УДК 004.421.5(045) **Давлет'янц О.І., Бурзаковський Р.В.**

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМ КАНАЛОМ

Для захисту інформації від витоку акустичним каналом застосовують пасивні і активні методи. Пасивні методи мають на меті послаблення акустичних сигналів на межі контрольованої зони до рівня, при якому неможливе їх виділення засобами розвідки на фоні природних шумів. При застосуванні активних методів створюються маскуючі акустичні, вібраційні завади для зменшення співвідношення сигнал/шум на границі контрольованої зони для унеможливлення їх виділення. [1, 2]

Одним із поширених активних методів захисту інформації є зашумлення, яке полягає у застосуванні маскуючих (шумових) сигналів. Сам маскуючий сигнал найчастіше формують у вигляді «білого шуму» [2], для перекриття усього діапазону частот небезпечного сигналу. При цьому не враховується спектральна характеристика останнього. Зрозуміло, що в такому випадку потужність такого генератора «білого шуму» буде використовуватись неефективно.

Ефективність маскування можна значно підвищити, якщо для маскування застосовувати процеси з характеристиками, подібними до характеристик небезпечного сигналу. Однак, варто звернути увагу на те, що генератори шуму в такому випадку повинні забезпечувати регулювання характеристик формованих випадкових процесів в широкому діапазоні, або бути вузькоспеціалізованими. Серед представлених на сьогодні на ринку таких пристроїв більшість з них досить габаритні і складні в користуванні та обслуговуванні.

Задача формування випадкових процесів із заданими характеристиками значно спрощується при використанні персонального комп'ютера, який є присутнім практично на всіх об'єктах, що потребують захисту. З метою зниження витрат на захист інформації, комп'ютер можна використовувати для генерації маскуючого сигналу. При цьому такий генератор може працювати у фоновому режимі і не заважатиме оператору виконувати основні штатні задачі.

Для спрощення каналів передачі маскуючого сигналу до місць його відтворення пропонується використовувати широтно-імпульсну модуляцію (ШІМ). В такому випадку передаватись буде послідовність імпульсів, тривалість яких буде випадковою величиною із заданими (необхідними) характеристиками. За необхідності збільшення потужності шумового сигналу при заданому виді ШІМ замість дорогого підсилювача можна використовувати елементарну ключову схему, керовану формованими комп'ютером імпульсними сигналами.

Основна складність реалізації запропонованого методу захисту інформації полягає у визначенні необхідних характеристик випадкових тривалостей і інтервалів слідування імпульсів в послідовності, які б забезпечили можливість формування простими технічними засобами маскуючого сигналу із заданими статистичними характеристиками

Точне розв'язання цієї задачі пов'язане з необхідністю аналізу проходження випадкових процесів через нелінійні інерційні кола, а також синтезу цих кіл для отримання необхідних характеристик випадкового процесу.

Проілюструємо працездатність запропонованого методу на прикладі спрощеної процедури синтезу алгоритму формування маскуючого сигналу для захисту інформації від витоку акустичним каналом. Спектральна щільність мовного сигналу, усереднена по чоловічим і жіночим голосам [3], представлена на рис.1а, на рис.1б наведена апроксимація його щільності розподілу [4].

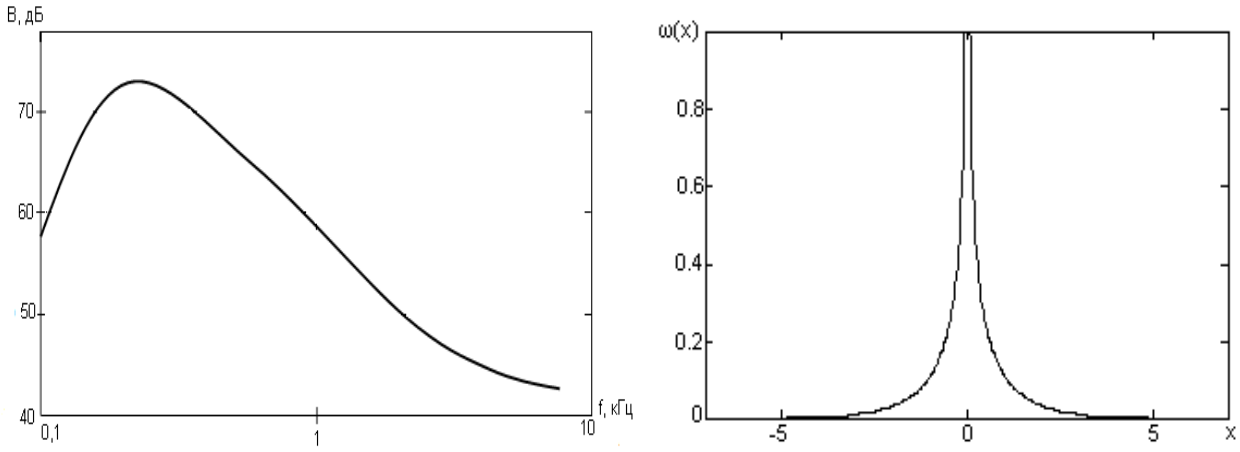

Рис. 1. Характеристики мовного сигналу:
а – спектральна щільність, б – щільність розподілу.

Аналітична форма запису щільності розподілу має вигляд

$$\omega(x) = \sqrt{\frac{\sqrt{3}}{8\pi\sigma|x|}} exp\left[-\frac{\sqrt{3}}{2\sigma}|x|\right],\ x \in (-\infty;\infty). \qquad (1)$$

Пік щільності розподілу (1) в області нульового значення аргументу (див. рис.1б) зумовлений наявністю в мовному сигналі пауз між словами і фразами. Моделювати паузи в маскуючому сигналі недоречно. Тому, нехтуючи паузами, щільність розподілу мовного сигналу можна апроксимувати нормальним законом розподілу.

Для реалізації запропонованого методу формування випадкових сигналів спочатку необхідно змоделювати програмними засобами імпульсну послідовність із характеристиками, які дозволять отримати потрібну спектральну щільність вихідного процесу.

Для отримання імпульсної послідовності з необхідними характеристиками слід провести нормування спектральної щільності небезпечного сигналу, потім побудувати інтегральну функцію нормованої кривої. Далі, використовуючи обернену функцію нормованої кривої і послідовність рівномірно розподіленої величини, можна отримати послідовність, значення якої будуть визначати випадкові параметри модульованих за частотою і тривалістю імпульсів.

Задача дещо спрощується, якщо можлива апроксимація необхідної спектральної характеристики однією з відомих кривих розподілу.

Характер зміни кривої спектральної щільності (рис.1а) аналогічний поведінці кривої, що описує закон Релея

$$(f) = \frac{f}{\sigma^2}\exp\left(-\frac{f^2}{2\sigma^2}\right), f \geq 0, \qquad (2)$$

де σ – параметр розподілу, що визначає його числові характеристики.

Враховуючи відомий зв'язок періоду слідування імпульсів T з частотним спектром цієї послідовності при формуванні ШІМ сигналу можна стверджувати, що розподіл випадкових інтервалів слідування імпульсів визначається щільністю розподілу оберненої до частоти функції.

Визначимо аналітичний вираз щільності ймовірності $W(T)$ інтервалів слідування імпульсів. Розподіл випадкової величини $f = \frac{1}{T}$ описується законом Релея (2).

Для того, щоб знайти $W(T)$ скористаємось відомим співвідношенням [5]

$$W(T) = G(f)\left|\frac{df}{dT}\right|, \qquad (3)$$

де $\frac{df}{dT}$ - похідна оберненої функції.

Підставляючи в співвідношення (3) щільність розподілу (2) і враховуючи залежність $T = \frac{1}{f}$, отримаємо вираз для щільності розподілу тривалості імпульсів при ШІМ.

$$W(T) = \frac{1}{\sigma^2 T^3} exp\left(-\frac{1}{2\sigma^2 T^2}\right), T \geq 0. \quad (4)$$

Крива розподілу (4) для параметра σ=1 представлена на рис. 2

В даній роботі для формування програмними засобами випадкового імпульсного процесу

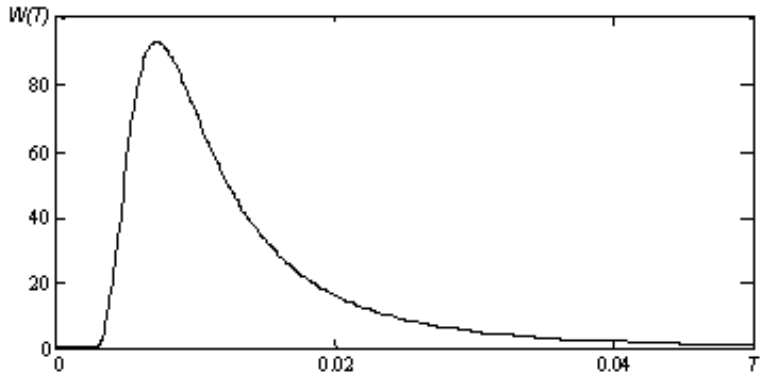

Рис. 2. Щільність розподілу випадкових інтервалів слідування імпульсів

із заданими характеристиками в якості первинного джерела випадкових величин використовувався датчик, який реалізує алгоритм «Mersenne Twister» MT19937 [6, 7]. До його основних переваг слід віднести великий період повторення $T_п = 2^{19937} - 1$, низьку кореляцію між сусідніми значеннями, рівномірність розподілу та високі швидкісні характеристики. Крім того алгоритм MT19937 відповідає більшості критеріїв випадковості.

Для моделювання випадкової величини, розподіленої за законом Релея, скористаємось його інтегральною формою

$$F(f) = 1 - \exp\left(-\frac{f^2}{2\sigma^2}\right), \ f \geq 0,$$

яка приводить до нелінійного перетворення виду [5]

$$f = \sigma\sqrt{-2\ln x}, \quad \textbf{(5)}$$

де σ - параметр розподілу Релея, x - випадкова величина, розподілена за рівномірним законом в інтервалі (0;1].

Використовуючи отримані в результаті моделювання значення f_i можна сформувати випадкові інтервали $T_i = \frac{1}{f_i}$ послідовності імпульсів. Шпаруватість імпульсів в кожному «періоді» візьмемо рівною 2. Це забезпечить стабільне середнє значення формованого процесу при зміні середньої частоти слідування імпульсів.

Структурна схема програмно-апаратного комплексу, в основу роботи якого покладено описаний вище метод, представлена на рис.3.

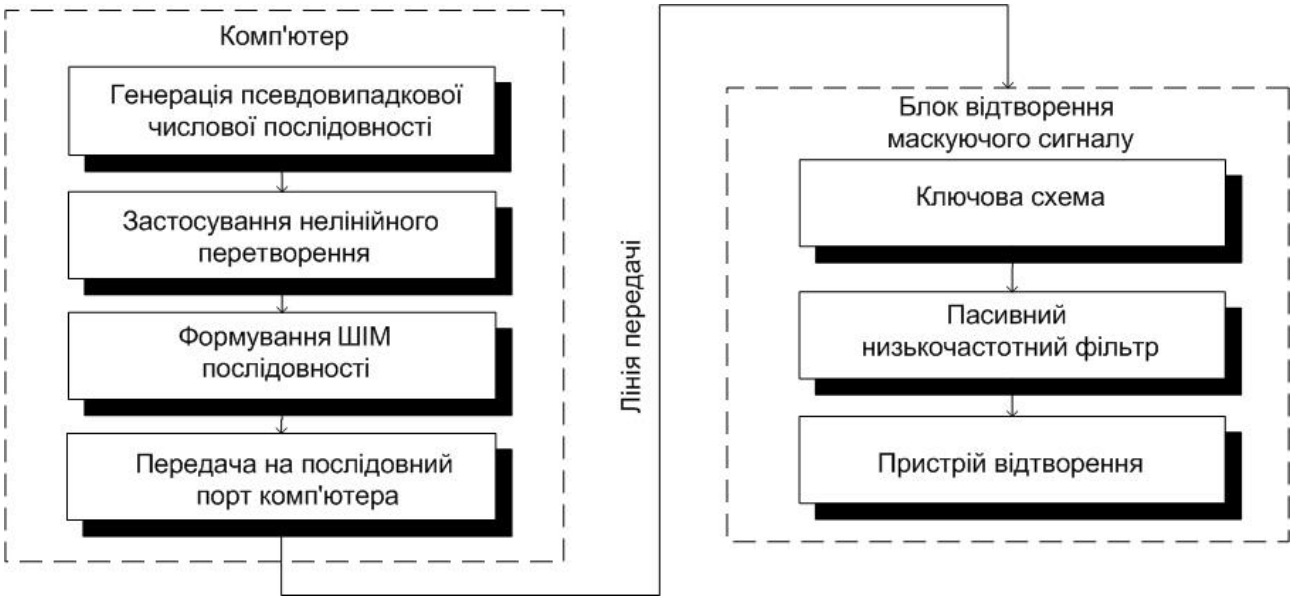

Рис. 3. Структурна схема програмно-апаратного комплексу захисту акустичної інформації

В даному випадку комп’ютер, на якому встановлене необхідне програмне забезпечення, виконує роль формувача випадкової імпульсної послідовності. Ця послідовність через один з послідовних портів комп’ютера передається в лінію передачі. Лінія передачі може бути представлена звичайною двопровідною лінією, до якої не висуваються особливих вимог щодо забезпечення якості переданого сигналу. Така лінія протягується від комп’ютера – формувача випадкової імпульсної послідовності до місця відтворення маскуючого сигналу.

Сукупність підсилювача, фільтра і пристрою відтворення представляють собою блок відтворення маскуючого сигналу.

Ключова схема, керована формованими комп’ютером імпульсами, в даному випадку виконує роль підсилювача. При чому рівень, до якого необхідно забезпечити підсилення, розраховується в кожному випадку окремо для забезпечення ефективного маскування небезпечного сигналу.

Далі підсилений сигнал поступає на низькочастотний фільтр, який необхідний для обмеження смуги маскуючого сигналу. В найпростішому випадку він може бути представлений звичайним низькочастотним пасивним фільтром.

Роль пристроїв відтворення маскуючого сигналу можуть виконувати малогабаритні акустичні колонки або п’єзовібратори, які встановлюються в місцях найбільш імовірного розміщення засобів акустичної розвідки.

В залежності від розмірів виділеного приміщення можливе застосування декількох блоків відтворення маскуючого сигналу для захисту інформації від витоку акустичним та віброакустичним каналами, при використанні лише одного комп’ютера – формувача випадкової імпульсної послідовності. На відміну від інших генераторів шуму один такий програмно-апаратний комплекс, може використовуватись для захисту декількох виділених приміщень. При захисті одним і тим же генератором шуму декількох приміщень зростає загроза застосування зловмисником багатоканальної компенсації маскуючого сигналу. В запропонованому апаратно-програмному комплексі ця проблема вирішується можливістю одночасного виконання декількох процесів формування маскуючих сигналів і передачею їх на різні послідовні порти комп’ютера.

В процесі експериментального дослідження запропонованого методу і відповідного йому алгоритму, було обрано значення параметру розподілу Релея таким, щоб забезпечити перекриття діапазону частот, які впливають на розбірливість мови.

Дослідження спектральних та статистичних характеристик маскуючого сигналу відбувалось в середовищі MATLAB R2009a, із застосуванням вбудованих методів та функцій.

На вхід фільтру з підсилювача подається випадкова послідовність імпульсних сигналів. Фрагмент такої послідовності наведений на рис.4.

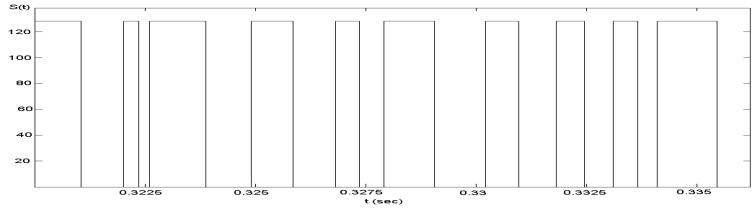

Рис. 4. Фрагмент осцилограми випадкової послідовності імпульсів

В результаті проходження випадкової імпульсної послідовності через пасивний низькочастотний фільтр із заданими параметрами на його виході отримуємо маскуючий шумовий сигнал з необхідними характеристиками. Фрагмент такого сигналу зображено на рис.5.

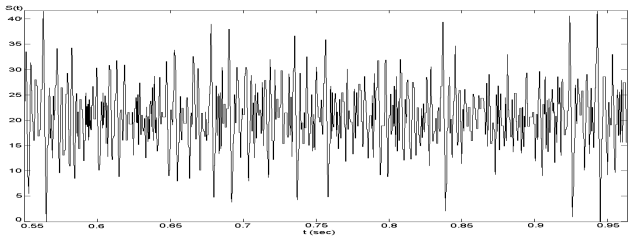

Рис. 5. Фрагмент осцилограми маскуючого сигналу

Оцінка спектральної щільності маскуючого сигналу наведена на рис.6а, а його гістограма - на рис.6б.

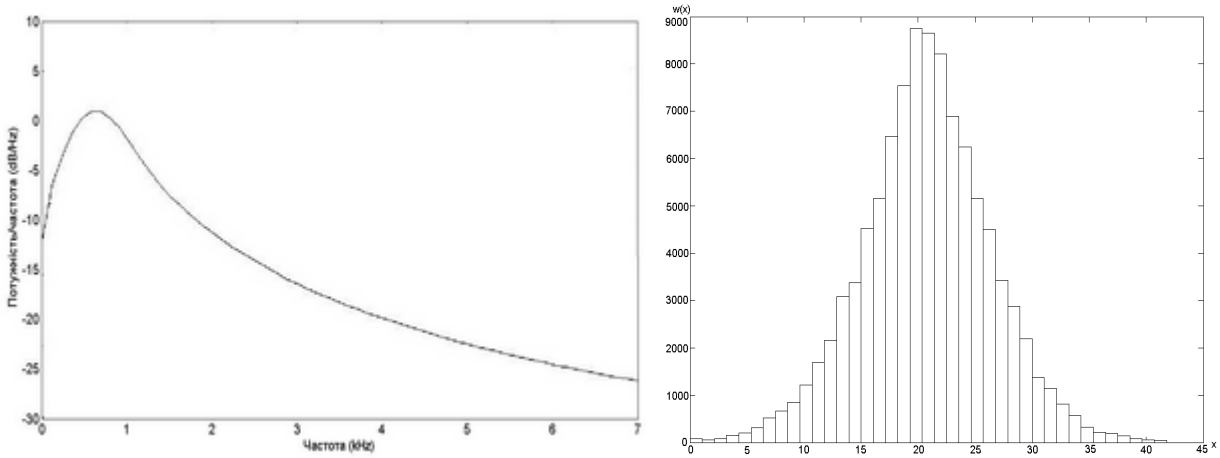

Рис.6. а) оцінка спектральної щільності маскуючого сигналу;
б) гістограма маскуючого сигналу.

Беручи до уваги форму кривої, зображеної на рис. 6а, а також гістограму, зображену на рис. 6б можна зробити висновок про відповідність характеристик маскуючого та мовного сигналів.

Застосування апаратно-програмного комплексу захисту інформації, що реалізує запропонований метод формування маскуючих сигналів можна вважати перспективним, так як він має широкий діапазон регулювання характеристик маскуючих сигналів і дозволяє значно зменшити витрати на захист інформації. Проте він потребує подальших досліджень пов’язаних з аналізом ефективності його робити, а також порівняння з іншими, представленими на ринку, генераторами шумових сигналів.

Список літератури

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - ДСТСЗІ СБ України. К. 1999
2. *В.А. Хорошко, А.А. Чекатов* Методы и средства защиты информации. - Юниор, 2003, - 504с
3. *Вемян Г.В*. Передача речи по сетям электросвязи. – М.: Радио и связь, 1985, -272с
4. *Рабинер Л.Р., Шафер Р.В.* Цифровая обработка речевых сигналов: Пер. с англ./ Под ред. М.В. Назарова. Ю.Н. Прохорова. – М.: Радио и связь, 1981, -495с
5. *Тихонов В.И.* Статистическая радиотехника. - М.: Советское радио, 1966.- 687с
6. *Дональд Кнут.* Искусство программирования — 3-е изд. — М.: «Вильямс», 2007. — Т.2 Получисленные алгоритмы
7. *M. Matsumoto, T. Nishimura,* Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator, ACM Trans. Model. Comput. Simul. 8, 3 (1998)

Рецензент: Петров О.С.
Надійшла 20.09.2010