

Учреждение образования  
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 621.391.16; 534 (043.3)

**БУРАЧЁНОК**  
**Ирина Брониславовна**

**ОЦЕНКА ЗАЩИЩЁННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ  
С ИСПОЛЬЗОВАНИЕМ ВЗАИМОКОРРЕЛЯЦИОННОЙ  
ЧАСТОТНО-ВРЕМЕННОЙ ОБРАБОТКИ  
ИЗМЕРИТЕЛЬНОГО СИГНАЛА**

**АВТОРЕФЕРАТ**

диссертации на соискание учёной степени  
кандидата технических наук

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

Минск 2016

Работа выполнена в учреждении образования «Полоцкий государственный университет»

Научный руководитель **Железняк Владимир Кириллович**,  
доктор технических наук, профессор,  
заведующий кафедрой радиоэлектроники  
учреждения образования «Полоцкий  
государственный университет»

Официальные оппоненты: **Липницкий Валерий Антонович**,  
доктор технических наук, профессор  
заведующий кафедрой высшей математики  
учреждения образования «Военная академия  
Республики Беларусь»

**Петров Сергей Николаевич**,  
кандидат технических наук, доцент, доцент  
кафедры защиты информации учреждения  
образования «Белорусский государственный  
университет информатики и  
радиоэлектроники»

Оппонирующая организация Учреждение образования «Белорусская  
государственная академия связи»

Защита состоится «16» февраля 2017 г. в 14<sup>00</sup> 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. +375 293 89 89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «\_\_» января 2017 г.

Учёный секретарь совета  
по защите диссертаций Д 02.15.06  
кандидат технических наук, доцент

Н. В. Насонова

## **КРАТКОЕ ВВЕДЕНИЕ**

Приоритетным направлением национальной безопасности в информационной сфере, установленным Концепцией национальной безопасности Республики Беларусь п. 54 (Указ Президента Республики Беларусь от 09.11.2010 г. № 575), является «... разработка и внедрение современных методов и средств защиты информации». Совершенствование средств извлечения речевой информации (РИ) и новые методы ее обработки в шумах высокого уровня обусловили необходимость улучшения важнейших параметров защиты и повышения быстродействия оценки защищённости РИ в технических каналах утечки информации (КУИ).

В работе выполнено научное обоснование использования сложных измерительных сигналов (ИС) для оценки защищённости РИ в условиях шумов высокого уровня и значительной неравномерности амплитудно-частотной характеристики (АЧХ) в КУИ. Установлены оптимальные параметры сложных ИС, определяемые величиной их базы, в полосах равной разборчивости (ПРР) спектра речевого сигнала (РС), что позволило значительно снизить время оценки защищённости в сравнении с известными методами. Предложен способ формирования показателя защищённости РИ, основанный на определении отношения мощности сложного ИС с большой базой к мощности шума (ОСШ), и его математической зависимости от нормативного показателя, установленного для гармонического измерительного сигнала, включенного в СТБ 34.101.29-2011. Использование взаимокорреляционной временной и частотно-временной обработок сложного ИС с большой базой, компенсация его временного запаздывания и частотного сдвига, а также его синхронное накопление в точке приёма в КУИ в каждой ПРР спектра РС позволили значительно улучшить значения ОСШ, повысить помехоустойчивость, точность, разрешающую способность по времени и частоте и оперативность представления результатов оценки защищённости РИ в технических КУИ.

На основании изложенного системное решение научных целевых задач и представление полученных новых результатов определило актуальность исследований диссертационной работы.

## **ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ**

### **Связь работы с научными программами (проектами), темами**

Тема диссертационной работы утверждена приказом ректора учреждения образования «Полоцкий государственный университет» № 727-ув от 19.12.2012 г. и соответствует приоритетным направлениям научных исследований и научно-технической деятельности в Республике Беларусь в области технической защиты информации по созданию современных систем защиты информации.

Исследования диссертационной работы включены при формировании тех-

нических требований на ОКР по Государственной научно-технической программе «Защита информации-3», утвержденной Постановлением Совета Министров Республики Беларусь от 25.02.2016 г. № 153.

### **Цель и задачи исследования**

*Цель диссертационной работы* – обоснование, разработка и реализация методики оценки защищённости речевой информации в технических каналах утечки для обнаружения измерительных сигналов в маскирующих шумах высокого уровня при неравномерности амплитудно-частотной характеристики со значительным повышением оперативности представления результатов.

Для достижения поставленной цели в диссертационной работе необходимо решить следующие *научные задачи*.

1. Выполнить системный анализ и обосновать выбор измерительного сигнала для выявления противоречия между фактическим состоянием и необходимостью повышения численных значений основных параметров оценки защищённости речевой информации в технических каналах утечки.

2. Математически обосновать и определить показатель оценки защищённости речевой информации в технических каналах утечки сложным измерительным сигналом с большой базой в полосах равной разборчивости спектра речевого сигнала.

3. Разработать методику оценки защищённости речевой информации в технических каналах утечки с использованием взаимокорреляционной обработки во временной области сложного измерительного сигнала с большой базой при компенсации его временного запаздывания в условиях воздействия маскирующего шумового сигнала.

4. Разработать методику оценки защищённости речевой информации в технических каналах утечки с использованием взаимокорреляционной частотно-временной обработки сложного измерительного сигнала с большой базой, представленного преобразованием Гильберта в аналитическом виде, при снижении порога обнаружения синхронным накоплением его спектральных составляющих и одновременной компенсации временного запаздывания и частотного сдвига в условиях воздействия маскирующего шумового сигнала.

### **Научная новизна**

Новыми являются следующие научные результаты.

1. Теоретически и экспериментально обоснована оценка защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки, взаимокорреляционной обработкой во временной области сложного измерительного сигнала с большой базой при компенсации с высокой точностью его временного запаздывания с использованием функции взаимной корреляции по времени между сложными измерительными сигналами с большой базой в точках излучения и приёма в техническом канале утечки информации.

2. Теоретически и экспериментально обоснована оценка защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки,

взаимокорреляционной частотно-временной обработкой сложного измерительного сигнала с большой базой, представленного преобразованием Гильберта в аналитическом виде, при компенсации с высокой точностью его временного запаздывания и частотного сдвига с использованием функций взаимной корреляции по времени и частоте между сложными измерительными сигналами с большой базой в точках излучения и приёма в техническом канале утечки информации.

### **Положения, выносимые на защиту**

1. Способ формирования показателя защищённости речевой информации, основанный на определении отношения мощности сложного измерительного сигнала с обоснованными оптимальными значениями его базы в пределах полос равной разборчивости спектра речевого сигнала к мощности шума, математической зависимостью от нормативного показателя, установленного для гармонического измерительного сигнала, позволяющий улучшить отношение мощности сигнала к мощности шума на 16 дБ при использовании сигналов длительностью  $T_c = 4$  с и снизить суммарное время оценки защищённости более чем в 6 раз (с 500 до 80 с) в сравнении с гармоническим измерительным сигналом.

2. Методика оценки защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки, основанная на использовании взаимокорреляционной обработки во временной области сложного измерительного сигнала с большой базой (от 560 до 11000) при компенсации его временного запаздывания, позволяющая улучшить отношение мощности сигнала к мощности шума и снизить порог обнаружения до 27 дБ, а также сократить время синхронного накопления сигнала в точке приёма более чем в 10 раз в сравнении с гармоническим измерительным сигналом.

3. Методика оценки защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки, основанная на использовании взаимокорреляционной частотно-временной обработки сложного измерительного сигнала с большой базой (от 560 до 11000), представленного преобразованием Гильберта в аналитическом виде, при компенсации его временного запаздывания и частотного сдвига, позволяющая улучшить отношение мощности сигнала к мощности шума на 6 дБ в каждой полосе равной разборчивости спектра речевого сигнала и повысить разрешающую способность по частоте и времени при обеспечении точности частотно-временной обработки, равной одному периоду дискретизации.

### **Личный вклад соискателя учёной степени**

Содержание диссертационной работы отражает личный вклад автора. В совместных с руководителем публикациях вклад автора 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.

Соавтором основных публикаций является научный руководитель, доктор технических наук, профессор В. К. Железняк, совместно с которым осуществлялось определение целей и постановка задач исследований, выбор методов и направлений исследований, планирование работ и обсуждение результатов, интерпретация и обобщение научных результатов.

### **Апробация диссертации и информация об использовании её результатов**

Основные положения и результаты диссертации докладывались и обсуждались на следующих научных конференциях и семинарах: X Международной научно-практической конференции «Управление информационными ресурсами» (г. Минск, АУП РБ, декабрь 2013 г.); XVIII, XIX, XX, XXI Международных научно-технических конференциях «Современные средства связи» (г. Минск, ВГКС (БГАС), октябрь 2013 г., 2014 г., 2015 г., 2016 г.); Республиканских семинарах «Математическое моделирование сложных систем, анализ данных и защита информации» (г. Минск, БГУ, март, ноябрь 2014 г., март 2015 г., апрель, ноябрь 2016 г.); Международных научно-практических конференциях «Теоретические и прикладные проблемы информационной безопасности» (г. Минск, АМВД РБ, июнь 2014 г., март 2016 г.); 6th, 7th, 8th Junior researchers conference European and National dimension in research (Новополоцк, ПГУ, апрель, 2014 г., 2015 г., 2016 г.); V Международной научно-практической конференции «Интеллектуальные системы на транспорте» (ИнтеллектТранс-2015) (г. Санкт-Петербург, ПГУПС, апрель 2015 г.); 5-й Республиканской научно-практической конференции «Обеспечение пограничной безопасности и охрана Государственной границы Республики Беларусь: теория и практика» (г. Минск, ИПГС РБ, май 2015 г.); XX научно-практической конференции «Комплексная защита информации» (г. Минск, БГУ, май 2015 г.); ежегодной Международной научной конференции молодых учёных «Молодежь в науке – 2015» (г. Минск, НАН РБ, декабрь 2015 г.); XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации» (г. Минск, БГУИР, июнь 2016 г.).

### **Опубликование результатов диссертации**

По результатам исследований, представленных в диссертации, опубликовано 22 работы, в том числе 6 статей в журналах из перечня рецензируемых научных журналов и изданий в соответствии с пунктом 18 «Положения о присуждении учёных степеней и присвоении учёных званий в Республике Беларусь» общим объёмом 3,2 авторского листа; 11 статей и 5 тезисов докладов в сборниках и материалах международных научных конференций. Поданы заявки на выдачу патентов Республики Беларусь: «Способ определения разборчивости речи» (№ 05-245, 27.05.2014, № а 20140302 от 02.06.14) и «Устройство определения разборчивости речи» (№ 05-246, 27.05.2014, № а 20140303 от 02.06.14).

## Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырёх глав, заключения, библиографического списка и 7 приложений. Общий объём диссертации составляет 184 страницы, из них 149 страниц основного текста, 104 рисунка на 45 страницах, 6 таблиц на 8 страницах, библиографический список из 150 наименований на 10 страницах, список собственных публикаций автора из 22 наименований на 3 страницах, приложений на 20 страницах.

## ОСНОВНАЯ ЧАСТЬ

Во **введении и в общей характеристике** работы на основании системного анализа обоснована актуальность темы диссертационной работы, сформулированы цель и научные задачи исследований, определены основные направления теоретических и экспериментальных исследований. Представлены новые научные результаты, описана их практическая значимость, сформулированы основные положения, выносимые на защиту.

В **первой главе** проанализированы технические каналы утечки (КУ) речевой информации, а также известные методы и средства оценки их защищённости, наиболее значимые свойства и характеристики ИС.

Методы оценки защищённости РИ в КУИ реализуют точность, чувствительность и оперативность, определяемые длительностью ИС и временем его обработки в точке приёма в КУИ, и представляют результаты оценки в виде разборчивости речи или ОСШ в КУ речевой информации. Установлено, что для надежной оценки защищённости РИ в КУИ необходимо учитывать воздействующие факторы: неравномерность спектральной плотности РС, предельную бинауральную чувствительность уха, затухание в типовых элементах ограждающих конструкций, спектральную плотность фонового акустического шума, реверберационные помехи и резонансные явления замкнутых пространств.

Оценка защищённости РИ в КУИ обеспечивается методом корреляционной разборчивости. Установлено, что метод оценки защищённости РИ в КУИ гармоническим ИС, включенным в СТБ 34.101.29-2011, в двадцати ПРР спектра РС обладает рядом преимуществ, необходимых для получения высокой точности при допустимом времени обработки. Узкополосная фильтрация в  $k$  ПРР ( $k = 1, 20$ ) обеспечивает высокую разрешающую способность по частоте  $2\Delta f_k / z$ , где  $2\Delta f_k$  – ширина  $k$ -й ПРР;  $z$  – количество параллельных фильтров в каждой  $k$ -й ПРР. Чувствительность каждого фильтра зависит от его полосы пропускания. Однако применение гармонического ИС на средних частотах в двадцати ПРР допускает увеличение погрешности при оценке защищённости РИ в КУИ в диапазоне частот от 100 Гц до 10 кГц с явно выраженными неравномерностями АЧХ в условиях шумов высокого уровня. Более высокая чувствительность оценки защищённости РИ в КУИ получена при использовании метода широкополосного

ЛЧМ-сигнала с предварительной обработкой преобразованием Вигнера, однако при некоторых методических преимуществах перед методом гармонического ИС данный метод уступает по времени обработки. Выявленные недостатки известных методов оценки защищённости РИ в КУИ и совершенство современных средств обработки ИС обусловили необходимость разработки новых методик оценки с сохранением ранее достигнутых параметров чувствительности, точности, разрешения по времени и частоте при значительном повышении оперативности представления результатов. Предложено оценку защищённости РИ в КУИ проводить сложным ИС с большой базой  $B \gg 1$ , равной произведению девиации частоты  $2\Delta f_k$  на длительность сигнала  $T_c$  в каждой ПРР спектра РС. Проанализированы последние достижения в области систем измерительных автоматизированных для оценки защищённости РИ в КУИ.

Таким образом, в первой главе определены основные направления исследований: необходимость проведения системного анализа сложных ИС с большой базой в ПРР спектра РС для выявления наиболее значимых их свойств и подбора оптимальных исходных данных для оценки защищённости РИ в КУИ; установление математической зависимости показателя оценки защищённости РИ в КУИ сложным ИС с большой базой от нормативного показателя защищённости гармоническим ИС; разработка и обоснование методик оценки защищённости РИ, маскируемой шумовым сигналом, основанных на использовании взаимокорреляционной временной и частотно-временной обработок сложного ИС с большой базой при компенсации его временного запаздывания и частотного сдвига в точке приёма в КУИ; моделирование и имитационный эксперимент с обоснованием преимуществ предложенных методик для подтверждения правильности положений, выносимых на защиту.

Во **второй главе** обоснованы требования к сложному ИС с большой базой. Установлено численное значение показателя защищённости РИ в КУИ сложным ИС с большой базой по аналитической зависимости от нормативного показателя защищённости РИ в КУИ для гармонического ИС. Предложен способ формирования показателя защищённости РИ в КУИ по критерию разборчивости речи в ПРР спектра РС шумах высокого уровня сложным ИС с большой базой.

Для детерминированного сигнала отношение энергии к спектральной мощности шума в диапазоне  $0 \leq t \leq T_c$  определяют как  $q_{\text{вых}}^2 = \frac{2E}{N_0}$ , где  $N_0$  – спектральная плотность мощности шума.

Энергетический спектр  $W_k$  сложного ИС с большой базой в каждой  $k$ -й ПРР спектра РС представляют известным выражением

$$W_k = \frac{\pi U_0^2}{2\mu_k} = \frac{\pi U_0^2 T_c}{2\pi \Delta f_k} = \frac{U_0^2 T_c^2}{2\Delta f_k T_c} = \frac{U_0^2 T_c^2}{B_k}, \quad (1)$$

где  $U_0$  – амплитуда огибающей сигнала;

$T_c$  – длительность сигнала;



$\mu_k = \Delta\omega_k / T_c$  – скорость нарастания частоты сигнала в каждой  $k$ -й ПРР;  
 $B_k = 2\Delta f_k T_c$  – база сигнала в  $k$ -й ПРР.

Следовательно, ОСШ в КУ речевой информации для сложного ИС с большой базой в каждой  $k$ -й ПРР можно записать

$$q_{\text{вых\_сл } k}^2 = \frac{2U_0^2 T_c^2}{B_k N_0 R} 2\Delta f_k = \frac{2U_0^2 T_c^2 2\Delta f_k}{T_c 2\Delta f_k N_0 R} = \frac{2U_0^2 B_k}{2\Delta f_k N_0 R} = \left( \frac{P_c}{P_{\text{ш}}} \right)_k 2B_k, \quad (2)$$

где  $P_{\text{ш}} = N_0 2\Delta f_k$  – мощность шума в  $k$ -й ПРР;

$P_c = U_0^2 / R$  – мощность сигнала, выделяемая на сопротивлении  $R = 1$  Ом.

Таким образом, ОСШ в КУ речевой информации  $q_{\text{вых\_сл}}^2$  связано с ОСШ на его входе в точке излучения  $\rho_{\text{вх}}^2 = P_c / P_{\text{ш}}$ :

$$q_{\text{вых\_сл}}^2 = 2B\rho_{\text{вх\_сл}}^2. \quad (3)$$

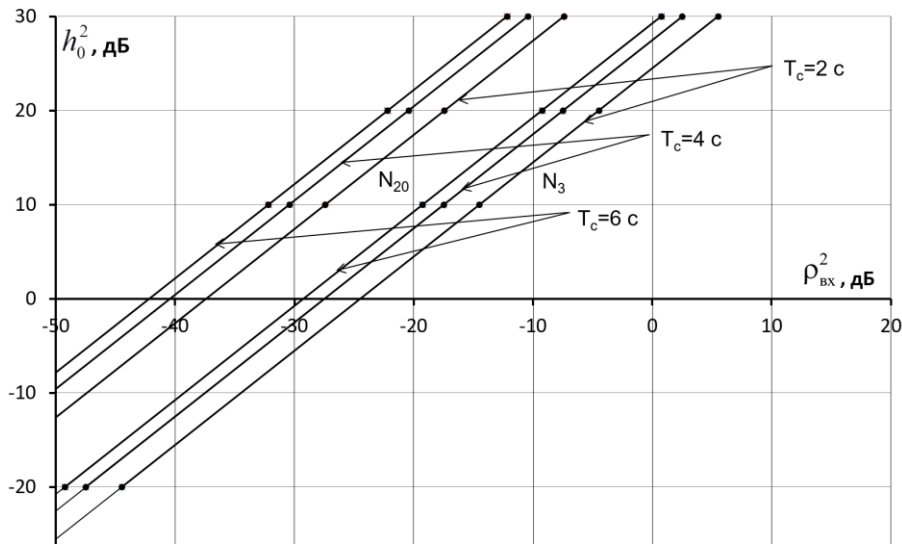
ОСШ в КУ речевой информации  $q_{\text{вых\_сл}}^2$  определяет рабочие характеристики приёма сложных ИС с большой базой, а ОСШ на его входе в точке излучения  $\rho_{\text{вх\_сл}}^2$  – энергетику сигнала и шума. Величина  $q_{\text{вых\_сл}}^2$  может быть получена даже если  $\rho_{\text{вх\_сл}}^2 \ll 1$ . Для этого достаточно выбрать сложные ИС с величиной базы  $B$ , удовлетворяющей выражению (3). Как видно из отношения (2), приём сложных ИС с большой базой сопровождается подавлением шума в КУИ.

Исходя из того, что в широкополосных системах связи приём информации характеризуется ОСШ  $h_0^2 = q_{\text{вых}}^2 / 2$ , т. е.  $h_0^2 = B\rho_{\text{вх}}^2$ , имеем зависимость ОСШ сложных ИС с большой базой в точке приёма в КУ речевой информации  $h_0^2$  от ОСШ в точке излучения  $\rho_{\text{вх}}^2$  при длительностях сложных ИС с большой базой  $T_c = 2, 4, 6$  с в третьей  $N_3$  и двадцатой  $N_{20}$  ПРР (рисунок 1).

При условии, что значение девиации частоты  $\pm\Delta f_k$  в каждой ПРР фиксировано, увеличение длительности  $T_c$  сложного ИС позволяет увеличить размер базы  $B_k$  и тем самым улучшить ОСШ в КУ речевой информации. Однако необходимо учитывать и то, что увеличение длительности сложных ИС обуславливает увеличение суммарного времени оценки защищённости РИ в КУИ (дальнейшее обоснование и подбор оптимальных исходных данные для сложных ИС в ПРР спектра РС приведены в третьей главе диссертации).

При использовании для оценки защищённости РИ в КУИ гармонического ИС (база  $B = 1$ ) ОСШ в КУИ в точке приёма можно представить в виде

$$q_{\text{вых\_гар}}^2 = \frac{2E}{N_0} = \frac{2P_c T_c 2\Delta f_k}{P_{\text{ш}} R} = \frac{2P_c B_k}{P_{\text{ш}} R} = 2 \left( \frac{P_c}{P_{\text{ш}}} \right)_k. \quad (4)$$



**Рисунок 1. – Зависимость ОСШ сложного ИС с большой базой в точке приёма в КУ речевой информации от ОСШ в точке излучения при  $T_c=2,4,6$  с в третьей  $N_3$  и двадцатой  $N_{20}$  полосах равной разборчивости**

Нормированный показатель, устанавливающий математическую зависимость между нормативным показателем защищённости РИ в КУИ гармоническим ИС и показателем защищённости сложным ИС с большой базой, определяют как ОСШ в точке приёма в КУ речевой информации, оценённое сложным ИС с большой базой  $q_{\text{вых\_сл}}^2$ , к нормативному показателю  $q_{\text{вых\_гар}}^2$  в виде численного значения ОСШ для гармонического ИС:

$$\delta_{\text{сл}} = \frac{q_{\text{вых\_сл}}^2}{q_{\text{вых\_гар}}^2}. \quad (5)$$

Если нормативный показатель защищённости РИ в КУИ гармоническим ИС определяется как  $q_{\text{вых\_гар}}^2 = \left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{норм}}$ , то при равенстве ОСШ выходных ИС гармонического и сложного с большой базой  $\left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{сл}} = \left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{норм}}$  имеем отношение

$$\delta_{\text{сл}} = \frac{q_{\text{вых\_сл}}^2}{\left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{норм}}} = \frac{B \left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{сл}}}{\left( \frac{P_c}{P_{\text{ш}}} \right)_{\text{норм}}} = B. \quad (6)$$

С помощью (6) установлена математическая зависимость нормированного показателя защищённости РИ в КУИ сложным ИС с большой базой от нормативного показателя, установленного для оценки защищённости гармоническим ИС. Установлено однозначное преимущество оценки защищённости РИ в КУИ сложным ИС с большой базой, равное величине его базы  $B$ , определяемой произведением длительности  $T_c$  сигнала на девиацию его частоты  $2\Delta f$  в пределах каждой ПРР спектра РС).

Научная новизна способа формирования показателя защищённости РИ, маскируемой шумовым сигналом в КУИ, заключается в том, что установленная математическая зависимость показателя оценки защищённости РИ в КУИ сложным ИС с большой базой от показателя оценки защищённости гармоническим ИС позволила установить численное значение данного показателя для оценки сложным ИС с большой базой. При использовании сложных ИС с большой базой в двадцати ПРР длительностью  $T_c = 4$  с улучшено ОСШ на 16 дБ и сокращено суммарное время оценки более чем в 6 раз (с 500 до 80 с) в сравнении с гармоническим ИС.

В **третьей главе** предложена и обоснована методика оценки защищённости РИ, маскируемой шумовым сигналом в технических КУ, взаимокорреляционной обработкой во временной области сложного ИС с большой базой. Разработанная методика позволяет определить максимальное ОСШ в точке приёма в КУ речевой информации при компенсации временного запаздывания, обеспечив высокую точность и чувствительность оценки при уменьшении длительности ИС.

В основе предлагаемой методики лежит применение взаимокорреляционной функции (ВКФ) по времени  $R_{1,2}(\tau)$  не зашумлённого в точке излучения (входного)  $s_1(t)$  и зашумлённого шумом  $n(t)$  в КУИ в точке приёма (выходного)  $s_2(t)$  сложных ИС с большой базой:

$$R_{1,2}(\tau) = \int_{-\infty}^{\infty} s_1(t) s_2(t - \tau) dt, \quad (7)$$

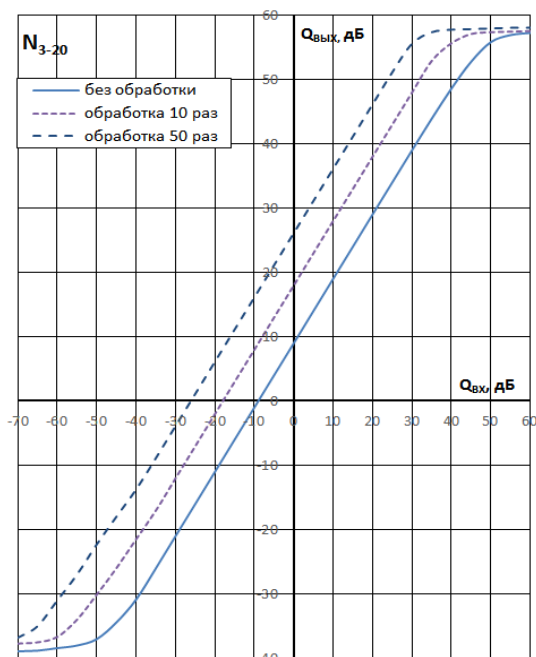
где  $\tau$  – сдвиг по времени между входным  $s_1(t)$  и выходным  $s_2(t) = s_1(t) + n(t)$ , зашумлённым шумом  $n(t)$  сложными ИС с большой базой.

Функция (7) оценивает степень сходства двух ИС, а также их взаимное расположение по оси времени. В момент времени, когда выходной ИС  $s_2(t)$  наиболее подобен входному  $s_1(t)$ , она максимальна. Если  $s_1(t) = s_2(t)$ , то выражение (7) является автокорреляционной функцией (АКФ) ИС. Сдвиг пика ВКФ относительно  $\tau = 0$  равен времени задержки сигнала  $s_2(t)$  относительно  $s_1(t)$ . Математический подход при использовании производных от ВКФ позволил, установив положение точки на временной оси, в которой данная производная равна нулю, с высокой точностью определить величину задержки  $\tau$  между сложными ИС с большой базой на входе  $s_1(t)$  и выходе  $s_2(t)$  КУИ и, тем самым, скомпенсировать случайное временное запаздывание сложного ИС в КУИ. Сдвиг определяют как разность между точками максимального значения АКФ сложного ИС с большой базой в точке излучения в КУИ и максимального значения построенной ВКФ. По вновь построенным ВКФ оценивают мощности сложных ИС с большой базой в каждой  $k$ -й ПРР спектра РС и определяют величину ОСШ. Далее рассчитывают разборчивость речи на основании средних значений коэффициентов разборчивости речи в каждой  $k$ -й ПРР спектра РС и сравнивают с установленным во второй главе нормативным значением ОСШ. Использование ВКФ ослабило шумовую составляющую  $n(t)$  сложного ИС с большой базой и исключило погрешности, свя-

занные с его запаздыванием в КУИ. Это позволило определить максимальное значение ВКФ с точностью, равной одному периоду дискретизации  $T_0$ , и повысило точность оптимальной оценки параметров сложных ИС с большой базой при приеме в шуме высокого уровня.

В предложенной методике для дополнительного повышения точности оценки защищённости РИ в КУИ используя быстрое прямое (БПФ) и обратное преобразования Фурье (ОБПФ) применяется предварительное  $n$ -кратное синхронное накопление спектральных составляющих сложного ИС с большой базой в точке приёма КУ речевой информации до превышения над уровнем шума.

По результатам экспериментов выделения сложных ИС с большой базой из шумов высокого уровня получены значения предельной чувствительности для каждой  $k$ -й ПРР спектра РС при относительной погрешности  $|\gamma| < 3\%$ . На рисунке 2 приведён график, отображающий зависимость  $Q_{\text{вых}}$  от  $Q_{\text{вх}}$  для двадцати ПРР с точечной среднестатистической обработкой выходных сложных ИС с большой базой в шумах высокого уровня длительностью  $T_c = 4$  с. Показано, что при длительности сложного ИС с большой базой  $T_c = 4$  с имеется выигрыш в надпороговой области, равный 8 дБ, а применение дополнительно последовательного  $n$ -кратного синхронного накопления сложного ИС с большой базой в точке приёма КУИ позволяет получить выигрыш в ОСШ: при обработке накоплением 10 раз – до 18 дБ, при обработке накоплением 50 раз – до 27 дБ.



**Рисунок 2.** – Зависимость  $Q_{\text{вых}}$  от  $Q_{\text{вх}}$  сложного ИС с большой базой длительностью  $T_c = 4$  с в третьей  $N_3$  и в двадцатой  $N_{20}$  полосах равной разборчивости

На основании анализа влияния размера базы  $B_k$ , зависящей от девиации частоты  $\pm \Delta f_k$ , перекрывающей каждую  $k$ -ю ПРР, и длительности сигнала  $T_c$ , на показатели оценки разборчивости речи в КУИ при минимизации времени обработки

экспериментально подтверждён выбор оптимальных исходных данных сложных ИС с большой базой в каждой  $k$ -й ПРР спектра РС.

Обоснованные размеры баз сложных ИС для каждой ПРР спектра РС представлены в таблице 1.

Таблица 1. – Зависимость  $B = f(2\Delta f_k T_c)$  при  $T_c = 4$  с

Номер полосы $N_k$	1	2	3	4	5	6	7	8	9	10
Девияция частоты $2\Delta f_k$ , Гц	320	150	140	155	165	190	190	190	180	180
База $B$	1280	600	560	620	660	760	760	760	720	720

Окончание таблицы 1

Номер полосы $N_k$	11	12	13	14	15	16	17	18	19	20
Девияция частоты $2\Delta f_k$ , Гц	180	180	230	350	400	360	390	960	2240	2750
База $B$	720	720	920	1400	1600	1440	1560	3840	8960	11000

Установлено, чем больше длительность сложного ИС с большой базой, тем меньше значение вариации для каждой  $k$ -й ПРР. Однако, учитывая необходимость снижения времени оценки при достижении высокой чувствительности, оптимальным является выбор постоянного значения длительности  $T_c = 4$  с ИС в каждой  $k$ -й ПРР. Выбор для оценки защищённости РИ в КУИ сложных ИС, одинаковых по длительности, позволяет сократить время оценки в каждой из  $k$  ПРР и суммарное время оценки более чем в 5 раз в сравнении с временем обработки сложных ИС с постоянным значением базы.

Так как оценка величины разборчивости речи, представленная в виде отдельного цифрового программного компонента, является наиболее ёмкой по вычислительным ресурсам, то определена её временная эффективность с учетом количества базовых операций. Для выполнения алгоритма расчёта разборчивости речи при использовании взаимокорреляционной обработки сложного ИС с большой базой, например, при частоте дискретизации  $F_s = 4,41$  кГц количество базовых операций составит  $C(n) = 3,9 \cdot 10^{10}$ , а при  $F_s = 100$  кГц –  $C(n) = 2,0 \cdot 10^{11}$ . Расчетное время обработки сложного ИС с большой базой длительностью  $T_c = 4$  с при частоте дискретизации  $F_s = 4,41$  кГц с использованием ПЭВМ (Intel® Core™ Duo U2400)  $3,18 \cdot 10^9$  флоп/с составит 48,9 с, длительностью  $T_c = 2$  с – 12,2 с. Использование более современных ПЭВМ (например, Intel® Core™ i7-975 XE) позволит обрабатывать сложный ИС с большой базой длительностью  $T_c = 4$  с около 3 с, длительностью  $T_c = 2$  с – 1 с. Снижение суммарного времени обработки обеспечивается за счёт оптимизации количества временных составляющих ИС, однако значительное уменьшение количества элементов в выборке

снижает информативность тонкой структуры ИС, что отражается на методической точности оценки защищённости РИ в КУИ, поэтому при практическом использовании программно-аппаратного комплекса (ПАК) в процессе исследования объекта информатизации устанавливается частота дискретизации, позволяющая детально установить факторы, обуславливающие наличие утечки в КУИ.

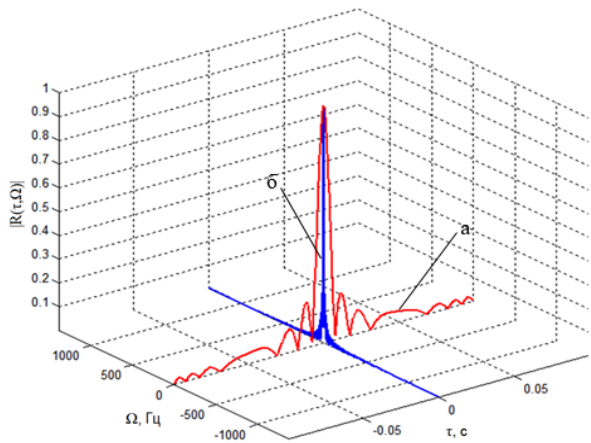
Научная новизна разработанной методики оценки защищённости РИ, маскируемой шумовым сигналом в технических КУ, основанной на использовании взаимокорреляционной обработки во временной области сложного ИС с большой базой при компенсации с высокой точностью его временного запаздывания с использованием ВКФ по времени между сложными ИС с большой базой в точках излучения и приёма в техническом КУ заключается в том, что при использовании сложных ИС с большой базой, одинаковых по длительности, равной  $T_c = 4$  с, и с разными значениями баз в каждой  $k$ -той ПРР спектра РС повышена чувствительность оценки на 27 дБ, упрощена процедура автоматизированных измерений и сокращено время обработки ИС в 2,5 раза в каждой из ПРР в сравнении с методом широкополосного ЛЧМ-сигнала с частотно-временной обработкой преобразованием Вигнера, а также сокращено время синхронного накопления ИС в точке приёма более чем в 10 раз в сравнении с гармоническим ИС. Достигнутые результаты значительно снизили суммарное время оценки защищённости РИ в КУИ.

В четвертой главе представлен имитационный эксперимент созданной и оптимизированной инфологической модели с целью точного и полного отображения методики оценки защищённости РИ, маскируемой шумовым сигналом в технических КУ, с использованием взаимокорреляционной частотно-временной обработки сложного ИС с большой базой, представленного преобразованием Гильберта в аналитическом виде, для определения максимально возможного ОСШ в точке приёма КУИ. Представлены результаты моделирования оперативной оценки численных показателей разборчивости речи на базе разработанной методики с использованием алгоритмов цифровой обработки сложных ИС с большой базой в ПРР спектра РС в шумах высокого уровня средствами среды имитационного моделирования MatLAB R2013b.

Представление сложного ИС с большой базой в диапазонах частот  $k$ -полосного разделения в точках излучения и приёма в техническом КУИ в виде комплексной переменной частотно-временным преобразованием Гильберта расширило возможности методики, описанной в третьей главе. Временная форма  $s(t)$  сигнала и его частотное представление  $F(\omega)$  позволили проводить оценку одновременно по времени и по частоте, так как оба представления взаимосвязаны и модификация одного из них приводит к изменению другого. В частности, некоторый временной сдвиг эквивалентен частотному фазовому сдвигу:  $s(t - \tau) \Leftrightarrow F(f)e^{-2\pi i f \tau}$ , а частотный сдвиг эквивалентен временному фазовому сдвигу:  $F(f - \varphi) \Leftrightarrow s(t)e^{2\pi i \varphi t}$ .

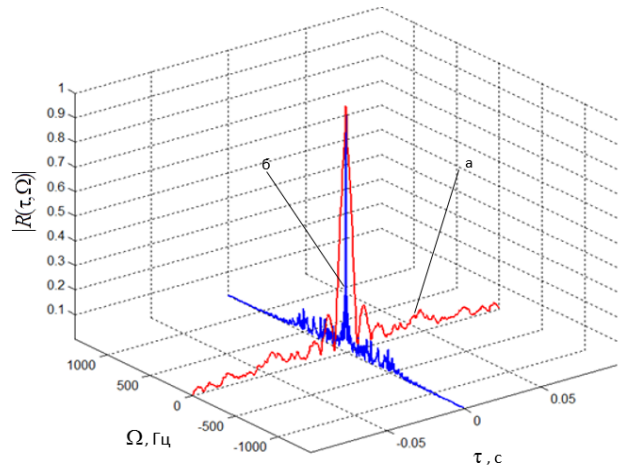
На рисунке 3 в трехмерном пространстве представлены АКФ ИС в точке излучения в КУИ по времени (рисунок 3, а) и частоте (рисунок 3, б). На рисунке 4

в трехмерном пространстве представлены АКФ зашумлённого ИС в точке приёма в КУИ по времени (рисунок 4, а) и частоте (рисунок 4, б).



а – АКФ по времени; б – АКФ по частоте

**Рисунок 3. – АКФ в трехмерном пространстве в точке излучения в КУИ**



а – АКФ по времени; б – АКФ по частоте

**Рисунок 4. – АКФ в трехмерном пространстве в точке приёма в КУИ**

Одновременное формирование временных и частотных АКФ и ВКФ, а также использование математического подхода по производной ВКФ между сложными ИС с большой базой в точках излучения и приёма в КУИ одновременно по времени и частоте позволило, установив положение точки на оси, в которой данная производная равна нулю, определить с минимальной погрешностью временное запаздывание и частотный сдвиг сложного ИС с большой базой в КУИ. Использование двух комплексно-сопряженных сигналов при построении ВКФ позволило получить выигрыш по амплитуде сигнала в 2 раза, а одновременная компенсация с высокой точностью временного запаздывания и частотного сдвига сложного ИС с большой базой в точке приёма в КУИ значительно повысила точность и чувствительность оценки защищённости РИ в КУИ.

На основании полученных ВКФ по времени и по частоте строится обобщённая ВКФ комплексных огибающих двух сложных ИС с большой базой. Обобщённую ВКФ представляют во временной и спектральной плоскостях в виде пары отдельно взятых функций:

$$R_{1,2}(\tau, \Omega) = \frac{1}{E} \int_{-\infty}^{\infty} \dot{s}_1(t) \dot{s}_2^*(t - \tau) e^{i\Omega t} dt \quad \text{или} \quad R_{1,2}(\tau, \Omega) = \frac{1}{2\pi E} \int_{-\infty}^{\infty} F_1(\omega - \Omega) F_2^*(\omega) e^{i\Omega t} d\omega, \quad (8)$$

где  $\dot{s}_1(t)$ ,  $\dot{s}_2^*(t - \tau)$  – комплексные огибающие входного и принятого сложных ИС с большой базой с учётом операции комплексного сопряжения (\*);

$E$  – энергия сигнала;

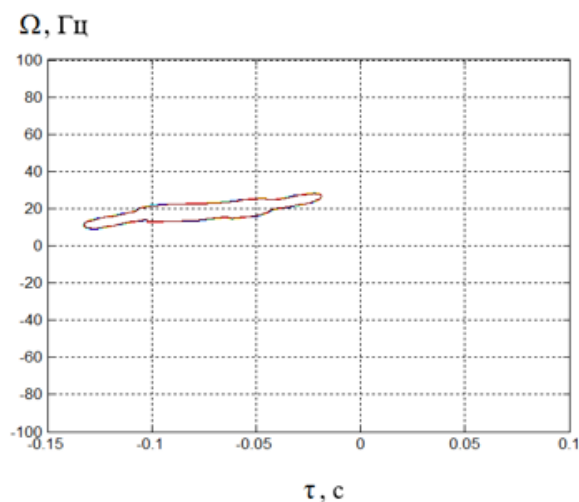
$F_1(\omega - \Omega)$ ,  $F_2^*(\omega)$  – их спектральные плотности с учётом операции комплексного сопряжения (\*);

$\Omega$  – частотная переменная сдвига по частоте между  $F_1(\omega)$  и  $F_2(\omega)$ ;

$i$  – мнимая единица.

Функция  $R_{1,2}(\tau, \Omega)$  является взаимной функцией неопределённости (ВФН), позволяющей одновременно оценить степень различия сигналов, отличающихся значениями запаздывания  $\tau$  и частотного сдвига  $\Omega$ .

Площадь сечения плоскостью, параллельной плоскости  $(\tau, \Omega)$  по уровню 0,5, представляет собой основание цилиндра с высотой, равной главному максимуму, и объёмом, равным объёму, ограниченному всей поверхностью  $|R_{1,2}(\tau, \Omega)|^2$ , и служит мерой совместной разрешающей способности сложного ИС с большой базой по времени и частоте. На рисунке 5 показано сечение тела ВФН сложного ИС с большой базой в третьей  $N_3$  ПРР спектра речевого сигнала в точке приёма в КУИ.



**Рисунок 5. – Сечение тела ВФН сложного ИС в третьей  $N_3$  полосе равной разборчивости в канале утечки информации**

Для моделирования оценки защищённости РИ в КУИ использовался некоррелированный шум (хаотическая импульсная последовательность (ХИП)) с энтропийным коэффициентом качества не ниже 0,94 и наилучшими маскирующими свойствами защиты РИ. Шум ХИП обеспечивает генератор маскирующих сигналов на базе диодов-генераторов серии ND100. Исследование предельных параметров оценки защищённости РИ в КУИ с использованием взаимокорреляционной частотно-временной обработки сложного ИС с большой базой выполнено с помощью оборудования лаборатории технической защиты информации: шумомера SPL-Laboratory USB Noise Meter, аналогово-цифрового преобразователя L-Card E14-440, аудиоанализатора UPP 800 и анализатора сигналов FSV4 Rohde&Schwarz. Выбранные средства цифровой обработки позволяют обеспечить высокую точность оценки и достичь разрешающей способности по частоте, близкой к потенциальной, во всем диапазоне частот РС.



Спектральное представление сложного ИС с большой базой, используемое при реализации его синхронного накопления, осуществлялось преобразованием Фурье. Для уменьшения числа операций используется алгоритм БПФ (алгоритм Кули–Тьюки), который устраняет избыточность и использует соображения симметрии в расчётах. Это преимущество используется и при ОБПФ.

Научная новизна методики оценки защищённости РИ, маскируемой шумовым сигналом в технических КУ, основанной на использовании взаимокорреляционной частотно-временной обработки сложного ИС с большой базой, представленного преобразованием Гильберта в аналитическом виде, при компенсации с высокой точностью его временного запаздывания и частотного сдвига с использованием ВКФ по времени и частоте между сложными ИС с большой базой в точках излучения и приёма в техническом КУ заключается в том, что её применение улучшило ОСШ в КУИ на 6 дБ в каждой ПРР спектра РС и обеспечило высокую разрешающую способность по времени и частоте и точность оценки.

При разделении спектра РС на две ПРР с коэффициентом разборчивости 0,5 суммарное время оценки защищённости РИ в КУИ предлагаемой методикой сокращено более чем в 10 раз, чем при разбиении его на двадцать полос с коэффициентом разборчивости 0,05, что открывает новые возможности при оценке защищённости РИ в технических КУ.

## ЗАКЛЮЧЕНИЕ

### Основные научные результаты диссертации

1. Предложен и обоснован способ формирования показателя защищённости речевой информации в технических каналах утечки сложным измерительным сигналом с большой базой по критерию разборчивости речи в полосах равной разборчивости спектра речевого сигнала в условиях значительной неравномерности амплитудно-частотной характеристики и маскирующих шумов высокого уровня математической зависимостью от нормативного численного значения показателя защищённости гармоническим измерительным сигналом [15, 20].

Установленный нормированный показатель защищённости позволил теоретически обосновать преимущество сложного измерительного сигнала перед гармоническим, равное численному значению его базы, и улучшить значение отношения мощности сигнала к мощности шума в техническом канале утечки информации на 16 дБ при равной длительности измерительных сигналов  $T_c = 4$  с в каждой полосе равной разборчивости спектра речевого сигнала, снизив суммарное время оценки защищённости более чем в 6 раз в сравнении с использованием гармонического измерительного сигнала [3, 11, 19].

2. Разработана методика оценки защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки, с использованием

взаимокорреляционной обработки во временной области сложного измерительного сигнала с большой базой с оптимальными численными значениями исходных данных [1, 2]. Применение функции взаимной корреляции между сложными измерительными сигналами с большой базой в точках излучения и приёма в канале утечки информации позволило за счёт некоррелированности полезного сигнала и шума, а также компенсации с высокой точностью временного запаздывания при использовании производной от функции взаимной корреляции, получить выигрыш в отношении мощности сигнала к мощности шума [4, 5, 9, 11]. Разработанная методика оценки позволила снизить порог обнаружения на 27 дБ и сократить время синхронного накопления сигнала в точке приёма более чем в 10 раз в сравнении с гармоническим измерительным сигналом [1, 9].

3. Разработана методика оценки защищённости речевой информации, маскируемой шумовым сигналом в технических каналах утечки, с использованием взаимокорреляционной частотно-временной обработки сложного измерительного сигнала с большой базой с оптимальными численными значениями исходных данных [1, 2]. Применение функций взаимной корреляции одновременно в частотной и временной областях между сложными измерительными сигналами с большой базой, представленными в аналитическом виде преобразованием Гильберта [12–14], в точках излучения и приёма в канале утечки информации позволило получить выигрыш в отношении мощности сигнала к мощности шума за счёт некоррелированности полезного сигнала и шума и компенсацией с высокой точностью временного запаздывания и частотного сдвига при использовании производных от функций взаимной корреляции по времени и частоте [5, 6]. Разработанная методика позволила улучшить отношение мощности сигнала к мощности шума в канале утечки информации на 6 дБ в каждой полосе равной разборчивости спектра речевого сигнала, значительно повысив разрешающую способность по частоте и времени и обеспечив точность оценки, равную одному периоду дискретизации [2, 12].

Предложенные алгоритмы оценки численных показателей разборчивости речи дискретной обработкой сложных измерительных сигналов с большой базой обеспечивают допустимую скорость и точность оценки [7, 8, 10, 16].

Таким образом, диссертация является законченной научно-квалификационной работой, проведенной в рамках приоритетных направлений развития науки, технологий и техники. Автором исследований представлены теоретические положения, совокупность которых квалифицируют как научно обоснованные решения, направленные на обеспечение реализации алгоритмов и программных средств математической обработки сложных ИС с большой базой, повышающих эффективность защиты от утечки речевой информации, внедрение которых вносит значительный вклад в дальнейшее развитие безопасности и технической защиты информации в Республике Беларусь.

### **Рекомендации по практическому использованию результатов**

Применение способа формирования показателя защищённости речевой информации в техническом канале утечки информации по критерию разборчивости

речи в шумах высокого уровня сложным измерительным сигналом с большой базой и обоснованными с оптимальными численными значениями его исходных данных (длительности  $T_c$  и девиацией частоты  $\pm \Delta f_k$ , перекрывающей каждую из полос равной разборчивости спектра речевого сигнала) математической зависимостью от нормативного численного значения показателя защищённости гармоническим измерительным сигналом представляет собой основу для оценки защищённости с высокой чувствительностью и точностью ПАК [3, 15, 20].

Разработанные методики являются дальнейшим направлением развития и расширения функциональных возможностей ПАК «Филин-А», который в настоящее время используется для проведения контроля защищённости помещений от утечки речевой информации, включая генерацию протоколов, согласно нормативной базе Республики Беларусь [13]. Их рекомендуется использовать с целью проведения оценки защищённости речевой информации в технических каналах утечки информации при маскировании информационных сигналов шумами высокого уровня при разработке тактико-технического задания на ОКР «Разработка и создание переносной автоматизированной измерительной программно-аппаратной системы комплексной оценки эффективности защиты речевой информации 1, 2, 3 категории», шифр ОКР – «ЕРМАК» по Государственной научно-технической программе «Защита информации-3», утвержденной Постановлением Совета Министров Республики Беларусь от 25.02.2016 г. № 153, а также в учебном процессе учреждения образования «Полоцкий государственный университет» по дисциплинам «Методы и средства защиты речевой и видеоинформации», «Технические средства и методы защиты информации», «Основы защиты информации».

## СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЁНОЙ СТЕПЕНИ

### Статьи в научных рецензируемых журналах

1. Железняк, В. К. Представление параметров широкополосного линейно-частотно-модулированного сигнала для оценки разборчивости речи в технических каналах утечки информации / В. К. Железняк, К. Я. Раханов, И. Б. Бурачёнок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2014. – № 12. – С. 2–12.

2. Железняк, В. К. Частотно-временные характеристики широкополосных ЛЧМ-сигналов в полосах равной разборчивости / В. К. Железняк, И. Б. Бурачёнок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – № 4. – С. 2–13.

3. Железняк, В. К. Оценка нормативного показателя защищённости речевого сигнала сложным сигналом с большой базой / В. К. Железняк, И. Б. Бурачёнок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – № 12. – С. 10–14.

4. Железняк, В. К. Оценка разборчивости речи взаимной корреляцией сигнала линейной частотной модуляции в каналах утечки информации / В. К. Железняк, К. Я. Раханов, И. Б. Бурачёнок // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2015. – № 12. – С. 22–27.

5. Бурачёнок, И. Б. Оценка с высокой точностью параметров измерительного сигнала компенсацией его временной задержки в каналах утечки речевой информации / И. Б. Бурачёнок, В. К. Железняк // Доклады БГУИР. – 2016. – № 5. – С. 60–66.

6. Бурачёнок, И. Б. Компенсация временного запаздывания измерительного сигнала на выходе канала утечки речевой информации / И. Б. Бурачёнок, В. К. Железняк // Доклады БГУИР. – 2016. – № 6. – С. 100–106.

### **Статьи в сборниках материалов научных конференций**

7. Бурачёнок, И. Б. Оценка тонкой структуры информационных признаков речевого сигнала / И. Б. Бурачёнок, В. К. Железняк // Современные средства связи : материалы XVIII Междунар. науч.-техн. конф., Минск, 15–16 октября 2013 г. / УО ВГКС; редкол.: А. О. Зеневич [и др.]. – Минск, 2013. – С. 184–186.

8. Burachonak, I. V. Determination of the fine structure information signs of the speech signal / I. V. Burachonak, V. K. Zheleznyak // European and National dimension in research : materials of VI junior researcher's conference, Novopovotsk, 22–23 April 2014 : in 3p. / Polotsk State University. – Novopovotsk, 2014. – Issue 3, part 3: Technology. – P. 147–150.

9. Бурачёнок, И. Б. Представление параметров обработкой сигналом широкополосной линейной частотной модуляции для оценки разборчивости речи в технических каналах утечки информации / И. Б. Бурачёнок, В. К. Железняк // Современные средства связи : материалы XIX Междунар. науч.-техн. конф., Минск, 14–15 октября 2014 г. / УО ВГКС; редкол.: А. О. Зеневич [и др.]. – Минск, 2014. – С. 168–169.

10. Бурачёнок, И. Б. Анализ вейвлет-преобразованием тонкой структуры гласных звуков речевого сигнала / И. Б. Бурачёнок, В. К. Железняк // Теоретические и прикладные аспекты информационной безопасности : материалы междунар. науч.-практ. конф., Минск, 19 июня 2014 г. / УО «Акад. М-ва внутр. дел Респ. Беларусь»; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2015. – С. 124–128.

11. Burachonak, I. V. Method of estimating protection from speech signals leakage through low-frequency technical channels of information leakage based on the correlation function / I. V. Burachonak, V. K. Zheleznyak // European and National dimension in research : materials of VII junior researcher's conference, Novopovotsk, 29–30 April 2015 : in 3p. / Polotsk State University. – Novopovotsk, 2015. – Issue 3, part 3: Technology. – P. 131–135.

12. Бурачёнок, И. Б. Корреляционная частотно-временная обработка широкополосных ЛЧМ-сигналов для оценки разборчивости речи в каналах утечки информации / И. Б. Бурачёнок, В. К. Железняк // Интеллектуальные системы на транспорте «ИнтеллектТранс-2015» : сб. материалов V Междунар. науч.-практ.

конф., Санкт-Петербург, 2015 г. / ПГУПС; под ред. А. А. Корниенко. – СПб., 2015. – С. 286–292.

13. Бураченок, И. Б. Определение разборчивости речи в условиях воздействия шумов высокого уровня / И. Б. Бураченок, В. К. Железняк, К. Я. Раханов // Обеспечение пограничной безопасности и охрана Государственной границы Республики Беларусь : теория и практика : материалы 5-й науч.-практ. конф., Минск, 2015 г. / ГУО «ИПС РБ»; в 3 ч. редкол.: А. Е. Виноградов [и др.]. – Минск, 2015. – Ч. 1. – С. 228–231.

14. Бураченок, И. Б. Обработка широкополосного ЛЧМ-сигнала методом взаимной корреляции по времени и частоте для оценки защищённости речевой информации / И. Б. Бураченок, В. К. Железняк // Комплексная защита информации : материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. / РИВШ. – Минск, 2015. – С. 126–129.

15. Рябенко, Д. В. Оценка нормативных показателей защищённости речевого сигнала в аналоговой и цифровой форме / Д. В. Рябенко, И. Б. Бураченок, В. К. Железняк // Современные средства связи : материалы XX Междунар. науч.-техн. конф., Минск, 14–15 октября 2015 г. / УО ВГКС; редкол.: А. О. Зеневич [и др.]. – Минск, 2015. – С. 142–144.

16. Burachonak, I. V. Analysis of fine structure vowel sound of the speech signal using wavelet transform / I. V. Burachonak, V. K. Zheleznyak // European and National dimension in research : materials of VIII junior researcher's conference, Novopovotsk, 27-28 April 2016 : in 3p. / Polotsk State University. – Novopovotsk, 2016. – Issue 3, part 3: Technology. – P. 183–186.

17. Бураченок, И. Б. Компенсация временного запаздывания и частотного сдвига измерительного сигнала на выходе канала утечки речевой информации / И. Б. Бураченок, В. К. Железняк, Д. В. Рябенко // Современные средства связи : материалы XXI Междунар. науч.-техн. конф., 20–21 октября 2016 г. / Бел. гос. акад. связи; редкол.: А. О. Зеневич [и др.]. – Минск, 2016. – С. 246–248.

### **Тезисы докладов на научных конференциях**

18. Бураченок, И. Б. Алгоритм выделения формант из зашумлённого сигнала / И. Б. Бураченок, В. К. Железняк // Управление информационными ресурсами : материалы X Междунар. науч.-техн. конф., Минск, 13 декабря 2013 г. / Акад. упр. при Президенте Респ. Беларусь; редкол. А. В. Ивановский, А. И. Шемаров, Б. В. Новыш. – Минск, 2013. – С. 125–127.

19. Бураченок, И. Б. Оценка защищённости от утечки речевых сигналов в полосах равной разборчивости с использованием частотно-временных характеристик широкополосных ЛЧМ-сигналов / И. Б. Бураченок, В. К. Железняк // Интеллектуальные системы на транспорте «ИнтеллектТранс-2015» : тез. док. V Межд. науч.-практ. конф., Санкт-Петербург, 2015 г. / ПГУПС. – СПб., 2015. – С. 43–44.

20. Бураченок, И. Б. Критерии оценки защищённости от утечки речевых сигналов / И. Б. Бураченок, В. К. Железняк, Д. В. Рябенко // Молодежь в науке – 2015

: материалы X Междунар. науч. конф., 1–4 декабря 2015 г. / НАН РБ. – Минск, 2015. – С. 234.

21. Бураченок, И. Б. Оценка с высокой точностью параметров измерительного сигнала компенсацией временной задержки в каналах утечки речевой информации / И. Б. Бураченок, В. К. Железняк // Технические средства защиты информации: тез. док. XIV Белорусско-российской науч. конф., Минск, 25–26 мая 2016 г. / БГУИР. – Минск, 2016. – С. 50.

22. Бураченок, И. Б. Компенсация временного запаздывания измерительного сигнала на выходе канала утечки речевой информации / И. Б. Бураченок, В. К. Железняк, Д. В. Рябенко // Технические средства защиты информации: тез. док. XIV Белорусско-российской науч. конф., Минск, 25–26 мая 2016 г. / БГУИР. – Минск, 2016. – С. 16.

### **Патенты**

23. Способ определения разборчивости речи: заявка ВУ / В. К. Железняк, К. Я. Раханов, А. Н. Горбач, А. Г. Филиппович, В. Э. Яскевич, И. Б. Бураченок; заявитель Полоц. гос. ун-т. – № а 20140302; заявл. 02.06.2014.

24. Устройство определения разборчивости речи: заявка ВУ / В. К. Железняк, К. Я. Раханов, А. Н. Горбач, А. Г. Филиппович, В. Э. Яскевич, И. Б. Бураченок; заявитель Полоц. гос. ун-т. – № а 20140303; заявл. 02.06.2014.

## РЭЗІЮМЭ

Бурачонак Ірына Браніславаўна

### **Ацэнка абароненасці гаворкавай інфармацыі з выкарыстаннем ўзаімакарэляцыйнай частотна-часавай апрацоўкі вымяральнага сігнала**

**Ключавыя словы:** крытэрыі ацэнкі абароненасці, складаны сігнал з вялікай базай, нарматыўны паказчык ацэнкі абароненасці гаворкавай інфармацыі, пераборлівасць гаворкі.

**Мэта працы:** абгрунтаванне, распрацоўка і рэалізацыя метадык ацэнкі абароненасці гаворкавай інфармацыі ў тэхнічных каналах ўцечкі для выяўлення вымяральных сігналаў у маскіруючых шумах высокага ўзроўню пры нераўнамернасці АЧХ са значным павышэннем аператыўнасці прадстаўлення вынікаў.

**Метады даследавання і выкарыстаная апаратура:** аналітычнае даследаванне і імітацыйнае мадэліраванне, мадэліраванне і лічбавая апрацоўка складанага сігнала з вялікай базай у шумах высокага ўзроўню выкананы ў асяроддзі MatLAB R2013b. Даследаванне гранічных параметраў ацэнкі абароненасці гаворкавай інфармацыі ўзаімакарэляцыйнай частотна-часавай апрацоўкі складанага вымяральнага сігнала з вялікай базай выканана з дапамогай аналага-лічбавага пераўтваральніка L-Card, E14-440, шумамера SPL-Laboratory USB Noise Meter, аўдыёаналізатара UPP 800 і аналізатара сігналаў FSV4 Rohde&Schwarz.

**Атрыманыя вынікі і іх навізна:** тэарэтычна абгрунтаваны і практычна рэалізаваны: крытэрыі колькаснага значэння велічыні пераборлівасці складаным вымяральным сігналам з вялікай базай і ацэнка абароненасці гаворкавай інфармацыі ў КУІ з дапамогай ўзаімакарэляцыйнай часавай і частотна-часавай апрацоўкамі складанага вымяральнага сігнала з вялікай базай. Распрацаваныя метадыкі забяспечваюць павышэнне адчувальнасці, дакладнасці, дазволу па часе і па частаце і зніжэнне часу ацэнкі абароненасці КУІ. Навізна працы пацверджана пададзенымі патэнтамі на вынаходства.

**Ступень выкарыстання:** вынікі даследаванняў ужываліся пры падрыхтоўцы тэхнічнага задання на ДКП па Дзяржаўнай навукова-тэхнічнай праграме «Абарона інфармацыі 3», зацверджанай Пастановай Савета Міністраў Рэспублікі Беларусь ад 25.02.2016 г. №153; укаранёны ў навучальны працэс ўстановы адукацыі «Полацкі дзяржаўны ўніверсітэт».

**Вобласць прымянення:** абароненасць гаворкавай інфармацыі ў тэхнічных каналах ўцечкі, бяспека інфармацыі, гаворкавая акустыка, апрацоўка сігналаў у шумах высокага ўзроўню.

## РЕЗЮМЕ

Бураченок Ирина Брониславовна

### **Оценка защищённости речевой информации с использованием взаимокорреляционной частотно-временной обработки измерительного сигнала**

**Ключевые слова:** критерий оценки защищённости, сложный сигнал с большой базой, нормативный показатель оценки защищённости речевой информации, разборчивость речи.

**Цель работы:** обоснование, разработка и реализация методик оценки защищённости речевой информации в технических каналах утечки для обнаружения измерительных сигналов в маскирующих шумах высокого уровня при неравномерности амплитудно-частотной характеристики со значительным повышением оперативности представления результатов.

**Методы исследования и используемая аппаратура:** аналитическое исследование и имитационное моделирование, моделирование и цифровая обработка сложного сигнала с большой базой в шумах высокого уровня выполнены в среде MatLAB R2013b. Исследование предельных параметров оценки защищённости речевой информации взаимокорреляционной частотно-временной обработки сложного измерительного сигнала с большой базой выполнено с помощью аналогово-цифрового преобразователя L-Card E14-440, шумомера SPL-Laboratory USB Noise Meter, аудиоанализатора UPP 800 и анализатора сигналов FSV4 Rohde&Schwarz.

**Полученные результаты и их новизна:** теоретически обоснованы и практически реализованы: критерий численного значения величины разборчивости сложным измерительным сигналом с большой базой и оценка защищённости речевой информации в КУИ с помощью временной и частотно-временной взаимокорреляционной обработок сложного измерительного сигнала с большой базой. Разработанные методики обеспечивают повышение чувствительности, точности, разрешения по времени и по частоте и снижение времени оценки защищённости КУИ. Новизна работы подтверждена поданными патентами на изобретение.

**Степень использования:** результаты исследований применены при подготовке технического задания на ОКР по Государственной научно-технической программе «Защита информации 3», утвержденной Постановлением Совета Министров Республики Беларусь от 25.02.2016 г. № 153; внедрены в учебный процесс учреждения образования «Полоцкий государственный университет».

**Область применения:** защищённость речевой информации в технических каналах утечки, безопасность информации, речевая акустика, обработка сигналов в шумах высокого уровня.



## SUMMARY

Burachonak Iryna Bronislavovna

### **Estimation of the speech information protection using cross-correlation time-frequency processing of measuring signal**

**Keywords:** evaluation of the protection criteria, a complex signal with a large base, standard index of estimation of the protection of speech information, speech intelligibility

**Aim of the work:** theoretical foundation, development and practical realization of methods for assessing of speech information protection in technical leakage channels for the detection of measuring signals in a high level masking noise taking into account non-uniformities of the amplitude-frequency characteristics with a significant efficiency increasing of results obtaining.

**Research methods and used facilities:** analytical research and simulation modeling, modeling and simulation and digital signal processing of complex digital signal with a large base in a high level noise are made in MatLAB R2013. Research limiting parameters of the method of the cross-correlation time-frequency processing of complex measurement signal with a large base has made with the help of the analog-to-digital converter L-Card E14-440, the noise level meter SPL-Laboratory USB Noise Meter, audio analyzers UPP 800 and signal analyzer FSV4 Rohde & Schwarz.

**Obtained results and their novelty:** the criterion of numerical significance of intelligibility by complex measuring signal with a large base and the estimation of the speech information protection in information leakage channels using cross-correlation time and time-frequency processing of complex measuring signal with a large base have theoretically grounded and practically implemented. The developed methods provide increase of sensitivity, accuracy, time resolution and frequency resolution and time reduction for estimation of the information protection in information leakage channels. The novelty of the work is confirmed by filed patents.

**Use guidelines:** the results of research have applied in the preparation of technical specifications for R & D by the State scientific and technical program "Information Security 3", approved by the Council of Ministers on February 25, 2016 №153, implemented in the educational process of the educational establishment "Polotsk State University" .

**Application area:** protection of speech information in information leakage channels, speech acoustic, signal processing in the level high noise.

*Научное издание*

**Бураченок Ирина Брониславовна**

**ОЦЕНКА ЗАЩИЩЁННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ  
С ИСПОЛЬЗОВАНИЕМ ВЗАИМОКОРРЕЛЯЦИОННОЙ  
ЧАСТОТНО-ВРЕМЕННОЙ ОБРАБОТКИ  
ИЗМЕРИТЕЛЬНОГО СИГНАЛА**

**АВТОРЕФЕРАТ**

**диссертации на соискание учёной степени  
кандидата технических наук**

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

Подписано в печать      Формат 60×84 1/16. Бумага офсетная. Гарнитура «Гаймс».  
Отпечатано на ризографе. Усл. печ. л.      Уч.-изд. л.      Тираж      экз. Заказ

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