УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 621.391.16; 534(043.3)

РАХАНОВ
Константин Яковлевич

ШИРОКОПОЛОСНАЯ ЛИНЕЙНО-ЧАСТОТНАЯ МОДУЛЯЦИЯ СИГНАЛА ДЛЯ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

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 «Полоцкий государственный университет».

Железняк Владимир Кириллович,
доктор технических наук, профессор,
профессор кафедры технологий
программирования учреждения образования
«Полоцкий государственный университет»

Официальные оппоненты: **Липницкий Станислав Феликсович**,
доктор технических наук,
главный научный сотрудник Государственного
научного учреждения «Объединенный институт
проблем информатики Национальной академии
наук Беларуси»

Прудник Александр Михайлович,
кандидат технических наук,
докторант кафедры защиты информации
учреждения образования «Белорусский
государственный университет информатики
и радиоэлектроники»

Оппонирующая организация: **Учреждение образования «Военная академия Республики Беларусь»**

Защита состоится 11 апреля 2013 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. 293-89-89, e-mail: dissovet@bsuir.by.

ВВЕДЕНИЕ

В «Концепции национальной безопасности Республики Беларусь», утвержденной Указом Президента Республики Беларусь от 09.11.2010 № 575, сформулированы цели системного формирования и реализации национальной безопасности. В частности, заданы приоритетные направления национальной безопасности (п. 54) по «...разработке и внедрению современных методов и средств защиты информации».

Совершенствование средств и методов извлечения сигналов из шумов высокого уровня (например, очисткой сигнала от шумов) обусловило развитие средств и методов оценки их защищенности в каналах утечки речевой информации. Из существующих методов оценки защищенности информации метод шумового сигнала функционально ограничен, методически не совершенен. Метод гармонического сигнала обладает рядом преимуществ, но обладает некоторыми методическими (теоретическими) погрешностями.

Анализ этих методов определил направление исследования, заключающееся в обосновании и разработке на новом принципе метода оценки защищенности присущих речевому сигналу каналов утечки информации. Новый метод базируется на преимуществах сигнала с широкополосной линейно-частотной модуляцией в надпороговой области, которую расширяют снижением порогового эффекта. Кроме того, частотно-временное представление сигнальной энергии функцией Вигнера позволило учесть тонкую структуру сигнала с широкополосной линейно-частотной модуляцией. Корреляционная теория разборчивости речи, разработанная для метода гармонического сигнала, значительно снизила методическую (теоретическую) погрешность нового метода, учитывающего ряд факторов, искажающих акустический речевой сигнал в замкнутом пространстве.

В этой связи основным направлением исследований является научное обоснование, разработка и использование в практике оценки разборчивости речи в каналах утечки информации методом сигнала с широкополосной линейно-частотной модуляцией, внедренным во вновь разработанный программно-аппаратный комплекс. Выбранное направление исследований является ключевым, так как решает задачу оценки программно-аппаратным комплексом нормативных показателей в виде числовых значений разборчивости речи с повышенными требованиями по сравнению с известными средствами, высокой точностью, высокой разрешающей способностью по частоте и предельной чувствительностью.

На основании изложенного возникла необходимость теоретического и практического решения научной задачи обоснования принципов создания качественно нового метода сигнала с широкополосной линейно-частотной модуляцией для оценки разборчивости речи в каналах утечки информации программно-аппаратным комплексом, что определяет **актуальность** темы диссертационной работы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Тема диссертационной работы утверждена приказом ректора учреждения образования «Полоцкий государственный университет» № 477 от 12.12.2008.

Работа выполнена инициативно в учреждении образования «Полоцкий государственный университет», является развитием научно-исследовательской работы «Разработка переносного автоматизированного программно-аппаратного комплекса по проведению специальных исследований технических средств обработки информации и контроля защищенности помещений от утечки информации по акустическим и виброакустическим каналам» № ГР 20081925 по программе Союзного государства Беларуси и России «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006 – 2010 годы», а также «Разработка и создание системы измерительной автоматизированной для измерения параметров низкочастотных магнитных излучений» № ГР 20081922, в которых автор являлся ответственным исполнителем, а научный руководитель – главным конструктором разработок.

Цель и задачи исследования

Цель диссертационной работы – теоретическое обоснование и практическая реализация оценки разборчивости речи с помощью широкополосной линейно-частотной модуляции сигнала в каналах утечки информации с высокой точностью, разрешающей способностью по частоте и предельной чувствительностью.

Для достижения поставленной цели необходимо решить следующие *научные задачи*:

1. Проанализировать существующие методы и программно-аппаратные комплексы для оценки разборчивости речи в каналах утечки речевой информации, определить точностные характеристики методов, их достоинства и недостатки для выбора научного направления исследования, обосновать критерий оценки защищенности речевого сигнала.

2. Обосновать и разработать на новых принципах метод оценки разборчивости речи с помощью широкополосной линейно-частотной модуляции сигнала, исключающий недостатки существующих методов, математическую модель представления широкополосной линейно-частотной модуляции сигнала в виде тонкой структуры частотно-временным преобразованием сигнальной энергии функцией Вигнера для оценки численных значений разборчивости речи.

3. Синтезировать и обосновать приемник помехоустойчивой оценки тонкой структуры спектральной плотности сигнала широкополосной линейно-

частотной модуляции, его параметров для оценки разборчивости речи в каналах утечки информации с использованием корреляционной теории разборчивости речи.

4. Разработать метод цифровой обработки в реальном масштабе времени широкополосной линейно-частотной модуляции сигнала, реализующий синхронное накопление его спектральных составляющих в цифровой форме с автоматическим принятием решения о накоплении и частотно-временное представление сигнальной энергии функцией Вигнера для оценки разборчивости речи с учетом фактора «разрешающая способность – время».

5. Синтезировать программно-аппаратный комплекс оценки разборчивости речи в каналах утечки речевой информации, обосновать структурную схему, реализующую метод широкополосной линейно-частотной модуляции сигнала и для сравнения – метод гармонического сигнала.

6. Исследовать и экспериментально установить предельные численные значения параметров и характеристик программно-аппаратного комплекса и показать преимущества метода широкополосной линейно-частотной модуляции сигнала.

Объектом диссертационного исследования являются технические каналы утечки информации. *Предмет исследования* – методы и средства оценки и защищенности технических каналов утечки речевой информации.

Положения, выносимые на защиту

1. Метод оценки разборчивости речи в каналах утечки информации с использованием сигнала с широкополосной линейно-частотной модуляцией, реализующий его преимущества в надпороговой области повышением до надпороговой области отношения сигнал/шум синхронным накоплением спектральных составляющих, полученных прямым и обратным быстрым преобразованием Фурье, частотно-временным представлением функцией Вигнера смеси энергии сигнала широкополосной линейно-частотной модуляции и шума, в формировании его тонкой структуры с разрешающей способностью по частоте от 0,0025 до 0,086 Гц в зависимости от номера полосы равной разборчивости.

2. Синтез приемника сигнала с широкополосной линейно-частотной модуляцией и его обработки в полосах равной разборчивости путем параллельной узкополосной фильтрации оптимальными корреляционными приемниками временных срезов частотно-временного представления смеси энергии сигнала линейно-частотной модуляции и шума функцией Вигнера и оценки коэффициента разборчивости речи с предельным отношением сигнал/шум минус 18 дБ без накопления, минус 22 дБ при 10-кратном синхронном накоплении и минус 24 дБ при 100-кратном синхронном накоплении.

3. Метод цифровой обработки сигнала с широкополосной линейно-частотной модуляцией для оценки разборчивости речи, реализующий снижение порогового эффекта сигнала синхронным накоплением спектральных составляющих с автоматическим принятием решения о накоплении по критерию максимального правдоподобия, параллельную узкополосную фильтрацию временных срезов частотно-временного представления функцией Вигнера смеси энергии сигнала с широкополосной линейно-частотной модуляцией и шума с разрешающей способностью по частоте, реализующей заданную точность амплитудно-частотной характеристики сигнала с широкополосной линейно-частотной модуляцией и сокращение времени вычислений на типовом процессоре до 20 с.

4. Синтез программно-аппаратного комплекса в виде локальной измерительной схемы для оценки разборчивости речи, включающей схемно-конструктивную реализацию метода сигнала с широкополосной линейно-частотной модуляцией, и сравнение его с методом гармонического сигнала. Это показало соответствие порогов чувствительности метода сигнала с широкополосной линейно-частотной модуляцией без его синхронного накопления и метода гармонического сигнала (9,7 % – разборчивость речи с относительной погрешностью ±3 %), снижение предельного значения разборчивости речи до 3,5 % и относительной погрешности до ±1,5 % при 10-кратном синхронном накоплении, предельного значения разборчивости речи до 2,3 % и относительной погрешности до ±1 % при 100-кратном синхронном накоплении, характеризующихся относительной методической погрешностью для однослойного оконного ограждения, составляющей 3,5 % для метода сигнала с широкополосной линейно-частотной модуляцией и 17,8 % для метода гармонического сигнала, что повышает методическую точность оценки на 14,32 %.

Личный вклад соискателя

Обоснование диссертационной работы отражает личный вклад автора. Основные научные результаты, практическая реализация, а также положения, выносимые на защиту, получены лично автором. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертационной работе результатов. Они заключаются в научном обосновании метода оценки защищенности речевой информации с использованием сигнала с широкополосной линейно-частотной модуляцией для оценки разборчивости речи, в снижении порогового эффекта сигнала с широкополосной линейно-частотной модуляцией с применением оптимального частотно-временного представления сигнальной энергии функцией Вигнера, в подготовке и проведении экспериментов по исследованию влияющих факторов на методическую точность оценки.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем доктором технических наук, профессором В.К. Железняком.

Апробация результатов диссертации

Материалы, вошедшие в диссертационную работу, докладывались и обсуждались: на XIV международной конференции «Комплексная защита информации» (Могилев, Беларусь, 2009 г.); V международной конференции-форуме «Информационные системы и технологии (IST)» (Минск, Беларусь, 2009 г.); II Junior researchers' conference (Новополоцк, Беларусь, 2010 г.); VI международной конференции-форуме «Информационные системы и технологии (IST)» (Минск, Беларусь, 2010 г.); III Junior researchers' conference (Новополоцк, Беларусь, 2011 г.); первой международной научно-практической конференции «Интеллектуальные системы на транспорте» (Санкт-Петербург, Россия, 2011 г.); XVI научно-практической конференции «Комплексная защита информации» (Гродно, Беларусь, 2011 г.); XVII научно-практической конференции «Комплексная защита информации» (Суздаль, Россия, 2012 г.); IV Junior researchers' conference (Новополоцк, Беларусь, 2012 г.); X белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Беларусь, 2012 г.); республиканском научном семинаре «Математическое моделирование сложных систем, анализ данных и защита информации» (Минск, Беларусь, 2012 г.).

Опубликованность результатов диссертации

Материалы по теме диссертации опубликованы в 6 статьях в изданиях, рекомендованных для опубликования результатов диссертационных исследований, рецензируемых научных журналах. Автору принадлежит 3,43 авторских листа, соответствующих п. 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь.

Опубликовано 12 статей в сборниках материалов конференций, семинаров, 2 тезисов докладов в сборниках тезисов конференций и семинаров, получено 2 патента Республики Беларусь на изобретение, которые внесены в перечень перспективных.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с выводами по каждой главе, заключения, библиографического списка и приложений. Общий объем диссертационной работы составляет 112 страниц, включая 84 страницы машинописного текста, 33 иллюстрации на 19 страницах, 7 таблиц на 4 страницах, библиографический список из 118 наименований, из них 20 собственных публикаций автора, и 3 приложения на 5 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** и в общей характеристике диссертационной работы обоснована актуальность темы диссертации, определено основное направление исследований, обоснована необходимость исследований методов оценки защищенности речевой информации в условиях воздействующих факторов, программно-аппаратных комплексов оценки разборчивости речи с повышением методической (теоретической) точности оценки разборчивости речи, с высокой разрешающей способностью по частоте и высокой предельной чувствительностью. Поставлена цель и научные задачи, определены ограничения исследования.

В **первой главе** представлены характеристики технических каналов утечки речевой информации. Анализируются внешние факторы, влияющие на точность оценки разборчивости речи в каналах утечки информации. Приведены обзор и анализ методов оценки защищенности речевой информации (метод шумового сигнала, метод гармонического сигнала по СТБ 34.101.29-2011), основных параметров современных программно-аппаратных комплексов: К6-6 «Трап» (ФГУП «ГНПП "Информакустика"»), «Спрут» (ЗАО НЦП «НЕЛК»), «Шепот» (ЦБИ «МАСКОМ»), а также «ФИЛИН-А», разработанный в Республике Беларусь (УО «ПГУ» совместно с ГП «НИИ ТЗИ»). Указано на ряд преимуществ и присущие методические (теоретические) погрешности метода гармонического сигнала. Анализируется точность оценки защищенности речевой информации при ограниченных измерительных ресурсах. Критерием точности принята методическая (теоретическая) погрешность оценки разборчивости речи при слабых сигналах в шумах высокого уровня в каналах утечки речевой информации.

На основе анализа литературных источников показано, что современные методы и средства оценки защищенности не позволяют выявлять каналы утечки речевой информации с требуемой методической точностью и учетом всех влияющих факторов, что обусловливает разработку более совершенного метода и его дальнейшее внедрение в программно-аппаратный комплекс.

Во **второй главе** обосновано использование нового метода сигнала с широкополосной линейно-частотной модуляцией (ШЛЧМ) для оценки разборчивости речи. В отличие от метода гармонического сигнала, который использует средние частоты в полосах равной разборчивости для оценки защищенности речевого сигнала, метод сигнала с ШЛЧМ расширил возможность оценки защищенности речи на всех частотах полос равной разборчивости, на которые разбивается спектр речевого сигнала.

Такому сигналу присущ пороговый эффект, снижение которого предложено повышением отношения сигнал/шум в $\sqrt{P}$ раз в результате P-кратного синхронного накопления выделяемых из смеси сигнала с ШЛЧМ и шума быстрым преобразованием Фурье когерентных спектральных составляющих ШЛЧМ сигнала и некогерентных шумовых составляющих. Дальнейшее обратное преобразование Фурье представляет собой исходный сигнал с ШЛЧМ с улучшенным отношением сигнал/шум для последующего преобразования.

Для учета тонкой структуры сигнала с ШЛЧМ предложено использовать совместные частотно-временные описания сигналов. Одним из продуктивных методов решения задачи оценивания параметров сигналов является подход на основе частотно-временного распределения Вигнера, которое характеризуется предельной концентрацией энергии (минимальным локальным и глобальным разбросами) сигнала вдоль линии его мгновенных частот. Это свойство указывает на преимущество распределения Вигнера перед другими частотно-временными распределениями, благодаря чему возможно измерять параметры сигнала на интервале частот сигнала с ШЛЧМ.

На рисунке 1 представлено преобразование Вигнера дискретной реализации смеси сигнала с ШЛЧМ в полосе от 100 до 420 Гц амплитудой 1 В длительностью 1 с и шума, на котором отслеживается изменение интенсивности сигнальной энергии по времени.

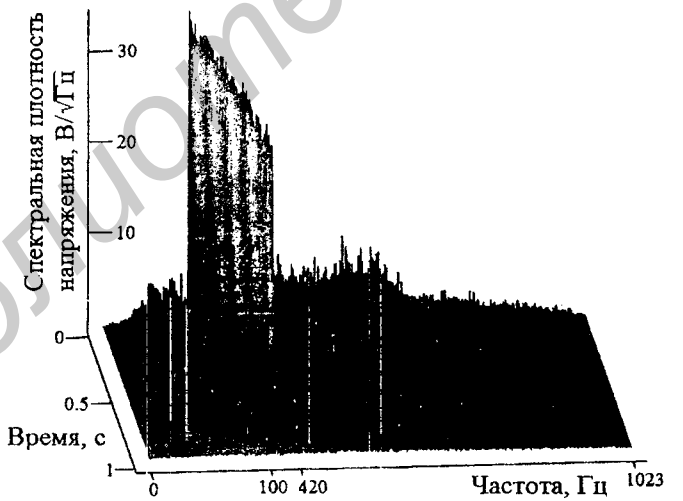


Рисунок 1 – Частотно-временное преобразование смеси сигнала с широкополосной линейно-частотной модуляцией и шума

Приведена математическая модель локализации энергии сигнала и определения энергетического критерия защищенности речевой информации (отношения сигнал/шум) на основании априорной информации о частоте сигнала в определенный момент времени.

Решена проблема автоматического выбора эффективного значения для порога принятия решения при обнаружении сигналов с низкой энергетикой в условиях отсутствия априорных знаний о характере шумов. Порог принятия решения определяется медианным значением спектра входной реализации без предварительного обучения по критерию максимального правдоподобия.

Несмотря на оптимальность преобразования Вигнера в смысле локализации энергии, практическое применение частотно-временного преобразования Вигнера связано с определенными сложностями. Так, бесконечность пределов функции Вигнера и отсутствие ограничений в реализации корреляции ведут к образованию ложных выбросов энергии в частотно-временной плоскости, возникающих в результате взаимного влияния соседних сигнальных компонент друг на друга, образующих интерференционный фон. Этот недостаток обусловил синтез приемника для приема и обработки сигнала с ШЛЧМ в полосах равной разборчивости.

На входе разработанного приемника сигнала с ШЛЧМ для оценки разборчивости речи установлены первичные измерительные преобразователи информационных полей рассеивания (акустического, виброакустического, магнитного, электромагнитного и др.), которые преобразуют первичные информационные поля в электрический сигнал. Блок синхронного накопления преобразованного измерительного сигнала снижает пороговый эффект сигнала с ШЛЧМ, что увеличивает предельную чувствительность извлечения слабого сигнала из шумов высокого уровня.

Надпороговый сигнал с ШЛЧМ частотно-временным преобразованием Вигнера разбивается на временные составляющие, для которых применяется узкополосная фильтрация M-параллельными оптимальными приемниками гармонического сигнала. Такая фильтрация определяет тонкую структуру сигнала с ШЛЧМ (уровни) во всем диапазоне частот полосы равной разборчивости. M-параллельные измерители уровней мощности сигнал плюс шум позволяют установить отношение сигнал/шум на каждой узкополосной составляющей тонкой структуры сигнала с ШЛЧМ для вычисления парциальных и интегральных коэффициентов разборчивости речи и величины разборчивости речи.

В **третьей главе** разработан метод цифровой обработки сигнала с ШЛЧМ для оценки разборчивости речи, реализующий снижение его порогового эффекта синхронным накоплением спектральных составляющих с автоматическим принятием решения о накоплении по критерию максимально-

го правдоподобия и параллельную узкополосную фильтрацию временных срезов частотно-временного представления функцией Вигнера смеси энергии сигнала с ШЛЧМ и шума с разрешающей способностью по частоте от 0,0025 до 0,086 Гц для используемого измерительного аналогово-цифрового преобразователя L-Card E14-440.

Представлен обобщенный принцип оценки защищенности и принятых мер защиты объекта информатизации, который формализует и делит обработку сигнала с ШЛЧМ на дискретные модули: снижение порогового эффекта сигнала с ШЛЧМ и оценка величины разборчивости речи с помощью сигнала с ШЛЧМ. Разработка метода цифровой обработки сигнала с ШЛЧМ реализует автоматизацию ПАК в составе обобщенного алгоритма оценки защищенности и принятых мер защиты объекта информатизации, реализующего свойства приемника сигнала с ШЛЧМ.

Обработка сигнала с ШЛЧМ для оценки величины разборчивости речи осуществляется в цифровом виде программным компонентом и является наиболее емкой по вычислительным ресурсам. Поэтому рассмотрена временная эффективность оценки разборчивости речи. Определено количество базовых операций для выполнения алгоритма оценки разборчивости речи методом сигнала с ШЛЧМ $C(n) = 1{,}16 \cdot 10^{12}$.

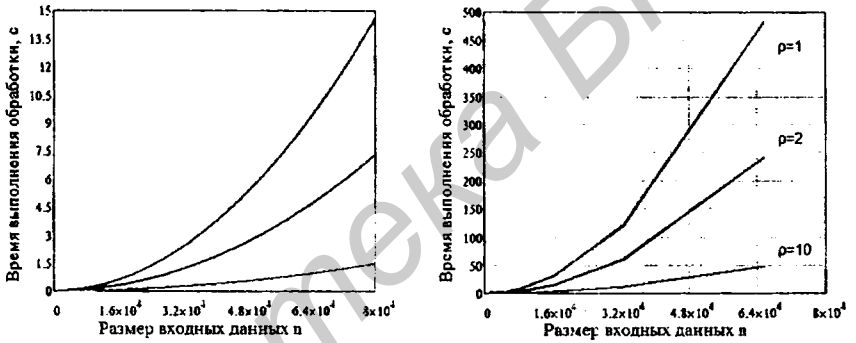
Для вычисления на ПЭВМ, имеющей производительность, например, $3{,}18 \cdot 10^9$ флоп/с (Intel® Core™ Duo U2400), получено время выполнения алгоритма $T(n) = 365$ с. Такая продолжительность выполнения алгоритма является приемлемой для практического использования ПАК при исследовании объекта информатизации, так как позволяет детально установить факторы, обусловливающие каналы утечки речевой информации.

Уменьшение времени выполнения обработки осуществляется за счет оптимизации количества временных составляющих в функции Вигнера, что сокращает количество полос разбиения с $M_{max} = n/4$ до $M = n/4\rho$, где ρ – коэффициент снижения количества полос разбиения, $\rho \in [1; n/4]$. Например, при $\rho = 1$ количество полос разбиения сигнала с ШЛЧМ составит $M = n/4$, а при $\rho = n/4$ – $M = 1$.

Коэффициент снижения количества полос разбиения обусловливает снижение вычислительных затрат, но также снижает информативность тонкой структуры сигнала с ШЛЧМ. Для примера на рисунке 2, *а* представлено расчетное время выполнения алгоритма процессором Intel® Core™ Duo U2400 в зависимости от размера входных данных n и коэффициента снижения количества полос разбиения $\rho = 1; 2; 10$. Хотя представленная оценка является приблизительной, она позволяет судить о характере увеличения временной эффективности алгоритма.

Полученное время выполнения алгоритма показывает высокую эффективность обработки по сравнению с временем расчета классической функции Вигнера с размером входных данных $n = 4 \cdot 10^5$, имеющей количество базовых операций $C(n) = 2n^3(7 + \log(n)) = 1{,}6 \cdot 10^{18}$. Время расчета классической функции Вигнера для процессора Intel® Core™ Duo U2400 составляет $T(n) = 1/3{,}18 \cdot 10^9 \cdot 1{,}6 \cdot 10^{18} = 5 \cdot 10^8$ с (порядка 15-ти лет). Это говорит о том, что практическое использование классической функции Вигнера весьма затруднительно.

Дальнейшая реализация предложенного алгоритма в среде Microsoft Visual Studio 2008 на языке C# позволила более точно оценить время выполнения обработки программным компонентом на практике. На рисунке 2, *б* представлено время выполнения обработки процессором AMD Sempron™ 2800+.



а) *б*)

***а* – расчетное время; *б* – практическое время**

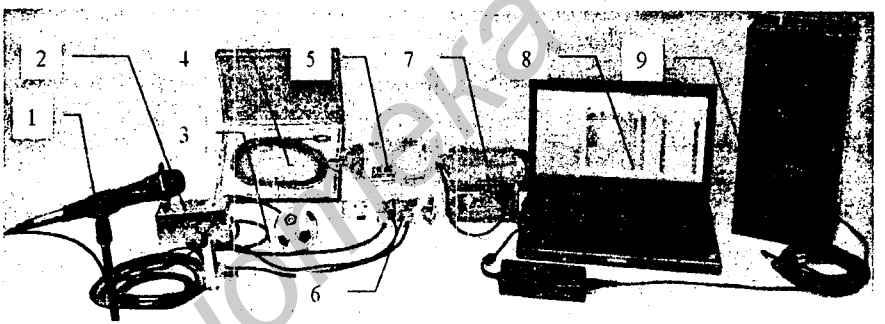
Рисунок 2 – Зависимость времени выполнения обработки с коэффициентом снижения количества полос разбиения ρ = 1; 2; 10 от размера входных данных

Полученное время выполнения обработки позволяет утверждать, что предложенная цифровая обработка пригодна для использования в ПАК с коэффициентом снижения количества полос разбиения $\rho > 10$, который может меняться в зависимости от производительности используемого процессора. Так, при частоте дискретизации $f_d = 2 \cdot 10^5$ коэффициент снижения количества полос разбиения $\rho = 10$ снижает информативность тонкой структуры сигнала с ШЛЧМ от $M_{max} = 10^5$ до $M = 10^4$, что незначительно отражается на методической погрешности.

Анализ сигнала с ШЛЧМ с количеством полос M_{max} является неоправданно объемным и затруднительным. Оптимальным количеством полос для каждой полосы равной разборчивости является $M = 125$, где коэффициент снижения количества полос разбиения $\rho = 800$, что обусловливает практическое выполнение обработки типовым процессором AMD Sempron™ 2800+ за 20 с.

В **четвертой** главе синтезирован ПАК, основанный на новом предложенном методе сигнала с ШЛЧМ для обоснования полученных теоретических основных параметров (чувствительность, погрешность), замена шумомера-анализатора на высокоточный разрядный измерительный аналогово-цифровой преобразователь.

Для подтверждения результатов оценки защищенности канала утечки речевой информации методом сигнала с ШЛЧМ синтезирован и разработан опытный образец и комплект конструкторской документации ПАК «ЕРМАК», внешний вид которого представлен на рисунке 3.



1 – остронаправленный микрофон;
2 – пространственно-избирательный преобразователь измерительный магнитный активный;
3 – пространственно-избирательный преобразователь измерительный электрический активный;
4 – вибропреобразователь; 5 – измерительный аналогово-цифровой преобразователь;
6 – устройство приемо-передающее; 7 – преобразователь токовый;
8 – персональная электронно-вычислительная машина типа ноутбук;
9 – активная акустическая система

Рисунок 3 – Программно-аппаратный комплекс «ЕРМАК»

Принципиальное отличие разработанного комплекса от существующих заключается в высокой точности результатов оценки разборчивости речи благодаря разработке и внедрению в него нового метода сигнала с ШЛЧМ, обладающего высокой теоретической точностью, схемно-конструктивному и про-

граммному решению основных элементов ПАК. Метод гармонического сигнала реализован в нем для сравнительной оценки с методом сигнала с ШЛЧМ.

Сравнение результатов, полученных методом сигнала с ШЛЧМ и методом гармонического сигнала, выполнено при воздействующих факторах (искусственные шумы и случайные помехи, фоновые и маскирующие шумы, реверберационные и резонансные явления замкнутого пространства, неравномерности АЧХ) в точке наблюдения за пределом объекта информатизации.

В качестве исследуемого объекта информатизации использовано выделенное помещение прямоугольной формы (ширина – 3 м, длина – 6 м, высота – 2,5 м) с входной дверью и однослойным оконным ограждением (ширина – 1 м, высота – 1,2 м, толщиной остекления – 0,005 м) из силикатного стекла. Объектом исследования выбрано однослойное оконное ограждение как наиболее уязвимое к утечке речевой информации. Для оценки разборчивости речи использовался уровень сигнала 74 дБ при уровне шума 54 дБ в точке приема.

Предварительно на основании математической модели исследован основной параметр оконного ограждения – зависимость затухания речевого сигнала от частоты в речевом диапазоне частот. Полученная зависимость показала, что исследуемое оконное ограждение имеет ярко выраженные резонансные частоты в диапазонах от 800 до 2000 Гц и от 2000 до 4000 Гц, характерные для однослойных ограждающих конструкций. Это значительно увеличивает вероятность утечки речевой информации. Теоретическая разборчивость речи, рассчитанная согласно корреляционной теории разборчивости речи для исследуемого оконного ограждения, составила 19,34 %.

Сравнивая экспериментальные неравномерности АЧХ объекта информатизации, полученные гармоническим и сигналом с ШЛЧМ (рисунок 4) при одинаковых исходных параметрах, отмечено, что на средних частотах полос равной разборчивости уровни гармонического и сигнала с ШЛЧМ совпадают. Это подтверждает, что метод сигнала с ШЛЧМ и метод гармонического сигнала обладают равной воспроизводимостью оценки уровней гармонических сигналов на средних частотах полос равной разборчивости.

Представленная неравномерность АЧХ, полученная сигналом с ШЛЧМ, имеет более высокую разрешающую способность (информативность), представленную 125-ю точками в каждой полосе равной разборчивости, по сравнению с гармоническим сигналом. Данное свойство сигнала с ШЛЧМ повышает точность оценки защищенности канала утечки речевой информации со значительной неравномерностью АЧХ (например, электроакустического канала утечки информации).

Различия в коэффициентах разборчивости речи, полученные на основании экспериментальных данных методов гармонического и сигнала с ШЛЧМ, имеют явно выраженный характер (рисунок 5).

Рисунок 4 – Нормированные уровни гармонического сигнала и сигнала с широкополосной линейно-частотной модуляцией в полосах равной разборчивости

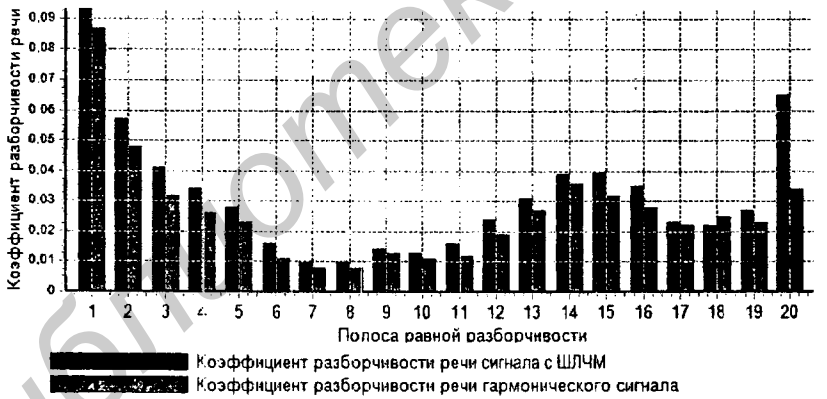


Рисунок 5 – Зависимости коэффициентов разборчивости речи от номера полосы равной разборчивости, полученные методами гармонического сигнала и сигнала с широкополосной линейно-частотной модуляцией

Экспериментальная разборчивость речи для метода гармонического сигнала составила 15,89 %, а для метода сигнала с ШЛЧМ – 18,66 %. Принятая в качестве действительного значения разборчивости речи исследуемого окон-

ного ограждения величина теоретической разборчивости речи 19,34 % позволила определить абсолютную и относительную погрешности метода сигнала с ШЛЧМ и метода гармонического сигнала (таблица 1).

Таблица 1 – Показатели защищенности при исследовании оконного ограждения

Показатель защищенности	Теоретический расчет	Метод сигнала с широкополосной линейно-частотной модуляцией	Метод гармонического сигнала
Разборчивость речи, %	19,34	18,66	15,89
Абсолютная погрешность, %	–	0,68	3,45
Относительная погрешность, %	–	3,52	17,84

На примере оконного ограждения экспериментально установлено, что методу гармонического сигнала присущи методические погрешности, обусловленные неравномерностью АЧХ, а предложенный метод сигнала с ШЛЧМ позволяет улучшить методическую точность оценки разборчивости речи для данного эксперимента на 14,32 %.

На основании дисперсионной обработки экспериментальных данных, полученных без накопления и с накоплением 10 и 100 раз, установлены предельные параметры метода оценки разборчивости речи с помощью сигнала с ШЛЧМ (таблица 2).

Таблица 2 – Предельные параметры метода сигнала с широкополосной линейно-частотной модуляцией

Наименование параметра	Значение
Предельное отношение сигнал/шум (без накоплений), дБ	–18
Предельное отношение сигнал/шум (10 накоплений), дБ	–22
Предельное отношение сигнал/шум (100 накоплений), дБ	–24
Предельная разборчивость речи (без накоплений), %	9,7
Предельная разборчивость речи (10 накоплений), %	3,5
Предельная разборчивость речи (100 накоплений), %	2,3
Максимальная относительная погрешность (без накоплений), %	±3
Максимальная относительная погрешность (10 накоплений), %	±1,5
Максимальная относительная погрешность (100 накоплений), %	±1
Разрешающая способность в полосах равной разборчивости, количество разбиений полосы равной разборчивости	не менее 1 и не более 100 000

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Впервые предложен метод сигнала с ШЛЧМ для оценки разборчивости речи в канале утечки речевой информации. Теоретически обоснованы снижение методической (теоретической) погрешности, повышение предельной чувствительности и разрешающей способности по частоте, реализованные снижением порогового эффекта сигнала с ШЛЧМ синхронным накоплением спектральных составляющих и частотно-временным представлением смеси сигнала с ШЛЧМ и шума функцией Вигнера, позволившей определить в полосах равной разборчивости тонкую структуру сигнала с ШЛЧМ [1; 3; 4; 5].

2. Синтезирован приемник сигнала с ШЛЧМ, оценивающий с высокой точностью, предельной чувствительностью и разрешающей способностью по частоте разборчивость речи в полосах равной разборчивости путем параллельной узкополосной фильтрации оптимальными корреляционными приемниками тонкой структуры частотно-временного представления функцией Вигнера смеси энергии сигнала с ШЛЧМ и шума [1].

3. Разработан метод обработки сигнала с ШЛЧМ, включающий снижение порогового эффекта сигнала с ШЛЧМ и оценку разборчивости речи, которые в составе обобщенного алгоритма оценки зашищенности и принятых мер защиты объекта информатизации реализуют свойства приемника сигнала с ШЛЧМ: высокую методическую точность, разрешающую способность по частоте, предельную чувствительность. Получена высокая разрешающая способность метода сигнала с ШЛЧМ по частоте от 0,0005 до 0,0172 Гц во всем диапазоне частот полос равной разборчивости, в отличие от метода гармонического сигнала на средних частотах полос равной разборчивости с шириной полосы от 0,025 до 1 Гц [1; 4; 5].

4. Подтверждено равенство уровней сигналов, оцененных экспериментально с помощью программно-аппаратного комплекса оценки разборчивости речи методом сигнала с ШЛЧМ и методом гармонического сигнала на средних частотах полос равной разборчивости, что указывает на воспроизводимость оценки разборчивости речи методом сигнала с ШЛЧМ и методом гармонического сигнала на средних частотах полос равной разборчивости. Метод сигнала с ШЛЧМ в отличие от метода гармонического сигнала учитывает в большей мере факторы, обусловленные неравномерностью АЧХ, что показано на примере однослойного оконного ограждения, и повышает методическую (теоретическую) точность оценки разборчивости речи на 14,3 %. Показано соответствие порогов чувствительности метода сигнала с ШЛЧМ без его синхронного нако-

пления и метода гармонического сигнала (минус 18 дБ по отношению сигнал/шум и 9,7 % по разборчивости речи с относительной погрешностью ±3 %). Экспериментально установлены предельные значения отношения сигнал/шум минус 22 дБ, разборчивости речи 3,5 % и относительной погрешности до ±1,5 % при 10-кратном синхронном накоплении и предельные значения отношения сигнал/шум минус 24 дБ, разборчивости речи 2,3 % и относительной погрешности до ±1 % при 100-кратном синхронном накоплении [2; 6].

Рекомендации по практическому использованию результатов

1. Увеличенная производительность обработки сигнала с ШЛЧМ за счет применения коэффициента снижения количества полос разбиения при реализации высокой разрешающей способности (от 2 до 69 Гц) во всем диапазоне полос равной разборчивости позволяет вычислить показатели защищенности типовым процессором за 20 с [5; 16].

2. Разработанный ПАК «ЕРМАК», оценивающий защищенность и принятые меры защиты информации ОИ, выполняет оценку разборчивости речи с методической погрешностью ±1 %, с предельной разрешающей способностью по частоте от 0,00025 до 0,086 Гц, с предельной разборчивостью речи 2,3 % [7; 2; 18; 20].

3. Разработанный ПАК «ЕРМАК» не требует использования уровня сигнала с ШЛЧМ более 84 дБ благодаря высокой предельной чувствительности, что, в отличие от метода шумового сигнала, не нарушает экологические нормы при оценке защищенности ОИ любых категорий [2; 18; 20].

4. Разработанные методы и принципы построения программно-аппаратного комплекса оценки разборчивости речи рекомендуется использовать для оценки защищенности КУИ и принятых мер защиты ОИ любых категорий, а также в учебном процессе УО «Полоцкий государственный университет» при проведении занятий по дисциплинам «Защита речевой и видеоинформации», «Программно-аппаратные средства обеспечения информационной безопасности», «Технические средства и методы защиты информации».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных журналах

1. Раханов, К.Я. Имитационная модель автоматизированной помехоустойчивой оценки разборчивости речи методом ЛЧМ-сигнала / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 35 – 41.

2. Раханов, К.Я. Математическая модель формирования параметров звукоослабления оконным ограждением помещения / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2008. – № 9. – С. 141 – 146.

3. Раханов, К.Я. Методы оценки защищенности речевой информации / К.Я. Раханов, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12 – С. 2 – 8.

4. Раханов, К.Я. Обнаружение сигналов ВЧ-диапазона перемножением спектров фрагментов их реализаций / К.Я. Раханов, В.К. Железняк, С.В. Дворников, Ю.П. Супян // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2010. – № 9. – С. 29 – 34.

5. Раханов, К.Я. Оценка разборчивости речи методом гармонических и ЛЧМ-сигналов / К.Я. Раханов, В.К. Железняк // Безопасность информационных технологий. Специальный выпуск «Комплексная защита информации-XVII». – 2012. – № 1. – С. 89 – 91.

6. Раханов, К.Я. Синтез программно-аппаратной системы оценки разборчивости речи методом ЛЧМ-сигнала : результаты эксперимента // К.Я. Раханов // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2012. – № 12. – С. 20 – 26.

Статьи в сборниках материалов конференций и семинаров

7. Раханов, К.Я. Автоматизированный измерительный комплекс / К.Я. Раханов, В.К. Железняк // Комплексная защита информации: материалы XIV междунар. конф., Минск, 19 – 22 мая 2009 г. ; отв. ред. А.П. Леонов. – Минск, 2009. – С. 94.

8. Раханов, К.Я. Анализ измерительных сигналов для автоматизированной оценки защищенности аналоговой и цифровой речи / К.Я. Раханов, В.К. Железняк // Комплексная защита информации : материалы XVI науч.-практ. конф., Гродно, 17 – 20 мая 2011 г. ; под общ. ред. А.Н. Курбацкого. – Минск : БелГИСС, 2011. – С. 270 – 273.

9. Раханов, К.Я. Измерительные сигналы для оценки защищенности КУИ в речевом диапазоне частот / К.Я. Раханов, В.К. Железняк // Информационные системы и технологии (IST' 2010) : материалы VI междунар. конф., Минск, 24 – 25 нояб. 2010 г. ; редкол. : А.Н. Курбацкий (отв. ред.) [и др.]. – Минск: Издатель А.Н. Вараксин, 2010. – С. 38 – 42.

10. Раханов, К.Я. Математическая модель, основанная на научном эксперименте по повышению точности оценки защищенности КУ речевой информации / К.Я. Раханов, В.К. Железняк // Информационные системы и технологии (IST' 2010) : материалы VI междунар. конф., Минск, 24 – 25 нояб. 2010 г. ; редкол. : А.Н. Курбацкий (отв. ред.) [и др.]. – Минск : Издатель А.Н. Вараксин, 2010. – С. 84 – 87.

11. Раханов, К.Я. Методика оценки оперативного контроля источников шумового сигнала / К.Я. Раханов, В.К. Железняк // Комплексная защита информации : материалы XVI науч.-практ. конф., Гродно, 17 – 20 мая 2011 г. ; под общ. ред. А.Н. Курбацкого. – Минск : БелГИСС, 2011. – С. 273 – 276.

12. Раханов, К.Я. О селекции измерительных сигналов при оценке разборчивости речи / К.Я. Раханов, В.К. Железняк // Комплексная защита информации : материалы XIV междунар. конф., Минск, 19 – 22 мая 2009 г. ; отв. ред. А.П. Леонов. – Минск, 2009. – С. 95 – 96.

13. Раханов, К.Я. Частотно-временная обработка измерительного сигнала для оценки защищенности речи / К.Я. Раханов, В.К. Железняк // Информационные системы и технологии (IST 2009) : материалы V междунар. конф.-форума, Минск, 16 – 17 нояб. 2009 г. ; редкол. : Н.И. Листопад [и др.] : в 2 ч. – Ч. 2. – Минск : Издатель А.Н. Вараксин, 2009. – С. 46 – 50.

14. Rakhanau, K. Regression model to optimize the accuracy of securety assessments leakage channels of speech information / K. Rakhanau // European and National dimension in research: materials of junior researchers' conference, Novopolotsk, April 27 – 28, 2011: 2 p. ; Polotsk State University. – Novopolotsk, PSU, 2011. – Issue 1. Part 1: Technology. – P. 122 – 125.

15. Rakhanau, K. Time-frequency processing of the measuring signal for the estimation of immunity of speechthe / K. Rakhanau, V. Zheleznyak // European and National dimension in research : materials of junior researchers' conference, Novopolotsk, April 28 – 29, 2010 : 2 p. ; Polotsk State University. – Novopolotsk : PSU, 2010. – Issue 2. Part 2 : Technology. – P. 165 – 168.

16. Rakhanau K. Fast algorithm for estimating speech legibility by frequency-time processing of LFM-signal // European and National dimension in research : materials of junior researchers' conference, Novopolotsk, April 25 – 26, 2012 : 3 p. ; Polotsk State University. – Novopolotsk : PSU, 2012. – Issue 3. Part 3 : Technology. – P. 150 – 153.

Тезисы докладов на научных конференциях

17. Раханов, К.Я. Актуальность оценки защищенности аналоговой и цифровой речи / В.К. Железняк, К.Я. Раханов, Д.С. Рябенко // Интеллектуальные системы на транспорте : тез. докл. I междунар. науч.-практ. конф. «Интеллект Транс-2011» 24 – 26 марта 2011 г. – СПб. : Петерб. гос. ун-т путей и сообщения. – С. 73.

18. Раханов, К Я. Оценка разборчивости речи в каналах утечки информации методом ЛЧМ-сигнала программно-аппаратной системой // К.Я. Раханов, В.К. Железняк // Технические средства защиты информации : тез. докл. X белорус.-рос. науч.-техн. конф., Минск, 29 – 30 мая 2012 г. ; редкол. : Л.М. Лыньков (отв. ред.) [и др.]. – Минск : БГУИР, 2012. – С. 12 – 13.

Патенты

19. Способ определения максимальной разборчивости речи : пат. 15204 Респ. Беларусь, МПК G 10L 15/00 / В.К. Железняк, К.Я. Раханов ; заявитель Полоц. гос. ун-т. -- № a2010000 ; заявл. 04.01.2010 ; опубл. 30.12.2011 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2011. – № 6. – С. 164.

20. Устройство для определения разборчивости речи : пат. 15314 Респ. Беларусь, МПК G 10L 15/00, H 04R 29/00 / В.К. Железняк, К.Я. Раханов ; заявитель Полоц. гос. ун-т. – № a20100291 ; заявл. 01.03.2010 ; опубл. 28.02.2012 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2012. – № 1. – С. 162.

РЭЗЮМЭ

РАХАНАЎ Канстанцін Якаўлевіч

Шырокапалосная лінейна-частотная мадуляцыя сігналу для ацэнкі разборлівасці гаворкі ў каналах уцечкі інфармацыі

Ключавыя словы: разборлівасць гаворкі, праграмна-апаратны комплекс, канал уцечкі інфармацыі, шырокапалосная лінейна-частотная мадуляцыя сігналу, ацэнка абароненасці.

Мэта працы: тэарэтычнае абгрунтаванне і практычная рэалізацыя ацэнкі разборлівасці гаворкі з дапамогай шырокапалоснай лінейна-частотнай мадуляцыі сігналу ў каналах уцечкі інфармацыі з высокай дакладнасцю, адрознівальнай здольнасцю па частаце і гранічнай адчувальнасцю.

Метады даследавання і абсталяванне: імітацыйнае мадэляванне, лічбавая апрацоўка сігналу з шырокапалоснай лінейна-частотнай мадуляцыяй у шумах высокага ўзроўню выканана ў асяроддзі распрацоўкі Visual Studio 2008 на мовах праграмавання C++, C# з выкарыстаннем прынцыпаў аб'ектна-арыентаванага падыходу. Задача вызначэння адчувальнасці ацэнкі параметраў вымяральных сігналаў рашаецца метадамі дысперсійнага аналізу, а заданне колькаснага апісання – метадамі рэгрэсійнага аналізу. Даследаванне гранічных параметраў метаду сігналу з шырокапалоснай лінейна-частотнай мадуляцыяй і характарыстык праграмна-апаратнага комплексу «ЯРМАК» выканана з дапамогай аналагава-лічбавага пераўтваральніка L-Card E14-440.

Атрыманыя вынікі і іх навізна: абгрунтаваны і распрацаваны новы метад ацэнкі разборлівасці гаворкі з дапамогай сігналу з шырокапалоснай лінейна-частотнай мадуляцыяй, які дазволіў сінтэзаваць праграмна-апаратны комплекс, што павышае метадычную (тэарэтычную) дакладнасць ацэнкі, знижае гранічную адчувальнасць, павялічвае адрознівальную здольнасць па частаце ў параўнанні з вядомымі сродкамі ацэнкі абароненасці каналаў уцечкі маўленчай інфармацыі на аб'екце інфарматызацыі.

Ступень выкарыстання: вынікі даследаванняў ужыты ў праграмна-апаратным комплексе «ЯРМАК» для ацэнкі разборлівасці гаворкі ў каналах уцечкі інфармацыі (установа адукацыі «Полацкі дзяржаўны ўніверсітэт») і ў навучальным працэсе ўстановы адукацыі «Полацкі дзяржаўны ўніверсітэт».

Вобласць ужывання: ацэнка абароненасці маўленчай інфармацыі ў каналах уцечкі інфармацыі аб'ектаў інфарматызацыі.

РЕЗЮМЕ

РАХАНОВ Константин Яковлевич

Широкополосная линейно-частотная модуляция сигнала для оценки разборчивости речи в каналах утечки информации

Ключевые слова: разборчивость речи, программно-аппаратный комплекс, канал утечки информации, широкополосная линейно-частотная модуляция сигнала, оценка защищенности.

Цель работы: теоретическое обоснование и практическая реализация оценки разборчивости речи с помощью широкополосной линейно-частотной модуляции сигнала в каналах утечки информации с высокой точностью, разрешающей способностью по частоте и предельной чувствительностью.

Методы исследования и оборудование: имитационное моделирование, цифровая обработка сигнала с широкополосной линейно-частотной модуляцией в шумах высокого уровня выполнены в среде разработки Visual Studio 2008 на языках программирования C++, C# с использованием принципов объектно-ориентированного подхода. Задача установления чувствительности оценки параметров измерительных сигналов решается методами дисперсионного анализа, а задача количественного описания – методами регрессионного анализа. Исследование предельных параметров метода сигнала с широкополосной линейно-частотной модуляцией и характеристик программно-аппаратного комплекса «ЕРМАК» выполнено с помощью аналогово-цифрового преобразователя L-Card E14-440.

Полученные результаты и их новизна: обоснован и разработан новый метод оценки разборчивости речи с помощью сигнала с широкополосной линейно-частотной модуляцией, позволивший синтезировать программно-аппаратный комплекс, повышающий методическую (теоретическую) точность оценки, снизить предельную чувствительность и увеличить разрешающую способность по частоте в сравнении с известными средствами оценки защищенности каналов утечки речевой информации на объекте информатизации.

Степень использования: результаты исследований применены в программно-аппаратном комплексе «ЕРМАК» для оценки разборчивости речи в каналах утечки информации (учреждение образования «Полоцкий государственный университет») и в учебном процессе учреждения образования «Полоцкий государственный университет».

Область применения: оценка защищенности речевой информации в каналах утечки информации объектов информатизации.

SUMMARY

RAKHANAU Kanstantsin Yakaulevich

Broadband linear-frequency modulation of signal to assess speech intelligibility in the channels of information leakage

Keywords: speech intelligibility hardware and software system, the channel of information leakage, linear-frequency modulation of signal, security assessment.

Aim of the work: theoretical basis and practical implementation of evaluation of speech intelligibility using a broadband linear-frequency modulation of signal in the channels of information leakage with high precision, frequency resolution and limit sensitivity.

Research methods and equipment: simulation modeling, digital broadband linear-frequency modulation of signal in the noise made in a high-level development environment Visual Studio 2008 on the programming languages C++, C#, using the principles of object-oriented approach. The task of establishing the sensitivity of the parameter estimates measured signals solved by the methods of dispersion analysis, and a quantitative description of the problem – by regression analysis. Research limits for parameters of broadband linear-frequency modulation of signal and performance of hardware and software system "ERMAK" performed by the analog-to-digital converter L-Card E14-440.

The results obtained and their novelty: proved and developed a new method for estimating speech intelligibility using a broadband linear-frequency modulation of signal will synthesize hardware and software system that improves the methodical (theoretical) precision of the estimate, to reduce the sensitivity limit, increase the frequency resolution compared to conventional means security assessment leakage channels speech information on the subject of information.

Extent of usage: research results are applied in the software and hardware system "ERMAK" to assess speech intelligibility in the channels of information leakage (Educational Establishment "Polotsk State University") and in the educational process of the educational establishment "Polotsk State University".

Field of application: security assessment of the speech information in the channels of information leakage of information objects.

Научное издание

Константин Яковлевич
РАХАНОВ

ШИРОКОПОЛОСНАЯ ЛИНЕЙНО-ЧАСТОТНАЯ МОДУЛЯЦИЯ СИГНАЛА ДЛЯ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

Автореферат
диссертации на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Подписано в печать 04.03.2013.	Формат 60x84 $^1/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,63.
Уч.-изд. л. 1,4.	Тираж 60 экз.	Заказ 66.

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