассоциация «Инфопарк»; редкол.: Н.И. Листопад [и др.]. – Минск, 2009. – С. 255.

10—А. Зельманский, О.Б. Система генерирования речеподобных сигналов для маскирования акустической информации / О.Б. Зельманский, А.Г. Давыдов // СВЧ-техника и телекоммуникационные технологии : материалы 20-й Междунар. Крымской конф., Севастополь, Крым, Украина, 13–17 сент. 2010 г. / СевНТУ, КНТЦ им. Попова; редкол.: П.П. Ермолов [и др.]. – Севастополь, 2010. – С. 506–507.

11—А. Зельманский, О.Б. Устройство автоматического распознавания диктора по речи / О.Б. Зельманский, А.Г. Давыдов, Аль-Хатми Моххамед Омар // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы Междунар. науч.-техн. семинара, Браслав, 20–24 сент. 2010 г. / БГУИР; редкол.: В.К. Конопелько, Е.Г. Макейчик, О.Р. Сушко. – Минск, 2010. – С. 84–86.

12—А. Зельманский, О.Б. Параметризация речевого сигнала в системах сегментации речи / О.Б. Зельманский, А.Г. Давыдов // Информационные системы и технологии (IST'2010): материалы VI междунар. конф., Минск, 24–25 нояб. 2010 г. / Науч.-технол. ассоциация «Инфопарк»; редкол.: А.Н. Курбацкий [и др.]. – Минск, 2010. – С. 163–166.

13—А. Зельманский, О.Б. Анализ методов оценки периода основного тона речевого сигнала / О.Б. Зельманский, Аль-Хатми Моххамед Омар // Управление информационными ресурсами: материалы VIII междунар. науч.-практ. конф., Минск, 10 февр. 2011 г. / Акад. управления при Президенте Респ. Беларусь; редкол.: А.В. Ивановский [и др.]. – Минск, 2011. – С. 156–158.

14—А. Зельманский, О.Б. Модуль сегментации речи для систем синтеза речеподобных сигналов / О.Б. Зельманский, А.Г. Давыдов // Milex 2011 : материалы 5-й Междунар. науч. конф., Минск, 25–26 мая 2011 г. / ГУ «БелИСА»; редкол.: В.Е. Кратенок [и др.]. – Минск, 2011. – С. 248–250.

15—А. Synthesis of speechlike signals for masking acoustic information / O.B. Zelmanski, A. Ganiyev, A. Kubankova, P. Munster // WOFEX 2011 : proceedings of the 9th annual workshop, Ostrava, 8–9 Sept. 2011 y. / Technical university of Ostrava; editors : Michal Kratky, Jiri Dvorsky, Pavel Moravec. – Ostrava, 2011. – P. 609–613.

16—А. Зельманский, О.Б. Синтезатор речеподобных сигналов с биометрической верификацией диктора / О.Б. Зельманский, А.Г. Давыдов //

СВЧ-техника и телекоммуникационные технологии : материалы 21-й Междунар. Крымской конф., Севастополь, Крым, Украина, 12–16 сент. 2011 г. / СевНТУ, КНТЦ им. Попова ; редкол.: П.П. Ермолов [и др.]. – Севастополь, 2011. – С. 517–518.

17–А. Зельманский, О.Б. Система активной защиты акустической информации / О.Б. Зельманский // Научные стремления : материалы II Междунар. науч.-практ. конф., Минск, 14–18 нояб. 2011 г. / Совет молодых ученых Национальной академии наук Беларуси ; редкол.: А.Н. Волченко [и др.]. – Минск, 2011. – С. 724–727.

Тезисы докладов

18–А. Зельманский, О.Б. Детектирование речи / О.Б. Зельманский // Технические средства защиты информации: материалы VI Белорус.-российск. науч.-техн. конф., Минск, 21–22 мая 2008 г. / БГУИР ; редкол.: В.Ф. Голиков [и др.]. – Минск, 2008. – С. 11.

19–А. Зельманский, О.Б. Особенности использования детекторов речи в системах обработки речевой информации / О.Б. Зельманский // Современные средства связи: материалы XII Междунар. науч.-техн. конф., Минск, 7–9 окт. 2008 г. / ВГКС ; редкол.: М.А. Баркун [и др.]. – Минск, 2008. – С. 145.

20–А. Зельманский, О.Б. Анализ современных способов детектирования речи / О.Б. Зельманский // Междунар. науч.-техн. конф., посвящ. 45-летию МРТИ–БГУИР : тез. докл. Междунар. науч.-техн. конф., Минск, 19 марта 2009 г. / БГУИР ; редкол.: М.П. Батура [и др.]. – Минск, 2009. – С. 29.

21–А. Классификация угроз безопасности в информационных объектах / О.Б. Зельманский, В.И. Пачинин, Г.А. Пухир, Г.В. Сечко // Информационные системы и технологии : материалы XV Междунар. науч.-техн. конф., Н. Новгород, 17 апр. 2009 г. / Нижегород. гос. техн. ун-т им. Р.Е. Алексеева ; редкол.: В.Г. Баранов [и др.]. – Н. Новгород, 2009. – С. 96–97.

22–А. Зельманский, О.Б. Программное средство верификации диктора по голосу: системное проектирование / О.Б. Зельманский // Технические средства защиты информации: материалы VII Белорус.-российск. науч.-техн. конф., Минск, 23–24 июня 2009 г. / БГУИР ; редкол.: Л.М. Лыньков [и др.]. – Минск, 2009. – С. 40.

23–А. Зельманский, О.Б. Автоматическая верификация диктора по голосу с предварительным детектированием речи / О.Б. Зельманский // Современные средства связи: материалы XIV Междунар. науч.-техн. конф., Минск, 29 сент.–1 окт. 2009 г. / ВГКС ; редкол.: М.А. Баркун [и др.]. – Минск, 2009. – С. 138.

24–А. Зельманский, О.Б. Подходы к решению задачи сегментирования речи в рамках разработки генератора речеподобных сигналов / О.Б. Зельманский, А.Г. Давыдов // Современные проблемы радиотехники и телекоммуникаций РТ – 2010: материалы VI Междунар. молодеж. науч.-техн. конф., Севастополь, 19–24 апр. 2010 г. / СевНТУ ; редкол.: Е.В. Пашков [и др.]. – Севастополь, 2010. – С. 386.

25–А. Зельманский, О.Б. К вопросу о возможности применения синтезатора речеподобных сигналов для систем защиты информации / О.Б. Зельманский, В.Л. Николаенко // Информационные системы и технологии : материалы XVI Междунар. науч.-техн. конф., Н. Новгород, 23 апр. 2010 г. / Нижегород. гос. техн. ун-т им. Р.Е. Алексеева ; редкол.: В.П. Кириенко [и др.]. – Н. Новгород, 2010. – С. 101.

26–А. Зельманский, О.Б. Система защиты речевой информации на основе генератора «речеподобных» сигналов / О.Б. Зельманский, А.Г. Давыдов // Технические средства защиты информации: материалы VIII Белорус.-российск. науч.-техн. конф., Браслав, 24–28 мая 2010 г. / БГУИР ; редкол.: Л.М. Лыньков [и др.]. – Минск, 2010. – С. 14–15.

27–А. Зельманский, О.Б. Исследование влияния структуры материалов на ослабление и разборчивость проходящих через них речевых сигналов / О.Б. Зельманский, И.С. Худoley, А.М. Прудник // Технические средства защиты информации: материалы VIII Белорус.-российск. науч.-техн. конф., Браслав, 24–28 мая 2010 г. / БГУИР ; редкол.: Л.М. Лыньков [и др.]. – Минск, 2010. – С. 72.

28–А. Зельманский, О.Б. Применение речеподобных сигналов в системах активной акустической маскировки / О.Б. Зельманский, А.Г. Давыдов // Современные средства связи : материалы XV Междунар. науч.-техн. конф., Минск, 28–30 сент. 2010 г. / ВГКС ; редкол.: А.О. Зеневич [и др.]. – Минск, 2010. – С. 118.

29–А. Зельманский, О.Б. Модуль сегментации речи для систем синтеза речеподобных сигналов / О.Б. Зельманский, А.Г. Давыдов // Современные проблемы радиотехники и телекоммуникаций РТ – 2011: материалы VII Междунар. молодеж. науч.-техн. конф., Севастополь, 11–15 апр. 2011 г. / СевНТУ ; редкол.: Ю.Б. Гимпилевич [и др.]. – Севастополь, 2011. – С. 476.

30–А. Зельманский, О.Б. Модуль сегментации речевых сигналов / О.Б. Зельманский, А.Г. Давыдов // Информационные системы и технологии : материалы XVII Междунар. науч.-техн. конф., Н. Новгород, 22 апр. 2011 г. / Нижегород. гос. техн. ун-т им. Р.Е. Алексеева ; редкол.: В.Г. Баранов [и др.]. – Н. Новгород, 2011. – С. 376.

31–А. Зельманский, О.Б. О возможности применения модуля верификации диктора по голосу в системах генерирования речеподобных сигналов / О.Б. Зельманский // Технические средства защиты информации: материалы IX Белорус.-российск. науч.-техн. конф., Минск, 28–29 июня 2011 г. / БГУИР ; редкол.: Л.М. Лыньков [и др.]. – Минск, 2011. – С. 13–14.

32–А. Зельманский, О.Б. Задача классификации речи в рамках разработки системы синтеза речеподобных сигналов / О.Б. Зельманский // Современные средства связи: материалы XVII Междунар. науч.-техн. конф., Минск, 27–29 сент. 2011 г. / ВГКС ; редкол.: А.О. Зеневич [и др.]. – Минск, 2011. – С. 109.

33–А. Зельманский, О.Б. Методика классификации речи / О.Б. Зельманский // Современные проблемы радиотехники и телекоммуникаций РТ – 2012: материалы VIII Междунар. молодеж. науч.-техн. конф., Севастополь, 23–27 апр. 2012 г. / СевНТУ ; редкол.: Е.В. Пашков [и др.]. – Севастополь, 2012. – С. 363.

Патенты

34–А. Способ детектирования речи : пат. 15755 Респ. Беларусь, МПК7 G 06 L 11/02 / О.Б. Зельманский, А.Г. Давыдов, Г.В. Давыдов, Л.М. Лыньков; заявитель БГУИР. – № а 20081472 ; заявл. 20.11.2008 ; опубл. 18.01.2012 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2012. – № 2. – С. 165.

35–А. Устройство автоматического распознавания диктора: пат. 6229 Респ. Беларусь, МПК7 G 10 L 15/00 / О.Б. Зельманский, А.Г. Давыдов, Г.В. Давыдов, Л.М. Лыньков; заявитель БГУИР. – № u 20090860 ; заявл. 20.10.2009 ; опубл. 16.02.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 1 (72). – С. 215–216.

36–А. Устройство автоматического распознавания диктора по речи: пат. 6754 Респ. Беларусь, МПК7 G 10 L 15/00 / О.Б. Зельманский, Аль-Хатми Мохаммед Омар ; заявитель БГУИР. – № u 20100311 ; заявл. 25.03.2010 ; опубл. 04.08.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 5 (76). – С. 242–243.

37–А. Звуконепроницаемая камера для мобильных средств связи: пат. 6910 Респ. Беларусь, МПК7 E 04 B 1/82 / О.Б. Зельманский, С.Н. Петров, Н.В. Насонова, Л.М. Лыньков; заявитель БГУИР. – № u 20100312 ; заявл. 25.03.2010 ; опубл. 01.10.2011 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 6 (77). – С. 228.

38–А. Устройство синтеза речеподобных сигналов для защиты речевой информации от утечки по вибрационным и акустическим каналам: пат. 8193

Респ. Беларусь, МПК7 Н 04 К 3/00, G 10 L 19/14 / О.Б. Зельманский, А.Г. Давыдов, Г.В. Давыдов, Л.М. Лыньков; заявитель БГУИР. – № и 20110834 ; заявл. 27.10.2011; опубл. 01.02.2012 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2012. – № 2. – С. 276.

39–А. Устройство анализа речи: пат. 8194 Респ. Беларусь, МПК7 G 10 L 15/00 / О.Б. Зельманский, А.Г. Давыдов; заявитель БГУИР. – № и 20110835 ; заявл. 27.10.2011; опубл. 01.02.2012 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2012. – № 2. – С. 270.

40–А. Устройство бесконтактного измерения вибрационных характеристик и акустических колебаний : пат. 8195 Респ. Беларусь, МПК7 G 01 H 9/00 / О.Б. Зельманский, Д.М. Каван, Г.В. Давыдов, Л.М. Лыньков; заявитель БГУИР. – № и 20110836 ; заявл. 27.10.2011 ; опубл. 01.02.2012 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2012. – № 2. – С. 257.

Отчеты

41–А. Доработать и подготовить к запуску в производство детектор речи для устройств защиты речевой информации типа «Прибой», систем аудиозаписей и систем связи : отчет об ОКР (заключ.) / БГУИР ; главн. констр. Г.В. Давыдов. – Минск, 2011. – 60 с. – № ГР 20113150.

42–А. Разработка программных модулей детектирования и сегментации речи : отчет о НИР (заключ.) / БГУИР ; рук. темы А.Г. Давыдов. – Минск, 2012. – 35 с. – № ГР 20112037.

3



РЭЗІЮМЭ

Зельманскі Алег Барысавіч

Сінтэз мовападобных перашкод для абароны інфармацыі ад уцечкі па акустычных каналах

Ключавыя словы: аналіз мовы, сінтэз мовы, мовападобныя перашкоды, дэтэктаванне мовы, сегментацыя мовы, класіфікацыя мовы, верыфікацыя дыктара.

Мэта працы: распрацоўка сінтэзу мовападобных перашкод для абароны перагавораў на некалькіх мовах і стварэнне на яго аснове шматфункцыянальнага ўстройства абароны маўленчай інфармацыі ад уцечкі па тэхнічных каналах.

Метады даследвання: тэарэтычныя і эксперыментальныя метады лічбавай апрацоўкі сігналаў, аналізу і сінтэзу мовы, метады камп'ютэрнага мадэліравання.

Атрыманыя вынікі і іх навізна: распрацаваны сінтэз мовападобных перашкод для абароны інфармацыі ад уцечкі па акустычных каналах, які заснаваны на кампеляцый часткаў запісаў прамовы дыктараў на розных мовах па фанэмнаму тэксту, і на ўжыванні верыфікацыі, сегментацыі і класіфікацыі мовы. Прапанаваны спосаб дэтэктавання маўленчага сігнала для сінтэзу мовападобных перашкод, які дазваляе вылучаць і запісваць маўленчыя ўчасткі аўдыясігнала, пры гэтым частата памылковых спрацоўванняў знізілася да 19,6 %, а частата пропуску маўленчых часткаў – да 14,9 %. Распрацаваны алгарытм фарміравання баз алафонаў непасрэдна з прамовы рознамоўных удзельнікаў перамоў для сінтэзу мовападобных перашкод, які складаецца з сегментацыі мовы на фанетычныя адзінкі і іх класіфікацыі і характарызуецца адноснай дакладнасцю выяўлення межаў фанем да 98 %, колькасцю лішніх межаў да 17,5 %, колькасцю межаў, якія патрэбна выяўляць, да 72 %. Гэта распрацоўка дазволіла прапанаваць устройства фарміравання баз алафонаў рознамоўных дыктараў.

Ступень выкарыстання: прапанаванае ўстройства, якое рэалізуе распрацаваныя метадыкі, можа ўжывацца для абароны перагавораў на розных мовах шляхам маскіравання прамовы ўдзельнікаў перамоў мовападобным шумам, які фарміруецца непасрэдна з гэтай прамовы. Вынікі дысертацыйнага даследавання ўкаранены ў практыку НДЛ 5.3 і навучальны працэс установы адукацыі «Беларускі дзяржаўны ўніверсітэт інфарматыкі і радыёэлектронікі».

Вобласць ужывання: абарона акустычнай інфармацыі ад уцечкі па тэхнічных каналах.

РЕЗЮМЕ

Зельманский Олег Борисович

Синтез речеподобных помех для защиты информации от утечки по акустическим каналам

Ключевые слова: анализ речи, синтез речи, речеподобные помехи, детектирование речи, сегментация речи, классификация речи, верификация диктора.

Цель работы: разработка синтеза речеподобных помех для защиты переговоров на нескольких языках и создание на его основе многофункционального устройства защиты речевой информации от утечки по техническим каналам.

Методы исследования: теоретические и экспериментальные методы цифровой обработки сигналов, анализа и синтеза речи, методы компьютерного моделирования.

Полученные результаты и их новизна: разработан синтез речеподобных помех для защиты информации от утечки по акустическим каналам, базирующийся на компиляции участков записей речи дикторов на разных языках по фонемному тексту, применении верификации, сегментации и классификации речи. Предложен способ детектирования речевого сигнала для синтеза речеподобных помех, который позволяет выделять и записывать речевые участки аудиосигнала, при этом частота ложных срабатываний снизилась до 19,6%, а частота пропуска речевых участков – до 14,9%. Разработан алгоритм формирования баз аллофонов непосредственно из речи разноязычных участников переговоров для синтеза речеподобных помех, заключающийся в сегментации и аллофонной классификации речи, характеризующийся относительной точностью обнаружения границ фонем до 98 %, количеством лишних границ до 17,5 %, количеством обнаруживаемых границ до 72 %, что позволило предложить устройство формирования баз аллофонов разноязычных дикторов.

Степень использования: предложенное устройство, реализующее разработанные алгоритмы, может применяться для защиты переговоров на разных языках путем маскирования речи участников переговоров речеподобным шумом, формируемым непосредственно из их речи. Результаты диссертационного исследования внедрены в практику НИЛ 5.3 и учебный процесс учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Область применения: защита акустической информации от утечки по техническим каналам.

SUMMARY

Zelmanski Oleg Borisovich

Synthesis of speech-like noise for information protection from a leakage through acoustic channels

Keywords: speech analysis, speech synthesis, speech-like noise, voice activity detection, speech segmentation, speech classification, speaker verification.

The aim of the work: is to develop a synthesis of speech-like noise for the protection of the negotiations in several languages and create on its basis the multifunctional device for information protection from a leakage through technical channels.

Research methods: theoretical and experimental methods of digital signal processing, speech analysis and synthesis, computer simulation techniques.

Obtained results and its novelty: the synthesis of speech-like noise is developed to protect the information from a leakage through acoustic channels. It is based on a compilation of parts of speech recordings of speakers in different languages according to a phonemic text and on use of speech verification, segmentation and classification. The voice activity detection technique for the synthesis of speech-like noise is proposed. It allows selecting and recording the speech sections of audio signal while the false alarm rate decreased to 19.6%, and the miss rate decreased to 14.9%. The technique of forming databases of allophones directly from the speech of multilingual speakers for the synthesis of speech-like noise is proposed. It includes the speech segmentation into phonetic units and their classification. It has a relative accuracy of the detection of boundaries of phonemes up to 98%, the number of extra boundaries up to 17.5%, the number of detected boundaries up to 72% that allowed proposing the device of automatic forming allophone databases of multilingual speakers.

Extend of usage: the proposed device that implements developed techniques can be applied to protect the talks in different languages by masking speech of the participants of the conversation by speech-like noise formed directly from their speech. The results of the dissertation research are introduced into practice of the SRL 5.3 and the learning process of the Belarusian State University of Informatics and Radioelectronics.

Field of application: protection of acoustic information from a leakage through technical channels.

Научное издание

ЗЕЛЬМАНСКИЙ ОЛЕГ БОРИСОВИЧ

**СИНТЕЗ РЕЧЕПОДОБНЫХ ПОМЕХ ДЛЯ ЗАЩИТЫ
ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ**

Специальность 05.13.19 – Методы и системы защиты информации,
информационная безопасность

**Автореферат диссертации на соискание ученой степени
кандидата технических наук**

Подписано в печать 05.07.2012.
Гарнитура «Таймс».
Уч.-изд. л. 1,5.

Формат 60x84 1/16.
Отпечатано на ризографе.
Тираж 60 экз.

Бумага офсетная.
Усл. печ. л. 1,86.
Заказ 361.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6