

Парламентское собрание Союза Беларуси и России
Постоянный Комитет Союзного государства
Оперативно-аналитический центр
при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Полоцкий государственный университет



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)
К63

К63

Комплексная защита информации : материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)

2. Палий А.И. Радиоэлектронная борьба: (Средства и способы подавления и защиты радиоэлектронных систем). - М.: Воениздат. 1981. – 320 с.: ил.

3. Саванович, С.Э. Радиоэкранирующие свойства электромагнитных экранов на основе влагосодержащего керамзита // С.Э. Саванович, В.Б. Соколов // Доклады БГУИР. 2014 №4 (82). С. 48 – 51.

4. Саванович, С.Э. Влияние размеров фракций влагосодержащего керамзита на экранирующие характеристики экранов ЭМИ // С.Э. Саванович, Т.В. Борботько, В.Б. Соколов, М.В. Русакович // Доклады БГУИР. 2014 №8 (86). С. 36 – 40.

5. Неамах, М.Р. Радиоэкранирующие модульные конструкции на основе порошкообразных материалов / М.Р. Неамах, О.В. Бойправ, Т.В. Борботько, Л.М. Лыньков, В.Б. Соколов; под ред. Л.М. Лынькова. – Мн. : Бестпринт, 2013. – 210 с.

ИЗМЕРИТЕЛЬНЫЕ СИГНАЛЫ ДЛЯ ОЦЕНКИ ЗАЩИЩЁННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ

И.Б. БУРАЧЁНОК, В.К. ЖЕЛЕЗНЯК

Полоцкий государственный университет

Введение. Сегодня задача защиты конфиденциальных переговоров является достаточно дорогим и сложным мероприятием, а совершенствование средств извлечения речевой информации (РИ) и новые методы её обработки в шумах высокого уровня определяют необходимость улучшения важнейших параметров её защиты. Отсутствие в соответствующих службах аппаратуры контроля, удовлетворяющей современным требованиям, обуславливает появление технических каналов утечки информации (КУИ) при кажущемся достаточным уровне защиты. Поэтому необходимость усовершенствования средств противодействия перехвату (аппаратуры контроля и защищённости РИ по техническим КУИ), обеспечивающих повышение точности, помехоустойчивости, чувствительности и приемлемое время обработки результатов, определяют актуальность представленной работы.

Целью работы является анализ и синтез измерительных сигналов (ИС), используемых для оценки защищённости РИ в КУИ в условиях шумов высокого уровня при значительных неравномерностях АЧХ для выявления наиболее значимых их свойств, позволяющих получить численные значения параметров оценки защищённости с высокой точностью и разрешающей способностью по частоте и времени при повышении оперативности представления результатов.

Защищённость РИ в КУИ объективно оценивают выделением слабых ИС из шумов высокого уровня на основании измерений отношения мощности акустического сигнала к мощности маскирующего (фонового) шума (отношение сигнал/шум) в точке приёма на выходе КУИ за пределами помещения, предназначенного для конфиденциальных переговоров, и, затем, определяют коэффициент разборчивости речи [1]. Защита РИ в КУИ считается достаточной, если в местах возможной установки акустических и вибрационных первичных измерительных преобразователей величина показателя измеренного отношения сигнал/шум не превышает нормативного значения. Для того, чтобы учесть основные факторы, влияющие на величину разборчивости речи, отношение сигнал/шум определяют на нескольких несовпадающих частотах (средних частотах 1/3-октавных или 20-ти полосах равной разборчивости (ПРР)) спектра речевого сигнала (РС). При контроле качества защищённости РИ в КУИ используют ИС: либо белый шум [2], либо гармонический сигнал ГОСТ 16465–70 [3]. В работе [4] оценку защищённости

РИ в КУИ предложено проводить с применением сложных ИС (иногда их называют широкополосными либо шумоподобными [5]) с обоснованными исходными данными в ПРР спектра РС [2] при использовании функций корреляции [5].

В представленной работе проведён сравнительный анализ ИС, используемых при оценке защищённости РИ в КУИ, при одинаковых условиях воздействия и рассмотрено влияние различных видов искажений АЧХ на основные параметры их спектров и автокорреляционных функций (АКФ) [5].

Шумовой сигнал, применяемый для оценки защищённости РИ в КУИ, – это случайный процесс, характеризуемый нормальным законом распределения плотности вероятности. Основными параметрами такого сигнала являются – математическое ожидание, дисперсия и АКФ, которая имеет высокий пик (представимый как дельта-функция Дирака [6]) в нуле и равна нулю во всех других точках. Так как при измерении уровней шумовых акустических сигналов используют шумомер, то следует отметить, что он вносит значительные методические погрешности в результаты измерений, так как пропускает как помехи, вызванные реверберацией помещения, так и искусственные, используемые для маскирования РС. В результате происходит ухудшение помехоустойчивости обработки, что значительно снижает точность оценки защищённости РИ в КУИ.

Гармоническому ИС, в отличие от шумового, не присущи выше перечисленные недостатки, снижающие точность оценки защищённости РИ в КУИ. Однако, обработка гармонического ИС на средних частотах ПРР допускает увеличение погрешности при оценке в КУИ с явно выраженными неравномерностями АЧХ, например, в условиях искусственного зашумления, используемого при маскировании полезного РС. На точность оценки существенное влияние оказывает и длительность ИС. Исследования корреляционных свойств гармонических ИС, расположенных на средних частотах ПРР спектра РС, показывают, что формы огибающих их АКФ зависят от длительности сформированного ИС и не зависят от его частоты.

Особенностью АКФ гармонического ИС является то, что её огибающая представляет собой треугольник. Чем больше длительность ИС, тем меньше наклон огибающей его АКФ, что снижает точность определения её максимального значения. Согласно исследованиям, при наложении ограничения на время воздействия гармонического ИС его параметры ухудшаются, что в свою очередь, снижает возможность реализации критерия достоверности воспроизведения с высокой точностью.

Предлагаемый для оценки сложный ИС описывается математической моделью [4]. Формирование сложного ИС с регулируемыми уровнями эффективной длительности позволяет осуществить функция вида: $f(t) = e^{-(\beta t)^2}$, представляющая собой гауссов импульс, совпадающий по форме с графиком нормального распределения вероятностей, где $\beta = \frac{1}{T_c} \cdot 2 \cdot \sqrt{-\ln(a)}$ – коэффициент наклона, а $t \in \left[-\frac{T_c}{2}; \frac{T_c}{2}\right]$, a – коэффициент задаваемого уровня эффективной длительности. Особенностью такого сигнала является то, что его форма совпадает с формой спектральной характеристики.

Важным свойством рассматриваемых ИС является и ширина главного лепестка огибающей АКФ [4], которая обратно пропорциональна девиации частоты сигнала [5]. Все исследуемые ИС имеют значительную девиацию частоты Δf , и поэтому главный лепесток АКФ получается весьма узким. Самый узкий главный лепесток АКФ имеет сложный ИС в двадцатой N_{20} ($f = [7250 \div 10000]$ Гц, $\Delta f_k = 1375$ Гц), самый широкий – в третьей N_3 ($f = [570 \div 710]$ Гц, $\Delta f_k = 70$ Гц) ПРР спектра РС.

С точки зрения корреляционных свойств, сложным ИС с прямоугольной огибающей $a = 1$ присущ недостаток: высота двух первых симметричных боковых лепестков составляет $\approx 0,212$ от высоты центрального лепестка. Чем меньше значение a , тем больше ширина главного лепестка огибающей АКФ сигнала и меньше уровень боковых лепестков. Определённого снижения уровня боковых лепестков можно добиться, применяя в качестве измерительных сложные сигналы с непрямоугольными (типа колокола) [7] огибающими, что в условиях шумов высокого уровня повышает точность определения временного положения ИС.

Использование полностью колоколообразного сложного ИС удовлетворяет условию минимизации боковых лепестков АКФ и позволяет получить оптимальное решение для обеспечения высокой разрешающей способности по частоте, однако приводит к ухудшению разрешающей способности по времени. Чтобы устранить данный недостаток, необходимо увеличивать длительность ИС, что в нашем случае является критичным.

Форма огибающих АКФ (рис. 1), принятых в КУИ сложных ИС с регулируемыми уровнями эффективной длительности, отображает даже незначительные их искажения.

Наиболее точно с использованием огибающих АКФ передаются искажения АЧХ ИС с меньшим значением уровня эффективной длительности сигнала a . Использование данной характеристики для оценки искажений гармонических ИС не обладает такой информативностью.

Анализ искажений и их влияния на оценку защищённости РИ в КУИ при использовании сложных ИС с различными уровнями эффективной длительности в одинаковых условиях зашумления показал, что с уменьшением уровня их эффективной длительности уменьшается и их средняя мощность.

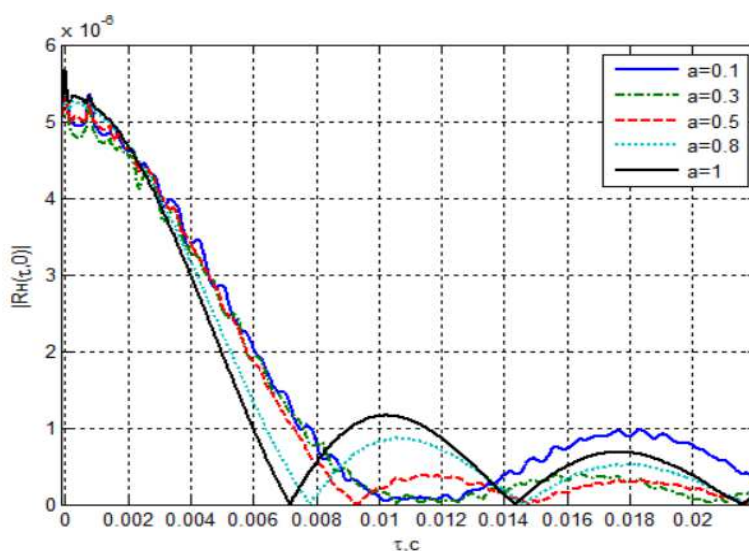


Рис. 1. – Огибающие АКФ сложных ИС с регулируемыми уровнями эффективной длительности в одинаковых условиях зашумления

Вывод. На основании проведённого анализа ИС в ПРР спектра РС при использовании наиболее значимых их свойств: спектрального представления и АКФ, установлено, что применение для оценки защищённости РИ в КУИ сложного ИС в отличие от применения гармонического ИС позволяет полностью контролировать возникающие искажения АЧХ в пределах каждой из ПРР, на которые разбивается спектр РС, а не в отдельных точках на числовой оси. Исследование деформаций АЧХ гармонического

и сложных ИС с регулируемым уровнем эффективной длительности при одинаковых воздействиях в каждой ПРП показывают, что наилучшие результаты оценки позволяют получить сложные ИС с регулируемым уровнем эффективной длительности $a = 1$. Если использовать $a = 0,8$, то это снижает точность оценки в 1,14 раза, а использование $a = 0,1$ – в 2,3 раза. Однако использование колоколообразного сложного ИС удовлетворяет условию минимизации боковых лепестков АКФ, что является важным при обнаружении ИС на фоне шумов. С учётом сказанного рекомендуется оценку проводить, используя ИС с регулируемым уровнем эффективной длительности $a = 0,8$ длительностью $T_c = 4$ с.

Список литературы

1. Железняк В. К. Защита информации от утечки по техническим каналам: учеб. пособие. СПб.: ГУАП. 2006. 188 с.
2. Левин Б. Р. Теоретические основы статистической радиотехники. М.: Сов. Радио. 1969. 752 с.
3. ГОСТ 16465–70 (с изменением №1). Сигналы радиотехнические измерительные. Термины и определения. М., ИПК Издательство стандартов. 2008. 30 с.
4. Железняк В.К., Раханов К.Я., Бураченко И.Б. Представление параметров широкополосного линейно-частотно-модулированного сигнала для оценки разборчивости речи в технических каналах утечки информации // Вестн. Полоц. гос. ун-та. Серия С Фундаментальные науки. 2014. №12. с. 2-12.
5. Варакин Л. Е. Теория сложных сигналов. М.: Советское радио. 1970. 376 с.
6. Акимов П. С., Евстратов Ф. Ф., Захаров С. И. и др. Обнаружение радиосигналов [Под ред. А. А. Колосова]. М.: Радио и связь. 1989. 288 с.
7. Слока В. К. Вопросы обработки радиолокационных сигналов. М.: Сов. Радио. 1970. 256 с.

РЕСПУБЛИКАНСКАЯ ПЛАТФОРМА КАК ГОСУДАРСТВЕННОЕ ОБЛАКО

А.Л. ВАХТЕРОВ, С.Ф. КАЗЮЧИЦ

ООО Белорусские облачные технологии

Стратегической целью проектов компании beCloud было создание национальной облачной платформы, которая позволит государству и бизнесу существенно снизить затраты на ИТ. Запуск современной облачной платформы на базе нового ЦОДа предоставляет возможность эффективно использовать инструменты в области управления ИТ-инфраструктурой и ее безопасностью.

Компания beCloud предоставляет следующие виды услуг:

- 1) Программное обеспечение как услуга (Software as a Service, SaaS)
- 2) Инфраструктура как услуга (Infrastructure as a Service, IaaS)
- 3) ЦОД как услуга (Data Center as a Service, DCaaS) – предоставление места в серверной стойке.

Компания beCloud законодательно определен как оператор Республиканской Платформы (АИС РП), которая предназначена для размещения программно-технических средств, информационных ресурсов и информационных систем государственных органов и иных государственных организаций