УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 621.391.16; 621.372.037.372

РЯБЕНКО
Денис Сергеевич

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ КАНАЛОВ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ В ЦИФРОВОЙ ФОРМЕ ЧАСТОТНО-МАНИПУЛИРОВАННЫМ СИГНАЛОМ С НЕПРЕРЫВНОЙ ФАЗОЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

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

Минск 2014

Работа выполнена в учреждении образования «Полоцкий государственный университет».

Научный руководитель

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

Сидоренко Алевтина Васильевна,
доктор технических наук, профессор,
профессор кафедры физики и аэрокосмических технологий Белорусского государственного университета

Комликов Дмитрий Александрович,
кандидат технических наук,
начальник отдела государственного предприятия
«Научно-исследовательский институт
технической защиты информации»

Оппонирующая организация

Учреждение образования «Высший государственный колледж связи»

Защита состоится 25 сентября 2014 года в 16^{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.

КРАТКОЕ ВВЕДЕНИЕ

Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 года № 575, определено одно из приоритетных направлений национальной безопасности в информационной сфере «… разработка и внедрение современных методов и средств защиты информации в информационных системах» (п. 54).

Обусловленное высокой достоверностью предельное качество передачи речевых сигналов в цифровой форме обладает несомненными преимуществами перед аналоговыми сигналами. Взаимное преобразование аналоговых сигналов и сигналов в цифровой форме генерирует новые каналы утечки информации, что усложнило способы их защиты и разработки новых методов и средств оценки защищенности. Особенность канала утечки речевой информации в цифровой форме – его широкополосность, что усложняет извлечение достоверной информации.

Критерием оценки защищенности речевого сигнала в цифровой форме от утечки предложено и научно обосновано числовое значение вероятности ошибочного приема бита, соответствующее критерию оценки защищенности речевого сигнала в аналоговой форме – нормированному значению величины разборчивости речи, для которой разработаны современные методы и средства оценки. Многообразие представления битовых речевых сигналов в цифровой форме с основанием кода m и манипулированных речевых сигналов в цифровой форме обусловило выбор и необходимость обоснования измерительного сигнала, основными из требований к которому являются высокая помехоустойчивость и достоверность.

Решение научной задачи выбора и обоснования единого оптимального измерительного сигнала, методов оценки защищенности, критерия оценки защищенности по значению величины вероятности ошибочного приема бита с однозначно установленной числовой зависимостью от нормированного значения величины разборчивости речи, новых способов защиты речевых сигналов в аналоговой и цифровой формах определяет направление исследования.

На основании изложенного возникла необходимость теоретически обосновать и практически реализовать: научные методы оценки защищенности каналов утечки информации, представленной в цифровой форме; единый критерий численного значения величины разборчивости речи каналов утечки информации в цифровой форме; помехоустойчивые оптимальные измерительные сигналы для битовых и манипулированных речевых сигналов в цифровой форме; методы единого маскирования речевых сигналов в цифровой и аналоговой формах, 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» № 574 от 10 декабря 2010 года.

Работа выполнена инициативно в учреждении образования «Полоцкий государственный университет», является отдельным направлением развития 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 работы «Разработка и создание системы измерительной автоматизированной для измерения параметров низкочастотных магнитных излучений» № ГР 20081922. Результаты работы использованы при подготовке технического задания на ОКР по Государственной научно-технической программе «Защита информации 2», утвержденной Постановлением Совета Министров Республики Беларусь от 1 февраля 2011 года № 116.

Цель и задачи исследования

Цель диссертационной работы – обосновать единый критерий оценки величины разборчивости речи в цифровой и аналоговой формах; установить нормированное численное значение показателя оценки защищенности речевых сигналов в цифровой форме в виде вероятности ошибочного приема бита и зависимость от нее коэффициента разборчивости речи; обосновать помехоустойчивые измерительные сигналы для оценки защищенности каналов утечки информации в цифровой форме; сформировать маскирующий сигнал речевых сигналов в цифровой и аналоговой формах.

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

- проанализировать существующие методы оценки защищенности речевых сигналов в аналоговой и цифровой форме в каналах утечки в условиях воздействия преднамеренных помех;
- обосновать и разработать на новых принципах метод оценки нормированного значения защищенности речевых сигналов в аналоговой и

цифровой формах от утечки по техническим каналам, предложить и обосновать единый нормативный критерий, а также помехоустойчивый измерительный сигнал оценки защищенности речевых сигналов в цифровой форме от утечки информации;

- разработать модель оценки защищенности от утечки информации речевых сигналов в цифровой форме;

- разработать единый адаптивный маскирующий сигнал для аналоговых сигналов и сигналов в цифровой форме в каналах утечки информации, методы активной защиты маскирующими сигналами;

- исследовать и экспериментально определить предельные численные значения параметров и характеристик модели оценки защищенности от утечки речевых сигналов в цифровой форме.

Объектом исследования являются технические каналы утечки речевых сигналов в цифровой форме.

Предмет исследования – методы и средства оценки защищенности каналов утечки информации в аналоговой и цифровой формах.

Положения, выносимые на защиту

1. Способ оценки защищенности от утечки речевого сигнала в цифровой форме, реализуя в качестве критерия вероятность ошибочного приема бита, основанный на установлении ее математического соответствия с нормированным числовым значением разборчивости речи при приравнивании пропускных способностей речевых сигналов в аналоговой и цифровой формах двоичного симметричного канала утечки, что позволило установить единые нормативные требования к оценке защищенности речевых сигналов в аналоговой и цифровой форме и установить зависимость коэффициента разборчивости речи от вероятности ошибочного приема бита.

2. Метод оценки защищенности от утечки битовых речевых сигналов в цифровой форме применением измерительного сигнала в виде меандровой последовательности путем ее приема и обработки с использованием быстрого преобразования Фурье, синхронного накопления ее спектральных составляющих и обнуления шумовых для улучшения отношения сигнал/шум, восстановления меандровой последовательности обратным быстрым преобразованием Фурье, перемножения ее с последовательностью счетных импульсов и нормирования, что позволило снизить в 1000 раз порог чувствительности по критерию оценки защищенности от утечки речевого сигнала в цифровой форме с высокой помехоустойчивостью и точностью.

3. Метод оценки защищенности от утечки манипулированных речевых сигналов в цифровой форме применением частотно-манипулированного сигнала с непрерывной фазой, обработкой его с использованием быстрого

преобразования Фурье, накопления с превышением над уровнем шума его спектральных составляющих, их селекцией с оценкой и обнулением шумовых, формированием обратным быстрым преобразованием Фурье сигнала, нормированием и измерением его энергии и спектральной плотности мощности шума, сужением полосы измерительного сигнала, что позволило снизить более чем в 100 раз порог чувствительности по критерию оценки защищенности от утечки речевого сигнала в цифровой форме с высокой помехоустойчивостью и точностью.

4. Метод формирования маскирующего сигнала для речевых сигналов в цифровой и аналоговой формах, основанный на формировании из широкополосного шумового сигнала многоуровневой хаотической импульсной последовательности со спектральными характеристиками, адаптированными к речевым сигналам в цифровой форме, что повышает их защищенность не менее чем в 3 раза по сравнению с известными, повышает акустическую комфортность в 2 раза при снижении уровня акустического шума.

Личный вклад соискателя

В диссертации представлены результаты, которые отражают личный вклад автора. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертационной работе результатов. Автор принимал непосредственное участие в разработке методик, проведении исследований, анализе полученных результатов и подготовке публикаций, научных сообщений на конференциях и заявок на изобретения.

Личный вклад соискателя состоит в разработке метода теоретического обоснования критерия и показателя оценки защищенности от утечки речевого сигнала в цифровой форме, а также метода оценки защищенности от утечки битовых речевых сигналов в цифровой форме с использованием измерительного сигнала в виде меандровой последовательности и метода оценки защищенности от утечки манипулированных речевых сигналов в цифровой форме с использованием измерительного сигнала в виде частотно-манипулированного сигнала с непрерывной фазой по единому для аналоговых и цифровых сигналов критерию, нормированному показателю оценки защищенности, в подготовке и проведении экспериментов по исследованию факторов, влияющих на методическую точность оценки параметров сигналов.

Определение целей и задач исследований, достижение и обобщение полученных результатов проводилось совместно с научным руководителем доктором технических наук, профессором В. К. Железняком. Им же предложена тема диссертационного исследования.

Апробация результатов диссертации

Материалы, вошедшие в диссертационную работу, докладывались и обсуждались: на V и VI международных конференциях-форумах «Информационные системы и технологии (IST)» (Минск, Беларусь, 2009 и 2010 гг.); I, III и V Junior researchers' conference (Новополоцк, Беларусь, 2009, 2011 и 2013 гг.); первой и третьей международных научно-практических конференциях «Интеллектуальные системы на транспорте» (Санкт-Петербург, Россия, 2011, 2013 гг.); XVI, XVII и XVIII научно-практических конференциях «Комплексная защита информации» (Гродно, Беларусь, 2011 г.; Суздаль, Россия, 2012 г.; Брест, Беларусь, 2013 г.); XI Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Беларусь, 2013 г.); 70-й научной конференции студентов и аспирантов БГУ (Минск, Беларусь, 2013 г.); XVIII международной научно-технической конференции «Современные средства связи» (Минск, Беларусь, 2013 г.); X международной научно-практической конференции «Управление информационными ресурсами» (Минск, Беларусь, 2013 г.); V ежегодном научно-практическом семинаре «Применение современных информационных технологий с учетом особенностей сетецентрических подходов к военным действиям» (Минск, Беларусь, 2014 г.); республиканском научном семинаре «Математическое моделирование сложных систем, анализ данных и защита информации» (Минск, Беларусь, 2014 г.); Международной научно-технической конференции, приуроченной к 50-летию МРТИ–БГУИР (Минск, Беларусь, 2014 г.).

Опубликованность результатов диссертации

Материалы по теме диссертации опубликованы в 9 статьях в рецензируемых научных журналах. Общий объем публикаций по теме диссертации, соответствующих п. 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, составляет 2,83 авторских листа. Опубликовано 11 статей в сборниках материалов международных конференций, семинаров, 5 тезисов докладов в сборниках тезисов конференций и семинаров, получено 2 патента Республики Беларусь на изобретение, которые внесены в перечень перспективных, получено 4 положительных решения о выдаче патента на изобретение.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, пяти глав с выводами по каждой главе, заключения, библиографического списка и приложений. Общий объем диссертационной работы составляет 123 страницы, включая 90 страниц машинописного текста, 67 иллюстраций на 22 страницах, библиографический список из 135 наименований, из них 31 публикация автора.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** и в общей характеристике диссертационной работы обоснована актуальность темы диссертации, определено основное направление исследований, определены научные цели и задачи исследования, обоснована необходимость исследований методов оценки защищенности от утечки речевых сигналов в цифровой форме в каналах утечки информации, выбора единого оптимального критерия защищенности и измерительного сигнала для оценки защищенности информации в канале ее утечки.

В **первой главе** представлены характеристики каналов утечки речевых сигналов в цифровой форме. При преобразовании электрических аналоговых речевых сигналов в речевые сигналы в цифровой форме с постоянными параметрами и аддитивной помехой типа белого гауссова шума в канале утечки информации возникают сигналы и наводки на несимметричные цепи и паразитная модуляция генераторов. Преобразование речевых сигналов в цифровой форме в аналоговые речевые сигналы сопровождается излучением наведенных манипулированных сигналов на высокочастотные колебания с гармониками частот дискретизации.

Особенностью каналов утечки речевых сигналов в цифровой форме является их широкополосность, несимметричность и высокий уровень шумов, влияющих на выбор измерительного сигнала.

Анализируются факторы, определяющие вероятность ошибочного приема бита в канале утечки информации.

Проанализированы ФМн-, ЧМн-, АМн-, ОФМ-, КАМ-сигналы, которые могут быть реализованы в качестве измерительных для оценки защищенности от утечки речевых сигналов в цифровой форме.

Проанализировано противоречие между возможностью оценки достоверности цифровой информации в каналах передачи и необходимостью оценки вероятности ошибочного приема бита в каналах утечки, приближенной к пределу Шеннона и скорости передачи информации.

Из анализа литературных источников следует вывод, что современные методы оценки передачи информации исследованы только для цифровых каналов связи. Такие методы не могут быть применены для каналов утечки речевых сигналов в цифровой форме, основной особенностью которых является вероятность ошибочного приема бита, близкая к пределу Шеннона. Это обусловливает разработку на новых принципах единых высокопроизводительных методов оценки защищенности каналов утечки речевой информации в цифровой форме по единому критерию и показателю

оценки защищенности для аналоговых речевых сигналов и речевых сигналов в цифровой форме.

Во **второй главе** впервые предложен способ оценки защищенности от утечки речевого сигнала в цифровой форме, реализуя в качестве критерия вероятность ошибочного приема бита $p_{ош}$ для двоичных и m-ичных сигналов, основанный на установлении ее математического соответствия с нормированным числовым значением разборчивости речи при приравнивании пропускных способностей речевых сигналов в аналоговой и цифровой формах двоичного симметричного канала утечки, что позволило установить единые нормативные требования к оценке защищенности речевых сигналов в аналоговой и цифровой форме.

Критерий оценки защищенности от утечки речевого сигнала в цифровой форме должен адекватно соответствовать критерию оценки защищенности от утечки аналогового речевого сигнала. Предложено критерий оценки защищенности речевого сигнала в цифровой форме установить по вероятности ошибочного приема бита $p_{ош}$, приведенной к информационному показателю нормированной величины разборчивости речи.

С использованием формулы Шеннона для отношения сигнал/шум определена пропускная способность аналогового речевого сигнала:

$$C_{а} = F \log\left(1 + P_{с} / P_{ш}\right), \text{ бит/с.} \qquad (1)$$

Как следует из формулы (1), пропускная способность гауссова канала $C_{а}$ определяется шириной полосы сигнала F (Гц), отношением мощности сигнала $P_{с}$ (Вт) к мощности шума $P_{ш}$ (Вт). Данное отношение установлено для нормированной величины разборчивости речи.

Известно, что при малом отношении сигнал/шум $P_{с} < P_{ш}$ для аналогового сигнала из формулы Шеннона значение пропускной способности определяется

$$C_{а} = F \log_{2} e \cdot \frac{P_{с}}{P_{ш}} = 1{,}443 \cdot F \cdot \frac{P_{с}}{P_{ш}} = 1{,}443 \frac{P_{с}}{N_{0}} = 1{,}443\Delta, \qquad (2)$$

где $C_{а}$ – пропускная способность канала, бит/с; F – ширина полосы частот, Гц; $P_{с}/P_{ш}$ – отношение мощности сигнала $P_{с}$ к мощности шума $P_{ш}$ для аналогового речевого сигнала; $P_{с}/N_{0} = \Delta$ – нормативное значение отношения мощности речевого сигнала $P_{с}$ к спектральной плотности мощности шума N_{0}.

Нормативным значением отношения мощности сигнала $P_{с}$ к спектральной плотности мощности шума N_{0} установлен нормированный показатель разборчивости речи.

Для двоичного симметричного дискретного канала пропускная способность канала $C_ц$ при ее равенстве максимальной скорости передачи информации R_{max} вычисляется следующим образом:

$$C_ц = R_{макс} = 1 + p_{ош}\log_2 p_{ош} + (1 - p_{ош})\log_2(1 - p_{ош}), \text{ бит/с.} \quad (3)$$

При равенстве $C_ц = C_а$ из формулы (3) вычисляют вероятность ошибочного приема бита $p_{ош}$ в зависимости от нормативного значения отношения Δ мощности сигнала $P_с$ к спектральной плотности мощности шума N_0. Нормативным значением оценки защищенности речевых сигналов в цифровой форме следует принять величину вероятности ошибочного приема бита $p_{ош}$, соответствующую нормированному показателю разборчивости речи.

Аналогично двоичному симметричному каналу нормативное значение ошибочного приема бита $p_{ош}$ для m-ичных сигналов определяется из установленного равенства пропускной способности аналогового $C_а$ и речевого сигнала в цифровой форме $C_ц$, определяемого из формулы

$$C_ц = \nu\left[\log_2 m + p_{ош}\log_2\frac{p_{ош}}{m-1} + (1 - p_{ош})\log_2(1 - p_{ош})\right], \text{ бит/с,} \quad (4)$$

где ν – скорость передачи символа, бит/с.

Построена графическая зависимость коэффициента разборчивости аналогового речевого сигнала от вероятности ошибочного приема бита $p_{ош}$ (рисунок 1). Корреляционная теория разборчивости речи по отношению сигнал/шум по мощности позволила получить расчетное численное значение величины разборчивости речи в автоматизированном режиме с помощью СИА (ПАК).

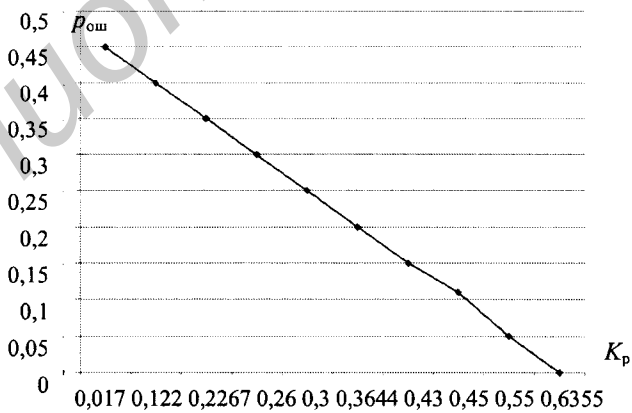

Рисунок 1 – Зависимость коэффициента разборчивости речи $K_р$ от вероятности ошибочного приема бита $p_{ош}$

Предложен научный способ оценки защищенности от утечки речевого сигнала в цифровой форме, реализуя в качестве критерия вероятность ошибочного приема бита $p_{ош}$ для двоичных и m-ичных сигналов, основанный на установлении ее математического соответствия с нормированным числовым значением разборчивости речи при приравнивании пропускных способностей речевых сигналов в аналоговой и цифровой формах двоичного симметричного канала утечки, что позволило установить единые нормативные требования к оценке защищенности речевых сигналов в аналоговой и цифровой форме. Нормированный показатель критерия оценки защищенности речевого сигнала в цифровой форме устанавливает возможность оценки защищенности битовых и манипулированных речевых сигналов в цифровой форме в канале утечки.

В **третьей главе** предложен принципиально новый метод оценки защищенности от утечки битовых речевых сигналов в цифровой форме.

Принцип метода заключается в применении помехоустойчивого измерительного сигнала в виде меандровой последовательности N прямоугольных с одинаковыми энергиями импульсов длительностью τ и периодом $T = 2\tau$, подаче его на вход системы передачи информации, приеме и выделении из полей рассеивания передаваемого сигнала, обработке быстрым преобразованием Фурье (БПФ), n-разовым синхронным накоплением ее спектральных составляющих и обнулением шумовых с улучшением отношения сигнал/шум в $\sqrt{n}$ и l раз, восстановлением меандровой последовательности обратным быстрым преобразованием Фурье (ОБПФ), h-кратным их перемножением со сформированной последовательностью счетных импульсов для улучшения в h раз отношения сигнал/шум, вычислении энергии сформированного счетного импульса $E_c = P_c \cdot \tau$ и спектральной плотности мощности шума N_0, определении отношения E_c/N_0 и величины вероятности ошибочного приема бита по зависимости $p_{ош} = f(E_c/N_0)$, сравнении нормированного значения вероятности ошибочного приема бита $p_{ош}$ со значением вероятности ошибочного приема бита для двоичных или m-ичных сигналов.

Получив численное значение вероятности ошибочного приема бита по зависимости $p_{ош} = f(E_c/N_0)$ для битовых речевых сигналов в цифровой форме, принимается решение о незащищенности $p_{ош.\ норм} < p_{ош.\ ц}$ или о защищенности $p_{ош.\ норм} > p_{ош.\ ц}$ от утечки по критерию оценки защищенности от утечки речевого сигнала в цифровой форме. Устанавливается зависимость $K_р = f(p_{ош})$.

Разработан и обоснован метод оценки защищенности от утечки битовых речевых сигналов в цифровой форме с основанием кода m. Метод основан на подаче через систему передачи информации измерительного сигнала в виде меандровой последовательности, оценке параметров такого сигнала в канале

утечки речевого сигнала в цифровой форме и принятии решения о незащищенности или о защищенности речевых сигналов по критерию и его показателю оценки защищенности от утечки речевого сигнала в цифровой форме.

Применение предложенной обработки обоснованного измерительного сигнала в методе оценки защищенности от утечки битовых речевых сигналов в цифровой форме позволило получить новые качественные результаты по выделению измерительного сигнала в канале утечки информации, сократить время измерений за счет единого измерительного сигнала, улучшить отношение сигнал/шум, повысить разрешающую способность и точность принятия решения по критерию оценки защищенности от утечки речевого сигнала в цифровой форме, снизить порог чувствительности в $\left(\sqrt{n}\cdot l\right)^h \approx 1000$ раз (n – количество накоплений измерительного сигнала при его обработке; l – коэффициент, определяющий снижение порога чувствительности при обнулении шумовых составляющих спектра; h – степенной показатель, определяющий снижение порога чувствительности путем перемножения меандровой последовательности с серией счетных импульсов).

В **четвертой главе** предложен метод оценки защищенности от утечки манипулированных речевых сигналов в цифровой форме частотно-манипулированным сигналом с непрерывной фазой.

Во-первых, каналы утечки информации несимметричны. Во-вторых, двоичный ФМн-сигнал только симметричный. Помехоустойчивость m-ичного ФМн-сигнала снижается пропорционально числу битов на символ $k = \log_2 m$, где m – набор символов. При этом помехоустойчивость ортогонального m-ичного сигнала повышается. Кроме того, из известных ортогональных наборов сигналов значительными преимуществами обладает квадратурный частотно-манипулированный сигнал с непрерывной фазой для оценки параметров сигнала в несимметричных каналах утечки информации.

Показано преимущество измерительного частотно-манипулированного сигнала с непрерывной фазой по сравнению с другими вариантами манипулированных сигналов для оценки параметров канала утечки речевого сигнала в цифровой форме, заключающееся в его высокой помехоустойчивости и узкополосности.

Частотно-манипулированный сигнал с непрерывной фазой подают на вход системы передачи информации. В канале утечки информации извлекают смесь измерительного сигнала и шума, которую обрабатывают путем БПФ, n-кратно накапливают спектральные составляющие сигнала и шума до уровня $S_с > S_ш$, селективно выделяют спектральные составляющие сигнала, при этом обнуляют

спектральные составляющие шума с улучшением отношения сигнал/шум в l раз и сужением полосы измерительного сигнала в k раз. Исходный сигнал формируют ОБПФ, измеряют его параметры и спектральную плотность мощности шума, определяют вероятность ошибочного приема бита для некогерентного детектирования. Общее выражение для вероятности ошибочного приема бита определяется согласно выражению

$$p_{\text{ош}} = 0,5 \exp\left(-0,5 \frac{E_c}{N_0}\right), \quad (5)$$

где E_c/N_0 – отношение энергии символа к спектральной плотности мощности шума.

Получив численное значение вероятности ошибочного приема бита по зависимости $p_{\text{ош}} = f(E_c/N_0)$ для манипулированных речевых сигналов в цифровой форме, принимается решение о незащищенности $p_{\text{ош. норм}} < p_{\text{ош. ц}}$ или о защищенности $p_{\text{ош. норм}} > p_{\text{ош. ц}}$ от утечки по критерию оценки защищенности от утечки речевого сигнала в цифровой форме. Устанавливается зависимость $K_{\text{р}} = f(p_{\text{ош}})$.

Разработан и обоснован новый метод оценки защищенности от утечки манипулированных речевых сигналов в цифровой форме частотно-манипулированным сигналом с непрерывной фазой. Метод основан на подаче через систему передачи информации частотно-манипулированного сигнала с непрерывной фазой, оценке параметров такого сигнала в канале утечки речевого сигнала в цифровой форме и принятии решения о незащищенности или о защищенности речевого сигнала по обоснованному единому нормативному критерию и его показателю оценки защищенности от утечки речевого сигнала в цифровой форме. Применение частотно-манипулированного сигнала с непрерывной фазой позволило сузить полосу измерительного сигнала в 2 раза, повысить помехоустойчивость измерительного сигнала в канале утечки информации в шумах высокого уровня. Улучшение отношения сигнал/шум при предложенной обработке позволило повысить разрешающую способность и точность принятия решения по критерию оценки защищенности от утечки речевого сигнала в цифровой форме, снизить порог чувствительности в $\sqrt{n \cdot l \cdot k} \geq 100$ раз (n – количество накоплений измерительного сигнала; l – достигнутое улучшение при обнулении шумовых составляющих спектра; k – показатель улучшения обработки сигнала за счет уменьшения полосы измерительного сигнала).

В **пятой главе** разработан метод формирования многоуровнего маскирующего сигнала для аналоговых речевых сигналов и речевых сигналов в

цифровой форме. Суть метода заключается в формировании многоуровневых хаотических импульсных последовательностей (ХИП), параметры которых адаптированы к параметрам маскируемых сигналов.

Метод реализуют следующим образом. Генерируют белый широкополосный шумовой сигнал. Сгенерированный белый широкополосный шумовой сигнал усиливают и фильтруют для ограничения сигнала по используемой полосе. Из усиленного отфильтрованного белого широкополосного шумового сигнала формируют многоуровневые случайные по длительностям и паузам между ними ХИП. Для этого из ХИП на нулевом пороговом уровне положительной и отрицательной полярности с амплитудами $+U$ и $-U$ формируют n положительных и n отрицательных пороговых уровней с шагом U/n и значениями k-го уровня: $U_k = U(n-k)/nk$, где $k=\overline{1,n-1}$.

При этом второй дискретный импульсно-опорный уровень формируют из амплитуд импульсов ХИП, сформированных на первом уровне, далее каждый последующий $(n-1)$ уровень формируют из импульсов ХИП предшествующего $(n-2)$ уровня. Формирование ХИП осуществляют путем превышения «по модулю» положительных и отрицательных значений амплитуд шумового широкополосного сигнала в момент времени совпадения с полученными дискретными импульсно-опорными уровнями амплитуд. В момент пересечения данных уровней амплитуд нарастающей амплитудой шумового сигнала формируют подъем импульса, убывающей амплитудой шумового сигнала – спад импульса. Длительность импульса равна времени превышения амплитуды широкополосного шумового сигнала каждого из дискретных импульсно-опорных уровней амплитуд. Сформированные ряды ХИП суммируют, масштабируют их по амплитуде, получая многоуровневый сигнал ХИП для маскирования аналоговых речевых сигналов, речевых сигналов в цифровой форме, видеосигналов и сигналов передачи данных.

Экспериментальная оценка параметров маскирующего сигнала, полученного с помощью генератора шума, построенного на шумовых диодах серии ND 100, показала следующие результаты:

- энтропийный коэффициент качества шумового сигнала – не менее 0,95;
- пик-фактор шумового сигнала – не менее 3;
- распределение плотности вероятности шума подчинено закону Гаусса (показано с использованием критерия согласия γ^2 при уровне значимости 0,05);
- среднеквадратичная частота шумового сигнала (автокорреляционная функция и среднеквадратичная частота характеризуют отсутствие гармонических составляющих в спектре);

- спектральная плотность мощности шумового сигнала экспоненциальна в заявленных диапазонах частот;

- обобщенная автокорреляционная функция шумового сигнала имеет вид, показанный на рисунке 2.

В результате исследования шумового сигнала выявлены его особенности:

- высокая устойчивость метрологических параметров и характеристик, контролепригодность параметров;

- предложенный шумовой сигнал превосходит известные ранее по ряду параметров (уровень излучения, неравномерность амплитудно-частотных характеристик в рабочем диапазоне частот, разброс характеристик при воздействующих факторах);

- энтропийный коэффициент качества шума как основной параметр приближается к единице.

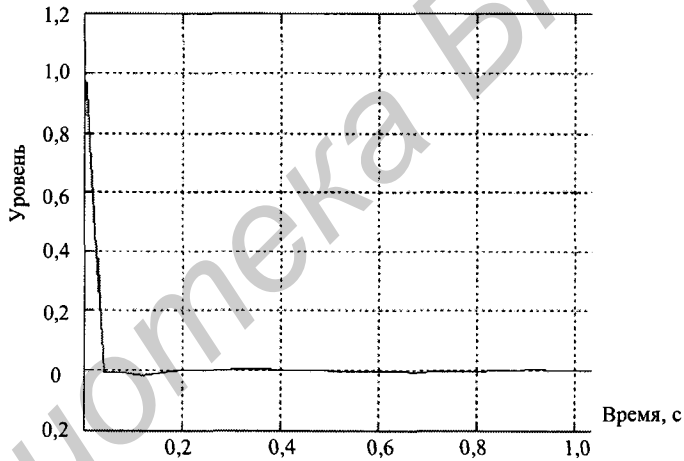

Рисунок 2 – Обобщенная автокорреляционная функция шумового сигнала

Проведена экспериментальная оценка защищенности от утечки речевого сигнала в цифровой форме, включающая реализацию метода оценки защищенности битового речевого сигнала в цифровой форме с основанием кода m с использованием измерительного сигнала в виде меандровой последовательности и манипулированного речевого сигнала в цифровой форме с использованием измерительного сигнала в виде частотно-манипулированного сигнала с непрерывной фазой по единому критерию оценки и

его показателю защищенности для аналоговых речевых сигналов и речевых сигналов в цифровой форме.

Разработанный метод формирования маскирующего сигнала позволил маскировать аналоговые речевые сигналы и речевые сигналы в цифровой форме, а также маскировать видеосигналы, сигналы звукового сопровождения видео и сигналы передачи данных, сократить количество генераторов маскирующих сигналов минимум в 2 раза, повысить адаптивность маскируемого и маскирующего сигналов и снизить уровень шумового излучения не менее чем в 3 раза. Кроме того, предложенный маскирующий сигнал повышает защищенность аналоговых и цифровых сигналов не менее чем в 3 раза по сравнению с известными маскирующими сигналами, повышает акустическую комфортность в 2 раза снижением уровня акустического шума.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Благодаря речевому сигналу, для которого разработаны научно обоснованные нормативные требования его защищенности, предложен способ оценки защищенности от утечки речевого сигнала в цифровой форме [2, 12, 13, 21], что позволило установить единые нормативные требования к оценке защищенности речевых сигналов в аналоговой и цифровой форме и установить зависимость величины коэффициента разборчивости речи от вероятности ошибочного приема бита [7, 10, 11, 25]. Суть способа заключается в использовании известного равенства отношения спектральной плотности мощности сигнала к спектральной плотности мощности шума и отношения энергии бита к спектральной плотности мощности шума, умноженной на битовую скорость. Это позволило в автоматизированном режиме получить численное значение вероятности ошибочного приема бита, зависящее от коэффициента разборчивости речи [26, 27].

2. Предложен метод оценки защищенности от утечки битовых речевых сигналов в цифровой форме с применением помехоустойчивого измерительного сигнала в виде меандровой последовательности, подачи ее на вход системы передачи информации, ее приема и выделения из полей рассеивания передаваемого сигнала обработкой БПФ, синхронным накоплением ее спектральных составляющих и обнулением шумовых для улучшения отношения сигнал/шум, восстановления ОБПФ, перемножением ее с последовательностью счетных импульсов и нормированием [6, 16, 19, 20].

Решение о защищенности принимают по критерию оценки защищенности от утечки речевого сигнала в цифровой форме.

Получены новые качественные результаты по выделению измерительного сигнала из канала утечки информации, сокращению времени измерений, улучшению отношения сигнал/шум и повышению точности принятия решения со снижением порога чувствительности более чем в 1000 раз.

3. Предложен метод оценки защищенности от утечки манипулированных речевых сигналов в цифровой форме, основанный на формировании измерительного сигнала в виде частотно-манипулированного сигнала с непрерывной фазой [3, 4, 5, 9, 14, 18, 22]. Измерительный сигнал принимается и обрабатывается путем БПФ в смеси с шумом, накопления спектральных составляющих сигнала и шума до уровня превышения сигнала над шумом, селективного выделения спектральных составляющих сигнала, обнуления спектральных составляющих шума с улучшением отношения сигнал/шум, восстановления исходного сигнала ОБПФ, нормирования, измерения параметров некогерентного детектирования и спектральной плотности мощности шума. Такая обработка позволила определить вероятность ошибочного приема бита для некогерентного сигнала, принять решение о защищенности от утечки речевого сигнала в цифровой форме. Применение частотно-манипулированного сигнала с непрерывной фазой позволило сузить полосу измерительного сигнала в 2 раза по сравнению с другими сигналами. Увеличение отношения сигнал/шум при предложенной обработке позволило снизить порог чувствительности не менее чем в 100 раз.

Выбор единого измерительного сигнала, критерия оценки и численного значения показателя защищенности повысил чувствительность и достоверность и снизил методическую погрешность оценки.

4. Разработан и обоснован единый метод формирования единого маскирующего сигнала для аналоговых речевых сигналов и речевых сигналов в цифровой форме, основанный на использовании белого гауссова широкополосного шумового сигнала для формирования многоуровневых случайных по длительностям и паузам между ними ХИП [15, 17, 24], что позволяет маскировать аналоговые речевые сигналы и речевые сигналы в цифровой форме, повышая их защищенность не менее чем в 3 раза, а также маскировать видеосигналы, сигналы звукового сопровождения видео, сигналы передачи данных [8, 23, 24, 28, 29]. Метод позволил повысить адаптивность маскируемого и маскирующего сигналов и снизить уровень шумового излучения не менее чем в 3 раза за счет сформированной рациональной АЧХ спектра ХИП по экспоненциальному закону в соответствии с АЧХ спектра маскируемых сигналов.

Рекомендации по практическому использованию результатов

1. Применение обоснованного нормированного показателя оценки защищенности от утечки речевого сигнала в виде вероятности ошибочного приема бита, зависящей от численного значения величины разборчивости речи, помехоустойчивых оптимальных измерительных сигналов, обеспечило снижение порога чувствительности с высокой помехоустойчивостью и точностью при преобразовании речевого сигнала из аналоговой формы в цифровую, передаче его в цифровой форме по системам передачи, а также при дальнейшем обратном преобразовании из цифровой формы в аналоговую [1, 2, 6, 26, 27].

2. Разработанные методы оценки защищенности от утечки речевого сигнала в цифровой форме на базе научно обоснованного нормативного показателя защищенности, помехоустойчивых измерительных сигналов оценки защищенности [4, 5, 6, 9, 18] являются дальнейшим направлением развития и модернизации программно-аппаратного комплекса «Ермак», который в настоящее время оценивает защищенность от утечки речевого сигнала.

3. Маскирование аналоговых речевых сигналов, речевых сигналов в цифровой форме, видеосигналов, сигналов звукового сопровождения видео и сигналов передачи данных возможно при применении разработанного метода формирования маскирующего сигнала, основанного на формировании многоуровневой хаотической импульсной последовательности из широкополосного шумового сигнала [8, 28, 29, 30, 31].

4. Предложенные методы оценки защищенности от утечки речевых сигналов в цифровой форме рекомендуется использовать для контроля в технических каналах утечки речевой информации при маскировании информационных сигналов, а также в учебном процессе УО «Полоцкий государственный университет» при проведении занятий по дисциплинам «Методы и средства защиты речевой и видеоинформации», «Технические средства и методы защиты информации».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных журналах

1. Рябенко, Д.С. Метод оценки защищенности информации, преобразованной в цифровую форму / Д.С. Рябенко, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2012. – № 12. – С. 12–19.

2. Рябенко, Д.С. Некоторые вопросы оценки защищенности информации, преобразованной в цифровую форму / Д.С. Рябенко, В.К. Железняк // Безопасность информационных технологий. «Комплексная защита информации-XVII». – 2012. – № 1. – С. 92–94.

3. Демодулятор сигналов относительной фазовой манипуляции с адаптивным порогом принятия решения / С.В. Дворников, В.В. Борисов, А.Г. Москалец, Е.В. Казаков, А.В. Железняк, Д.С. Рябенко // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2013. – № 4. – С. 18–21.

4. Рябенко, Д.С. Обоснование оптимального сигнала для оценки защищенности цифровых каналов утечки информации / Д.С. Рябенко, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2013. – № 12. – С. 2–8.

5. Рябенко, Д.С. Оценка защищенности цифровых сигналов АМ, ЧМ, ФМ, КАМ в каналах утечки информации / Д.С. Рябенко, В.К. Железняк // Электроника инфо. – 2013. – № 6. – С. 208–212.

6. Рябенко, Д.С. Оценка защищенности от утечки битовых символов при передаче речевых сигналов в цифровой форме / Д.С. Рябенко, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2014. – № 4 – С. 88–93.

7. Методика трансформации сигнальных созвездий сигналов КАМ / С.В. Дворников, А.В. Пшеничников, С.С. Дворников, Д.А. Бурыкин, А.В. Железняк, Д.С. Рябенко // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2014. – № 4. – С. 39–44.

8. Рябенко, Д.С. Формирование хаотических импульсных последовательностей для маскирования информационных сигналов / Д.С. Рябенко, В.К. Железняк // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2014. – № 4. – С. 67–71.

9. Рябенко, Д.С. Метод сигнала ортогональной частотной манипуляции без разрыва фазы для оценки защищенности от утечки речевых сигналов в цифровой форме / Д.С. Рябенко, В.К. Железняк // Докл. БГУИР. – 2014. – № 3(81). – С. 45–50.

Статьи в сборниках материалов конференций и семинаров

10. Rabenka, D. Assessment criterion of the information channel and induced signal in adjacent channel / D. Rabenka, V. Zheleznyak // European and National dimension in research : materials of junior researchers' conference, Novopolotsk, April 22–23, 2009 / Polotsk State University ; publishing board : D. Lazovski [etc]. – Novopolotsk, 2009. – Issue 1. – P. 280–283.

11. Рябенко, Д.С. Информационные показатели, гарантирующие защищенность цифровой речи / Д.С. Рябенко, В.К. Железняк // Информационные системы и технологии (IST 2009) : материалы V междунар. конф.-форума, Минск, 16–17 нояб. 2009 г. : в 2 ч. ; редкол. Н.И. Листопад [и др.]. – Ч. 2. – Минск : Издатель А.Н. Вараксин, 2009. – С. 50–51.

12. Рябенко, Д.С. Анализ инструментальных методов оценки защищенности цифровых каналов утечки речевой информации / Д.С. Рябенко, 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. 88–92.

13. Rabenka, D. The analysis of tool methods of estimation of digital channels security from speech information leak / D. Rabenka // European and National dimension in research : materials of junior researchers' conference, Novopolotsk, April 27–28, 2011 : 3 p. / Polotsk State University ; publishing board : D. Lazovski [etc]. – Novopolotsk, 2011. – Issue 3. Part 1 : Technology. – P. 126–128.

14. Рябенко, Д.С. Анализ измерительных сигналов для оценки защищенности аналоговой и цифровой речи / Д.С. Рябенко, 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.

15. Рябенко, Д.С. Методика оценки для оперативного контроля источников шумового сигнала / Д.С. Рябенко, К.Я. Раханов, В.К. Железняк, В.В. Буслюк, С.И. Ворончук, И.В. Лешкевич, С.С. Дереченник // 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.

16. Rabenka, D. Choice of the optimum signal for the estimation of security of digital channels of information leakage / D. Rabenka, V. Zheleznyak // European and National dimension in research : materials of junior researchers' conference, Novopolotsk, April 24–25, 2013. : 3 p. / Polotsk State University ; publishing board : D. Lazovski [etc]. – Novopolotsk, 2013. – Issue 5. Part 3 : Technology. – P. 230–232.

17. Рябенко, Д.С. Применение хаотических импульсных последовательностей для маскирования аналоговых и цифровых речевых

сигналов / Д.С. Рябенко, В.К. Железняк // Современные средства связи : материалы XVIII междунар. науч.-техн. конф., Минск, 15–16 окт. 2013 г. ; редкол. А.О. Зеневич [и др.]. – Минск : УО ВГКС, 2013. – С. 207–208.

18. Рябенко, Д.С. Метод сигнала ортогональной частотной манипуляции без разрыва фазы для оценки защищенности от утечки цифровых модулированных сигналов / Д.С. Рябенко, В.К. Железняк // Управление информационными ресурсами : материалы X междунар. науч.-практ. конф., Минск, 13 дек. 2013 г. ; / редкол. : А.В. Ивановский, А.И. Шемаров, Б.В. Новыш. – Минск : Акад. упр. при Президенте Респ. Беларусь, 2013. – С. 134–135.

19. Рябенко, Д.С. Оценка защищенности от утечки битовых символов при передаче цифровой речевой информации / Д.С. Рябенко, В.К. Железняк // Управление информационными ресурсами : материалы X междунар. науч.-практ. конф., Минск, 13 дек. 2013 г. ; редкол. : А.В. Ивановский, А.И. Шемаров, Б.В. Новыш. – Минск : Акад. упр. при Президенте Респ. Беларусь, 2013. – С. 132-133.

20. Рябенко, Д.С. Измерительные сигналы для оценки защищенности речи в цифровой форме / Д.С. Рябенко, В.К Железняк // Международная научно-техническая конференция, приуроченная к 50-летию МРТИ–БГУИР (Минск, 18–19 марта 2014 года) : материалы конф. в 2 ч. ч. 1. Секция защита информации, специальных и биологических объектов / редкол. : А.А. Кураев [и др.]. – Минск : БГУИР, 2014. – С. 424–425.

Тезисы докладов на научных конференциях

21. Рябенко, Д.С. 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.

22. Рябенко, Д.С. Обоснование оптимального сигнала для оценки защищенности цифровых каналов утечки информации / В.К. Железняк, Д.С. Рябенко // Интеллектуальные системы на транспорте : тез. докл. III междунар. науч.-практ. конф. «Интеллект Транс-2013» 3–5 апреля 2013 г. – СПб. : Петерб. гос. ун-т путей и сообщения. – С. 65.

23. Рябенко, Д.С. Подавление цифровых каналов утечки информации / Д.С. Рябенко, В.К. Железняк // Технические средства защиты информации : тез. докл. XI белорус.-рос. науч.-техн. конф., Минск, 5–6 июня 2013 г. ; редкол. : Л.М. Лыньков (отв. ред.) [и др.]. – Минск : БГУИР, 2013. – С. 31.

24. Рябенко, Д.С. Формирование многоуровневой хаотической импульсной последовательности для маскирования сигналов / Д.С. Рябенко,

В.К. Железняк // Применение современных информационных технологий с учетом особенностей сетецентрических подходов к военным действиям : тез. докл. V науч.-практ. семинара, Минск, 29 января 2014 г. – Минск : ВА РБ, 2014. – С. 15–18.

25. Рябенко, Д.С. Критерий оценки защищенности преобразованных в цифровую форму речевых сигналов / Д.С. Рябенко, В.К. Железняк // Применение современных информационных технологий с учетом особенностей сетецентрических подходов к военным действиям : тез. докл. V науч.-практ. семинара, Минск, 29 января 2014 г. – Минск : ВА РБ, 2014. – С. 14–15.

Патенты

26. Способ оценки защищенности от утечки речевого сигнала : пат. 15588 Респ. Беларусь, МПК G 10L 15/00, H 04R 29/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20100293 ; заявл. 01.03.2010; опубл. 30.04.2012 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2011. – № 2 (85). – С. 165–166.

27. Способ оценки защищенности информации от утечки при ее передаче в цифровой форме : пат. 16924 Респ. Беларусь, МПК H 04R 29/00, G 10L 15/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20110504 ; заявл. 18.04.2011 ; опубл. 30.04.2013 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2013. – № 2(91). – С. 146.

28. Генератор маскирующих сигналов : МПК H 04R 29/00, G 10L 15/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20120050 ; заявл. 16.01.2012 ; 18.02.2014 получено решение о выдаче патента.

29. Способ формирования маскирующей помехи : МПК H 04R 29/00, G 10L 15/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20120051 ; заявл. 16.01.2012 ; 27.02.2014 получено решение о выдаче патента.

30. Способ формирования сигнала для маскирования речевых сигналов, видеосигналов и сигналов передачи данных: заявка на изобретение Респ. Беларусь, МПК H 03 K 3/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20121293 ; заявл. 10.09.2012.

31. Устройство для получения сигнала маскирования каналов утечки информации: заявка на изобретение Респ. Беларусь, МПК H 04R 29/00, G 10L 15/00 / В.К. Железняк, Д.С. Рябенко ; заявитель Полоц. гос. ун-т. – № a 20121316 ; заявл. 10.09.2012.

РЭЗЮМЭ

РАБЕНКА Дзяніс Сяргеевіч

Метад ацэнкі абароненасці каналаў уцечкі маўленчых сігналаў у лічбавай форме частотна-маніпуліраваным сігналам з бесперапыннай фазай

Ключавыя словы: выразнасць маўлення, маўленчы сігнал у лічбавай форме, нарматыўны паказчык, высокая адчувальнасць, канал уцечкі маўленчай інфармацыі, прапускная здольнасць, маскіраванне.

Мэта працы: на аснове тэарэтычна абгрунтаванага адзінага крытэрыя лікавага значэння велічыні разборлівасці маўлення для каналаў уцечкі інфармацыі ў лічбавай і аналагавай формах, памехаабароненага аптымальнага вымяральнага сігналу распрацаваць навукова абгрунтаваныя метады ацэнкі абароненасці каналаў уцечкі інфармацыі ў лічбавай форме, а таксама метады сумеснага маскіравання маўленчых сігналаў у аналагавай і лічбавай формах.

Метады даследавання і абсталяванне: аналітычнае даследаванне і імітацыйнае мадэляванне, лічбавая апрацоўка сігналу, мадэляванне выкананае ў асяроддзі візуальнага матэматычнага мадэлявання Mathcad, Labview, Matlab. Задача ўстанаўлення адчувальнасці ацэнкі параметраў вымяральных сігналаў вырашаецца метадамі дысперсійнага аналізу, а задача колькаснага апісання – метадамі рэгрэсійнага аналізу.

Атрыманыя вынікі і іх навізна: тэарэтычна абгрунтаваныя і практычна рэалізаваныя навуковыя метады адзнакі абароненасці каналаў уцечкі інфармацыі ў лічбавай форме, адзіны крытэрый лікавага значэння велічыні разборлівасці маўлення каналаў уцечкі інфармацыі ў лічбавай форме, памехаабароненыя аптымальныя вымяральныя сігналы для бітавых і маніпуліраваных маўленчых сігналаў у лічбавай форме, метады адзінага маскіравання маўленчых сігналаў у лічбавай і аналагавай формах. Ужыванне прапанаваных метадаў дазволіла дасягнуць высокай дакладнасці і адчувальнасці ацэнкі абароненасці маўленчых сігналаў у лічбавай форме. Навізна працы пацверджаная наяўнасцю шэрагу патэнтаў на вынаходства.

Ступень выкарыстання: вынікі даследаванняў ужытыя пры падрыхтоўцы тэхнічнага задання на доследна-канструктарскія працы па Дзяржаўнай навукова-тэхнічнай праграме "Абарона інфармацыі 2", зацверджанай Пастановай Савета Міністраў Рэспублікі Беларусь ад 1 лютага 2011 года № 116; ужытыя ў навучальным працэсе ўстановы адукацыі "Полацкі дзяржаўны ўніверсітэт" і будуць прымяняцца пры далейшай мадэрнізацыі праграмна-апаратнага комплексу "Ярмак" для ацэнкі абароненасці маўленчых сігналаў у лічбавай форме ў каналах уцечкі інфармацыі (установа адукацыі "Полацкі дзяржаўны ўніверсітэт").

Вобласць ужывання: ацэнка абароненасці маўленчых сігналаў у лічбавай форме, маскіраванне аналагавых маўленчых сігналаў і маўленчых сігналаў у лічбавай форме.

РЕЗЮМЕ

РЯБЕНКО Денис Сергеевич

Метод оценки защищенности каналов утечки речевых сигналов в цифровой форме частотно-манипулированным сигналом с непрерывной фазой

Ключевые слова: разборчивость речи, речевой сигнал в цифровой форме, нормативный показатель, высокая чувствительность, канал утечки речевой информации, пропускная способность, маскирование.

Цель работы: на основе теоретически обоснованного единого критерия численного значения величины разборчивости речи для каналов утечки информации в цифровой и аналоговой формах, помехоустойчивого оптимального измерительного сигнала разработать научно обоснованные методы оценки защищенности каналов утечки информации в цифровой форме, а также методы совместного маскирования речевых сигналов в аналоговой и цифровой формах.

Методы исследования и оборудование: аналитическое исследование и имитационное моделирование, цифровая обработка сигнала, моделирование выполнены в средах визуального математического моделирования Mathcad, Labview, Matlab. Задача установления чувствительности оценки параметров измерительных сигналов решается методами дисперсионного анализа, а задача количественного описания – методами регрессионного анализа.

Полученные результаты и их новизна: теоретически обоснованы и практически реализованы научные методы оценки защищенности каналов утечки информации в цифровой форме, единый критерий численного значения величины разборчивости речи каналов утечки информации в цифровой форме, помехоустойчивые оптимальные измерительные сигналы для битовых и манипулированных речевых сигналов в цифровой форме, методы единого маскирования речевых сигналов в цифровой и аналоговой формах. Применение предложенных методов позволило достичь высокой точности и чувствительности оценки защищенности речевых сигналов в цифровой форме. Новизна работы подтверждена наличием ряда патентов на изобретение.

Степень использования: результаты исследований применены при подготовке технического задания на ОКР по Государственной научно-технической программе «Защита информации 2», утвержденной Постановлением Совета Министров Республики Беларусь от 1 февраля 2011 года № 116; в учебном процессе учреждения образования «Полоцкий государственный университет»; будут применены при дальнейшей модернизации программно-аппаратного комплекса «Ермак» для оценки защищенности речевых сигналов в цифровой форме в каналах утечки информации (учреждение образования «Полоцкий государственный университет»).

Область применения: оценка защищенности речевых сигналов в цифровой форме, маскирование аналоговых речевых сигналов и речевых сигналов в цифровой форме.

SUMMARY

RABENKA Dzianis Sergeevich

Method of security estimation of leakage channels of the voice signals in the digital form by means of a frequency shift-keying signal with the continuous phase

Key words: speech intelligibility, voice signal in digital form, normative characteristic, high sensitivity, leakage channel of voice information, carrier capacity, masking.

Research objective: to develop science-based methods of estimation of security of information leakage channels in digital form and methods of combined masking of voice signals in analog and digital forms basing on theoretically substantiated single criteria of numerical value of speech intelligibility for information leakage channels in digital and analog forms and antijamming optimal measuring signal.

Methods of testing and и equipment: analytical study and simulation technique, digital signal processing, modeling are performed in visual mathematical modeling environments Mathcad, Labview, Matlab. Problems of determination of estimation of characteristics sensitivity are solved with the help of methods of variance analysis and problems of quantitative description are solved with the help of regression analysis methods.

Results and their novelty: science methods of estimation of security of information leakage channels in digital form, single criteria of numerical value of speech intelligibility for information leakage channels in digital form, antijamming optimal measuring signals for bit and key-controlled voice signals in digital form, methods of single masking of voice signals in analog and digital forms are theoretically proved and realized in practice. Application of suggested methods made it possible to reach high precision and sensitivity in estimation of security of voice signals in digital form. Novelty of work is proved by a number of patents for invention.

Efficiency: research results were used during preparation of requirements specification for development work for government scientific and technical program "Information security 2" approved by Council of Ministers of the Republic of Belarus regulation from 1 February 2011 № 116; in training course at Polotsk State University; will be employed in further improvement of hardware-software complex "ERMAK" for estimation of security of voice signals in digital form in information leakage channels (Polotsk State University).

Field of application: estimation of security of voice signals in digital form, masking of analog voice signals and voice signals in digital form.

Научное издание

Денис Сергеевич
РЯБЕНКО

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИКАНАЛОВ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ В ЦИФРОВОЙ ФОРМЕ ЧАСТОТНО-МАНИПУЛИРОВАННЫМ СИГНАЛОМ С НЕПРЕРЫВНОЙ ФАЗОЙ

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

Подписано в печать 29.07.2014.	Формат 60x84 $^{1}/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,63.
Уч.-изд. л. 1,5.	Тираж 60 экз.	Заказ 327.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014, №2/113 от 07.04.2014, №3/615 от 07.04.2014
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6