УДК 681.325

С. І. Мельничук, М. І. Козленко, О. Б. Гарматій
Інститут менеджменту та економіки «Галицька академія»

Ентропійні методи захисту даних в інформаційних каналах комп'ютерних систем

При побудові надійних каналів в закритих розподілених інформаційних системах виникає необхідність формування таких сигналів які б в процесі обміну даними могли отримуватись тільки визначеним абонентом і були практично недоступні для сторонніх приймальних засобів. Для вирішення такої задачі традиційно використовують системи обміну даними з низькою ймовірністю детектування (LPD - low probability of detection) або перехоплення (LPI - low probability of intercept) сигналів [1]. Однією з основних задач при побудові таких систем є мінімізація ймовірності виявлення сеансу обміну даними сторонніми пристроями за використання мінімально необхідної потужності сформованих сигналів [1]. Реалізація згаданих систем значно спрощується за використання широкосмугових шумоподібних сигналів, оскільки зменшення щільності енергії, що характерне для цих сигналів, призводить до більш рівномірного і менш щільного розподілу енергії на заданій ділянці спектру [1]. Крім того, використання в таких розподілених інформаційних системах широкосмугових сигналів має низку інших незаперечних переваг [2].

Одним із перспективних методів формування та оброблення широкосмугових сигналів є метод, при якому формування випадкових сигналів при передаванні відбувається таким чином, що ентропія розподілу ймовірностей станів сигналу-носія поставлена у відповідність до символів інформаційного повідомлення, а оброблення при прийманні полягає у статистичному оцінюванні значення ентропії розподілу станів прийнятого з каналу сигналу, з подальшим порівнянням з порогом і прийняттям рішення щодо дискретного значення прийнятого інформаційного символу [3].

Для реалізації цього методу розроблені структурні схеми пристроїв формування (рис.1) та оброблення (рис. 2) сигналів.

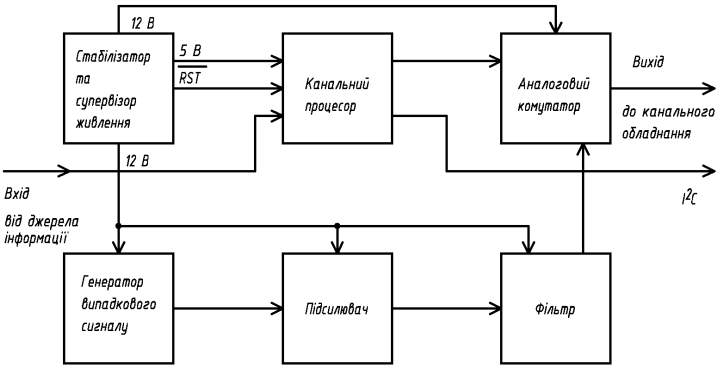

Рис. 1. Структурна схема формувача широкосмугових сигналів зі змінною ентропією

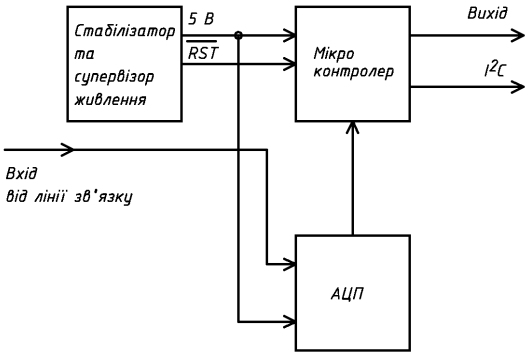

Рис. 2. Структурна схема пристрою оброблення сигналів зі змінною ентропією

Як відомо [4], завадостійкість такого способу (крива 2, рис. 3) є дещо меншою від завадостійкості оптимального кореляційного оброблення (крива 1, рис. 3) сигналів. Проте, цей показник досягається значно меншими апаратними та програмними затратами, оскільки відсутня необхідність використання алгоритмів формування псевдовипадкових послідовностей та відсутня необхідність зберігання еталонів форм сигналів.

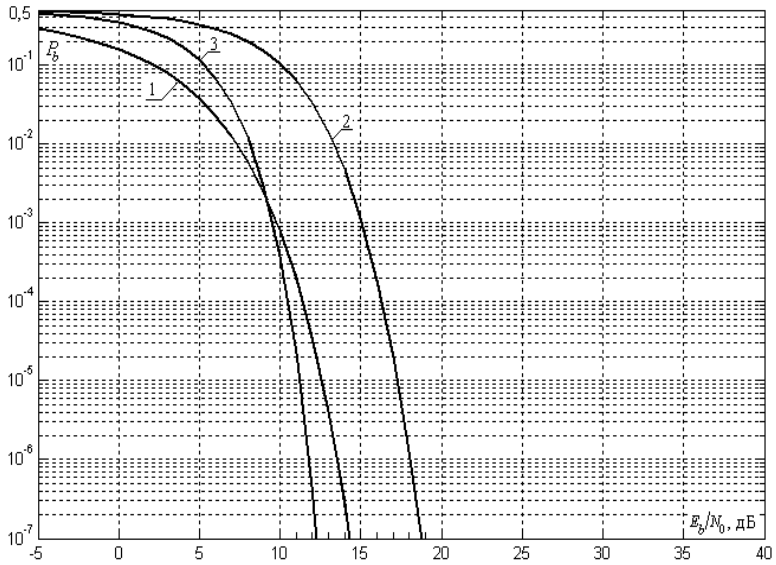

Рис. 3. Завадостійкість методу

Для визначення ефективності запропонованого способу проведено порівняння часової складності алгоритмічного забезпечення запропонованого методу з відповідним забезпеченням кореляційного оброблення, яке проведено на однакових апаратних ресурсах - мікроконтролер ATmega8-16PU з тактовою частотою 16 МГц.

В процесі проведення досліджень встановлено, що за однаковий інтервал часу програмне забезпечення оброблення, що реалізоване на основі запропонованого способу дозволяє опрацьовувати у ≈ 8,1 разів більшу кількість відліків сигналу, ніж програмне забезпечення кореляційного оброблення. Отже вивільняється додатковий обчислювальний ресурс, який можна використати для покращення завадостійкості шляхом використання сигналів з більшою базою. Тобто, при однакових обчислювальних затратах розроблене, на основі запропонованого методу, програмне забезпечення дозволяє обробляти сигнали з більшою у 8,1 разів базою, у порівнянні з традиційними кореляційними методами, що, відповідно, покращує завадостійкість (крива 3, рис. 3). Як можна побачити, максимальне покращення завадостійкості складає величину близько 5 дБ, а при зафіксованій на рівні 10^{-6} ймовірності помилок - не менше 2 дБ.

Таким чином, використання сигналів зі змінною ентропією не тільки дозволяє зменшити ймовірність перехоплення таких сигналів, а й підвищує завадостійкість обміну даними.

Список джерел.

1. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. : Пер. с англ. - М. : Издательский дом “Вильямс”, 2003. – 1004 с. : ил. - Парал. тит. англ.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

3. Пат. № 81017 Україна, МПК(2006) H04B 1/69. Спосіб передавання та приймання інформації / Мельничук С. І., Козленко М. І. (Україна). – заявка № а 2005 08893; Заявлено 19.09.2005; Опубл. 26.11.2007, Бюл. № 19.

4. Козленко М. І., Мельничук С. І. Дослідження завадостійкості способу передавання та приймання інформації на основі широкосмугових сигналів зі змінною ентропією для дискретних повідомлень // Електроніка та зв’язок. - 2007. - № 2(37). - С. 82 - 92.

Ключові слова: формування, обробка, широкосмуговий сигнал, ентропія.