УДК 681.391

В. Н. Журавльов, к. т. н.;
О. О. Архипова, студ.

КОРЕЛЯЦІЙНИЙ МЕТОД ЕКСПЕРИМЕНТАЛЬНОГО АНАЛІЗУ ФУНКЦІЇ ЕФЕКТИВНОСТІ МАСКУВАННЯ МОВНОГО СИГНАЛУ

Проаналізовано метод цифрової кореляційної обробки тестового мовного сигналу, який дозволяє на основі розрахунку коефіцієнта кореляції обґрунтувати аналітичну оцінку параметра функції ефективності адитивного маскування мови. Запропонований метод дозволяє застосовувати в якості тестових сигналів ключові слова дикторів, і, таким чином, адаптувати спектральну щільність потужності маскувального сигналу, для приховання інформації мовного сигналу обмеженої кількості співрозмовників.

Вступ. Постановка задачі

Під час атестації й проектування систем технічного захисту мовних сигналів (МС) у виділених приміщеннях від витоку по акустичних каналах несанкціонованого доступу (НСД), основним параметром, що визначає як показник ефективності маскування, так і категорію захисту, є осереднене на деякому інтервалі T значення функції $W(t)$, $t \in [T]$ словесної розбірливості, яку зараз визначають інструментально-розрахунковим методом [1]. Даний метод припускає, що тестовий і маскувальний сигнали характеризуються рівномірним розподілом спектральної щільності потужності (СЩП) $N(\Delta\omega, t)$, тобто спектром «білого шуму». Акустичне поле сигналу каналу витоку припускають плоским, акустичний опір середовища поширення — активним, а АЧХ рецептора каналу витоку на інтервалі часу T — постійним. Ґрунтуючись на цих припущеннях, відношення сигнал—завада $SN(\Delta\omega, t)$ розраховується як логарифм відношення усереднених на інтервалі часу T акустичних тисків, що можливо тільки для моногармонічних сигналів, що аналізуються, при активному вхідному опорі рецептора звукового тиску.

Основні протиріччя інструментально-розрахункового методу до інформаційно-фізичних процесів маскування мовного сигналу, на думку автора [2], полягають у такому. *Модель мовного сигналу* $si(t)$ реалізується детермінованими (гармонічними) або стохастичними (шумовими) сигналами з нормальним розподілом щільності ймовірності амплітуд, які не містять інформації $I(t)$ МС. *Модель сигналу маскування* реалізується сигналом «білий шум», що характеризується рівномірним законом розподілу функції щільності ймовірності потужності $N(t)$ в смузі частот $\Delta\omega$. Експериментально доведений факт невідповідності даної моделі сигналів промислових генераторів акустичного маскування [3]. *Часовий інтервал* T точкового аналізу параметра ефективності $W(t)$ не пов'язаний з інформаційними параметрами моделюючої функції мовослухового процесу. Таким чином, можна зробити висновок про протиріччя наявних спектрально-часових моделей мовослухового процесу щодо результатів експериментальних досліджень і природних методів синтезу й аналізу інформаційної складової $I(t)$ мовного сигналу. Наявні моделі погіршують параметр вірогідності об'єктивних моделей і методів аналізу ефективності технічних засобів маскування мовної інформації.

Вищенаведені аргументи *дозволяють вважати актуальною науково-технічну задачу* підвищення параметра достовірності методів оцінки функції ефективності маскування мови в технічних каналах витоку інформації.

Основна частина

Передумовами для розробки робочої гіпотези методу були такі факти експериментальних досліджень [4]. Сучасні спектрально-часові моделі мовослухового процесу припускають носієм 100 % інформації $I(t)$ часову реалізацію МС $si(t)$, що є випадковим процесом з девіацією параметрів функції щільності розподілу ймовірності [5]. Сигнал маскування $sn(t)$, за визначенням, — випадковий процес, таким чином у точці НСД відбувається додавання спектральних щільностей потужності $SN(\Delta t, \Delta\omega)$ сигналів $su(t) = si(t) + sn(t)$. Точкову оцінку функцій спектральної щільності потужності (СЩП) $SN(\Delta t, \Delta\omega)$ сигналів $su(t)$ і $si(t)$ доцільно аналізувати на часовому інтервалі психофізіологічної стаціонарності інформаційної модулювальної функції мови (т.зв. «складовому інтервалі» $\Delta t = T_a$ = (15...30) мс) [6].

Для точкової оцінки параметра тісноти зв'язку між часовими реалізаціями мовного $si(t)$ й маскованого сигналів $su(t)$ еквівалентного параметру ефективності маскування (розбірливості $W(t)$ [7]) у точці НСД, нами запропонований метод [2, 8], в основі якого лежать такі передумови.

Детермінованою характеристикою випадкового процесу є СЩП $N(\Delta\omega, t)$, що показує, як розподілена потужність сигналу в досліджуваній смузі частот $\Delta\omega$. СЩП випадкового процесу і його АКФ зв'язані перетворенням Фур'є (теорема Вінера-Хінчіна)

$$N(\Delta\omega, t) = \int_0^{T_a} R_{ss}(\tau)\, e^{i\omega t} d\tau . \qquad (1)$$

Зобразимо досліджувані сигнали $s(\Delta\omega, t)$ моделлю у вигляді впорядкованого набору фрагментів, що знаходяться впритул один до одного, довжиною T_a

$$s(\Delta\omega, t) = \sum_{i=1}^{N} s_i(\Delta\omega, t), \qquad (2)$$

де $s_i(t) = \begin{cases} s(t), & t \in [t_i, t_i + T_a); \quad t_i = t_0 + (i-1)T_a, \quad i = \overline{1, N}; \\ 0, & t_i + T_a < t \le t_i. \end{cases}$

Для спрощення подальшого аналізу припустимо, що в межах кожного відмінного від нуля фрагмента значень сигналу $s(t)$ амплітуди його центровані й розподілені, у загальному випадку, за нормальним законом з дисперсією $D[s(t)]$.

У зв'язку з тим, що залежності мовного $si(\Delta\omega, t)$ й маскованого $su(\Delta\omega, t)$ сигналів не мають функціонального характеру, тобто рівномірній зміні однієї ознаки відповідає зміна іншої ознаки в середньому, для оцінки тісноти зв'язку між досліджуваними сигналами можна застосувати методи кореляційного аналізу СЩП, зокрема коефіцієнт кореляційного відношення Пірсона [9]:

$$r = \frac{\sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \overline{x})^2} \sqrt{\sum_{i=1}^{N} (y_i - \overline{y})^2}}, \qquad (3)$$

де: x й y — досліджувані СЩП, $\overline{x}$ й $\overline{y}$ — вибіркові середні значення, що визначаються (зокрема для x) як $\overline{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$.

Таким чином, за системний об'єктивний параметр захищеності МС у точці доступу засобів технічної розвідки супротивника до каналу НСД можна прийняти коефіцієнт кореляційного відношення Пірсона, що визначається згідно з (3), і розраховується для функцій СЩП $N(\Delta\omega, t)$ на т.зв. «складових» часових інтервалах T_a квазістаціонарного стану мовних сигналів.

Результати експериментальних досліджень

Методика експерименту. Аналіз сигналів проводився на персональному комп'ютері, що оснащений звуковою картою SB Audigy2, з діапазоном квантування 16 біт і частотою дискретизації f_s

= 48 кГц, відношенням сигнал — завада порядку 80 дБ. Програмування алгоритму методу розроблялося в середовищі пакета програм MatLab 6.5. Параметр сегментації сигналу $si(\Delta\omega, t)$ на часові відрізки відповідав складовий постійної часу T_a = 23 мс. Властивість центрованості реалізацій забезпечується відповідною процедурою програми. Інтервал дискретизації $1/f_s$ = 20 мкс значно менше максимального інтервалу кореляції $1/2\omega_2$ сигналу $si(\Delta\omega, t)$, що дозволяє стверджувати про дієвість вибіркових оцінок математичних очікувань і дисперсій, що розраховують при аналізі. У якості МС $si(\Delta\omega, t)$ аналізувалося контрольне слово «лето», що містить голосні й приголосні, а також вокалізовані і невокалізовані фонеми. Контрольне слово вимовляється чоловічим і жіночим голосами. В якості сигналів маскування $sn(\Delta\omega, t)$ досліджувалися три процеси: зі спектральною щільністю потужності «білого шуму» («HG»), масив значень якого формувався стандартною процедурою пакета MatLab; сигнал промислового генератора типу «ANG2200» («Nang») і сигнал (*Nhb*) синтезований на кафедрі фізико-технічних засобів захисту інформації КПІ. Перед проведенням аналізу задавалося інтегральне значення відношення сигнал—завада $SN(\Delta\omega, t)$, з постійною інтегрування рівною тривалості контрольного слова, розраховане за загальноприйнятою методикою відношень середньоквадратичних значень амплітуд сигналу й завади. Маскування сигналу $si(\Delta\omega, t)$ виконувалося на інтервалі тривалості контрольного слова методом адитивного маскування СЩП (1). Для проведення кореляційного аналізу сигнал $N_{su}(\Delta\omega, t)$ сегментувався (2) на N часових інтервалів тривалістю T_a. На кожному інтервалі аналізу T_a розраховувалися точкові оцінки коефіцієнта кореляції $r(SN)$ (3).

Результати експериментів. На рис. 1, 2, 3 наведені результати моделювання процесу маскування МС при зміні інтегрального параметра сигнал—завада від 10 до — 30 дБ. На рисунках: лівий стовпчик — тривимірні залежності коефіцієнта кореляції від відношення сигнал—завада і кількості реалізацій $r(SN) = f(SN, N)$, середній стовпчик — залежність математичного очікування коефіцієнта кореляції $M\left[r(SN)\right] = f(SN)$ від відношення сигнал—завада, правий стовпчик — залежність середньоквадратичного відхилення коефіцієнта кореляції $\sigma\left[r(SN)\right] = f(SN)$ від відношення сигнал—завада з 5 % довірчим інтервалом.

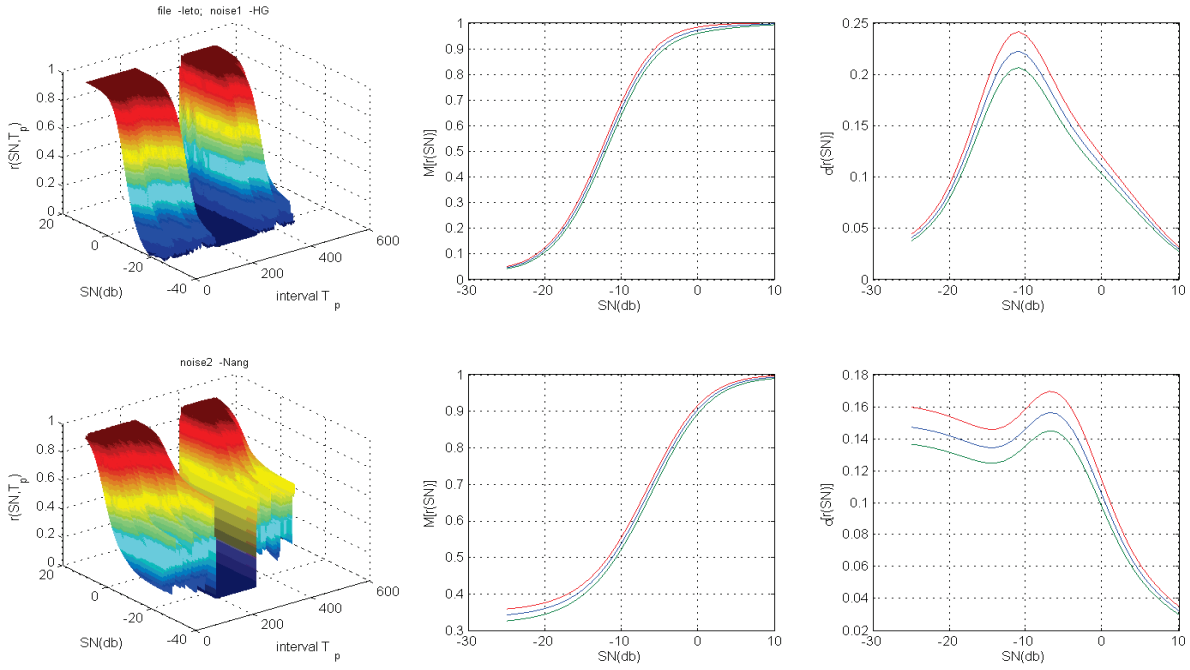

Рис. 1. Графіки залежностей значень точкових оцінок коефіцієнта кореляції $r = f(SN, T_a)$ від інтегрального значення відношення сигнал—завада для чоловічого голосу й сигналів маскування *HG* й Nang

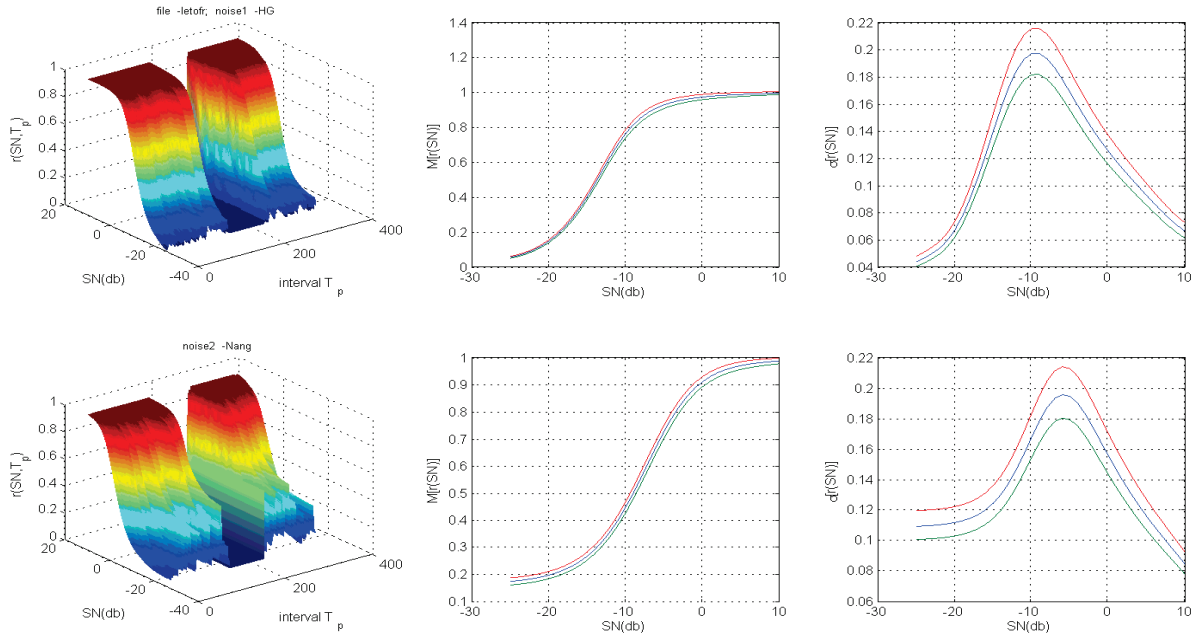

Рис. 2. Графіки залежностей значень точкових оцінок коефіцієнта кореляції $r = f(SN, T_a)$ від інтегрального значення відношення сигнал—завада для жіночого голосу й сигналів маскування HG й Nang

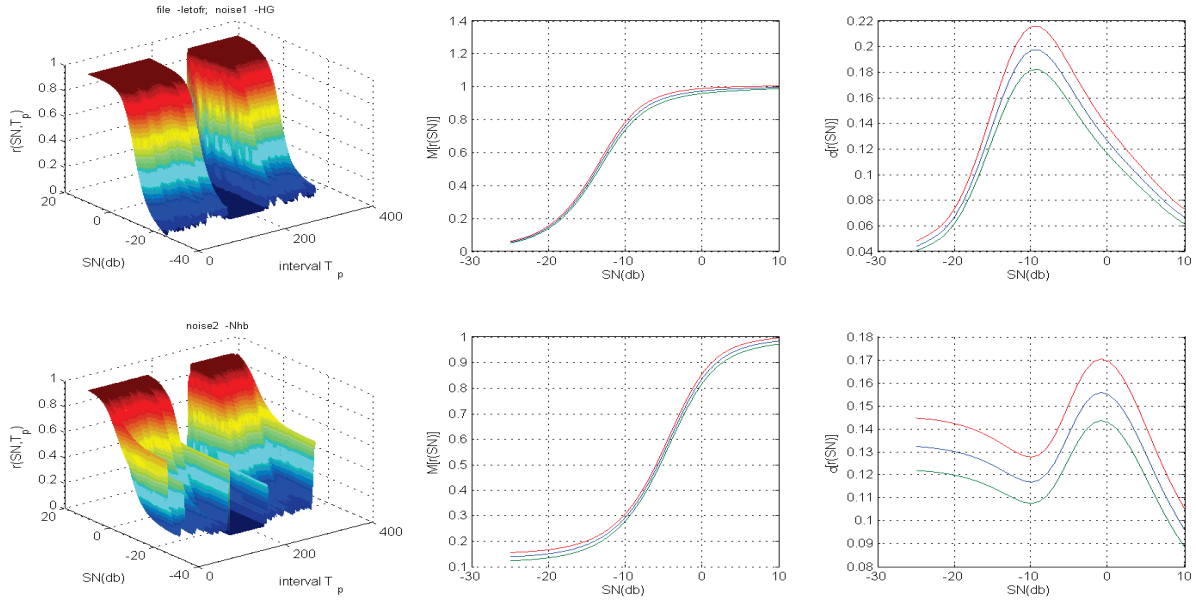

Рис. 3. Графіки залежностей значень точкових оцінок коефіцієнта кореляції $r = f(SN, T_a)$ від інтегрального значення відношення сигнал—завада для жіночого голосу й сигналів маскування HG й Nhb

Провівши аналіз графіків можна зробити висновки, що характеристики залежності коефіцієнта кореляції $r(t) = f(SN, T_a)$ показують більшу ефективність сигналу Nang у порівнянні із сигналом «білий шум» у всьому діапазоні змін інтегрального параметра сигнал—завада, такий же висновок можна зробити про сигнал Nhb стосовно Nang.

Характер зміни залежності $r(t) = f(SN, T_a)$ для сигналу Nang й Nhb показує внутрішні кореляційні зв'язки сигналів контрольного слова й маскувальних сигналів, особливо це проявляється на інтервалі часу активності фонеми «е». Характер зміни залежності $r(t) = f(SN, T_a)$ для МС, вимовлених чоловічим і жіночим голосами, показує різний ступінь адаптації маскувальних сигналів до сигналів контрольного слова.

Залежність математичного очікування $M\left[r(SN)\right] = f(SN)$, відображає порівняльну ефектив-

ність сигналів маскування стосовно контрольного слова, для сигналів Nang й Nhb вона вище ніж у НВ, даний факт підтверджує результати раніше проведених досліджень [2] і може бути непрямим підтвердженням адекватності запропонованого методу.

Максимум залежності середньоквадратичного відхилення $\sigma\left[r(SN)\right] = f(SN)$, в якому спостерігається максимальна дисперсія довірчих інтервалів, може ідентифікувати оптимальне значення відношення W/SN й вимагає додаткових артикуляційних досліджень.

Висновки. Напрямки подальших досліджень

Запропонована й досліджена аналітична функція (3) ефективності маскування мови, яка, не базуючись на спектральних моделях мовослухового процесу, є мірою оцінки тісноти кореляційного зв'язку між часовими реалізаціями спектральної щільності потужності мовного сигналу й сигналу в точці НСД.

Результати проведених експериментальних досліджень ефективності маскування реальних мовних сигналів добре узгоджуються з результатами раніше проведених артикуляційних випробувань [2].

Розроблений метод і методика дозволяють застосовувати як тестові сигнали ключові слова конкретних дикторів, і, таким чином, адаптувати потужність сигналу маскування у виділених приміщеннях ОІД.

Можна визначити такі області застосування методу: атестація виділених приміщень ОІД й автоматична адаптація потужності сигналу маскування до інформаційної складової мовного сигналу диктора в режимі реального часу.

Адекватність методу й, відповідно, достовірність запропонованої функції ефективності маскування необхідно підтвердити проведенням артикуляційних випробувань за стандартною методикою для української мови.

СПИСОК ЛІТЕРАТУРИ

1. Дворянкин С. В. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам [Текст] / С. В.Дворянкин, Ю. К. Макаров, А. А. Хорев // Защита информации. INSIDE. 2007. — № 2. — С. 18—25.

2. Журавлёв В. Н. Анализ метода расчета параметра эффективности маскування речи в технических каналах утечки [Текст] / В. Н. Журавлёв, Е. А. Архипова // Радіоелектроніка, інформатика, управління. — 2007. — № 15. — С. 57—64.

3. Прокофьев М. И. Анализ результатов артикуляционных и сегментальных испытаний сигналов маскирования речи [Текст] / М. И. Прокофьев, В. Н. Журавлев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2006. — № 13. — С. 14—23.

4. Галунов В. И. Современные речевые технологии [Электронный ресурс]: Обзорная статья — СПб.: 1999, — Режим доступа : http://www.auditech.ru/article/cntrid/click.php?action=download&id=5. — Загл. с экрана.

5. Журавлёв В. Н. Экспериментальные исследования зависимости формы фонем речевого сигнала от их информационного содержания [Текст] / В. Н. Журавлёв, И. В. Жуковицкий // Сучасні інформаційні технології на транспорті, промисловості та освіті: міжнародна науково-практична конференція. — Дніпропетровськ, ДНУЖТ, 2008. — С. 59—60.

6. Фант Г. Акустическая теория речеобразования [Текст] / Г. Фант; пер. с анг. В. С. Григорьева; ред. В. С. Григорьева. — М.: Наука, 1964. — 284 с.

7. Михайлов В. Г. Измерение параметров речи [Текст] / В. Г. Михайлов, Л. В. Златоустова — М.: Радио и связь, 1987. — 168 с.

8. Архипова О. О. Метод розрахунку функції ефективності маскування мови / О. О. Архипова // Теоретичні і прикладні проблеми фізики, математики та інформатики: VI Всеукр. наук.-практ. конф, 18 квітня 2008 р.: тези доповідей. — К., 2008. — С. 76—77.

9. Гайдышев И. Анализ и обработка данных [Текст] / И. Гайдышев. — СПб: Питер, 2001. — 752 с.

Рекомендована кафедрою захисту інформації

Надійшла до редакції 8.09.08
Рекомендована до друку 20.10.08

Журавльов Володимир Миколайович — доцент, ***Архипова Олена Олександрівна*** — магістрант.
Кафедра інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут»