О.В. Андреєв, к.т.н., доц.
К.В. Каленіков, студ., IV курс, гр. РТ-17, ФІКТ
Житомирський державний технологічний університет

КОМБІНОВАНИЙ МЕТОД АМПЛІТУДНО-ЧАСТОТНОГО СКРЕМБЛЮВАННЯ АНАЛОГОВИХ СИСТЕМ ЗВ'ЯЗКУ

На сьогодні проблема захисту інформації дуже актуальна з точки зору бажання обмежити можливості доступу сторонніх людей до важливих даних. Як правило, більшості користувачів не потрібно гарантований захист інформації, досить забезпечити нерозбірливість переданої інформації при прослуховуванні звичайним приймачем.

Надійний захист інформації може бути забезпечений в системах цифрового радіозв'язку, де можна застосувати методи криптографії. Криптографічні алгоритми набули широкого поширення у цифрових стандартах стільникового зв'язку, забезпечуючи досить високу ступінь захисту інформації від несанкціонованого доступу.

У вітчизняних системах радіозв'язку цифрові технології поки що не знайшли такого широкого застосування. У порівнянні з аналоговими радіостанціями вартість цифрових радіозасобів помітно вища. Під аналоговим скремблюванням мається на увазі перетворення вихідного мовного сигналу з метою мінімізації ознак мовного повідомлення, внаслідок якого цей сигнал стає нерозбірливим і невпізнанним. При цьому він займає таку ж смугу частот спектра, як і вихідний сигнал. Необхідною властивістю такого перетворення є можливість зворотного перетворення для відновлення мовного сигналу на приймальній стороні.

Технічні засоби, що забезпечують захист інформації аналоговими методами, називаються скремблерами. Іноді їх називають також мовними маскувачами. Як правило, в сигналі, закритому за допомогою аналогового скремблера, все-таки зберігаються окремі ознаки відкритого мовного повідомлення.

В цілому, аналогові методи захисту інформації забезпечують менший ступінь закриття мовних сигналів в порівнянні з цифровими, однак при практичній реалізації вони, як правило, більш прості, дешеві, а також характеризуються досить високою якістю відновленого мовного сигналу.

Основними технічними характеристиками аналогових скремблеров є рівень закриття інформації, залишкова розбірливість і якість відновлення сигналу.

Найбільш важливою характеристикою скремблера для користувача, який бажає забезпечити захист інформації в своїх каналах зв'язку, є рівень закриття інформації. Слід зазначити, що, якщо для складних цифрових систем передачі мови і даних поняття рівня закриття строго регламентується і визначається криптографічною стійкістю інформації, то для аналогових скремблерів (особливо в системах рухомого радіозв'язку) дане поняття носить умовний характер, так як до цього часу на цей рахунок не вироблено чітких стандартів або правил.

При скремблюванні можливе перетворення мовного сигналу по трьом параметрам: амплітуді, частоті і часу. Однак в системах рухомого радіозв'язку практичне застосування знайшли в основному частотні і часові перетворення сигналу, а також їх комбінації. Можливі перешкоди в радіоканалі істотно ускладнюють точне відновлення амплітуди мовного сигналу, в зв'язку з чим амплітудні перетворення при скремблюванні практично не застосовують на практиці.

При частотних перетвореннях сигналу в засобах рухомого радіозв'язку найчастіше використовуються наступні види скремблювання:

- частотна інверсія сигналу (в якій перетворення спектра мовного сигналу еквівалентно повороту частотної смуги сигналу навколо деякої середньої частоти (Fi));
- розбиття смуги частот мовного сигналу на кілька піддіапазонів і частотна інверсія спектра в кожному щодо середньої частоти піддіапазону;
- розбиття смуги частоти мовного сигналу на кілька піддіапазонів і їх частотні перестановки.

При часових перетвореннях проводиться розбиття сигналу на мовні сегменти і їх перестановки в часі. При цьому в основному на практиці, використовуються два основні способи закриття інформації:

- інверсія за часом сегментів мови;
- часові перестановки сегментів мовного сигналу.

Також іноді застосовують комбіновані методи перетворення сигналу, що припускають використання одночасно декількох різних способів скремблювання (як частотних, так і часових), число яких обмежується, як правило, можливостями технічної реалізації аналогових скремблерів. Вони забезпечують значно більший рівень захисту інформації, але в той же час мають дуже істотні недоліки такі як: значне ускладнення системи в цілому, дуже часто потребують синхронізації, також мають значно гіршу якість відтвореного сигналу.

Проаналізувавши існуючі методи аналогового скремблювання, їх переваги та недоліки, ознайомившись з характеристиками та параметрами існуючих систем захисту інформації, що нині можна знайти у продажу, було вирішено створити і дослідити відмінну від існуючих систему, яка змогла б поєднати в собі комбінований метод амплітудно-частотного скремблювання, вона дозволить досягти більшого ступеню захищеності інформації, яка буде передаватися по каналу зв'язку, не потребуватиме синхронізації та повинна забезпечити належний рівень якості розбірливості відтвореного мовного повідомлення.

Реалізація даної системи буде поділятися на дві основні частини, одна буде реалізовувати закриття повідомлення (скремблювання) в передавальній частині, а інша відповідатиме за відтворення початкового вигляду мовного повідомлення (дескремблювання) вже на приймальній частині.

Згідно назви методу стає очевидним, що два основних параметри, за якими буде відбуватися закриття

повідомлення, стануть частота та амплітуда. Комбіноване скремблювання буде здійснюватися почергово, спочатку за частотою, а потім за амплітудою, в свою чергу дескремблер, для правильного відновлення повідомлення, повинен буде здійснити обернений до попереднього процес зміни ключових параметрів, спочатку відновиться початковий стан амплітудни повідомлення, а потім здійснить відтворення частотного спектру сигналу.

Частина пристрою, що буде здійснювати частотне перетворення, шляхом частотної інверсії, реалізуються на базі мікросхеми FX118, яка виконує функцію частотного інвертора спектру сигналу. Дана реалізація дозволить здійснити частотне перетворення спектру в скремблері та дескремблері з потрібним рівнем захищеності і високою якістю відновленого сигналу. Крім того використання мікросхеми FX118DW дозволить реалізувати дуплексний режим роботи, що доволі рідко можна зустріти в системах, які здійснюють частотні перетворення сигналу. Якщо більш детально, то в передавальній частині частотний спектр сигналу фактично дзеркально обернеться навколо несучої, а в приймальній, при проходженні через таку ж мікросхему, частотний спектр повернеться до початкового положення.

Для реалізації амплітудної частини скремблювання пропонується, аналоговий сигнал спочатку за допомогою аналогово-цифрового перетворювача перетворити в цифровий, далі в цифровому вигляді буде переданий на мікроконтролер, в якому буде здійснена зміна амплітуди за певним псевдовипадковим законом (ключем), після чого він буде переданий на цифро-аналоговий перетворювач, що і завершить процес скремблювання. Дескремблююча частина повинна буде здійснити обернені дії, тобто прийнятий сигнал потрапить на аналогово-цифровий перетворювач, з нього на мікроконтролер, який за відомим законом відтворить початковій стан повідомлення, потім на цифро-аналоговий перетворювач, який завершить процес відтворення початкового вигляду мовного повідомлення,

Також в роботі проведено дослідження зміни захищеності і якості відновленого повідомлення, залежно від зміни розрядності та різних варіантів псевдовипадкових законів, під час виконання амплітудного скремблювання.

Окремо хотілось би відмітити те, що згідно запропонованого варіанту реалізації, система не потребуватиме синхронізації тому, що дескремблювання інформації буде здійснюватися згідно заздалегідь відомого значення ключа.

Загалом в роботі проведено дослідження методу комбінованого амплітудно-частотного скремблювання, наведена структурна схема скремблеру і результати моделювання роботи такої системи.