

Онищенко І. В., ст. гр. ЕЛ-16-16д
Кісельов Є.М., доцент, кандидат технічних наук

ПОБУДОВА СКРЕМБЛЕРУ ГОЛОСОВИХ ПОВІДОМЛЕНЬ

Інженерний інститут Запорізького національного університету, кафедра ЕС

У мовних системах зв'язку відомо два основні методи приховування сигналів, що розрізняються за способом передачі по каналах зв'язку: аналогове скремблювання і дискретизація повідомлень з подальшим шифруванням [1].

Для аналогових скремблерів характерно присутність при передачі в каналі зв'язку фрагментів вихідного відкритого мовного повідомлення, перетвореного в частотній і (або) часовій області. Аналогові скремблери поділяються на [2]: мовні скремблери найпростіших типів на базі часових або частотних перестановок мовного сигналу; комбіновані мовні скремблери на основі частотно-часових перестановок відрізків мовлення, представлених дискретними відліками, із застосуванням цифрової обробки сигналів.

Для побудови скремблеру мовних повідомлень було обрано аналоговий метод шифрування, так як це спрощує реалізацію системи, забезпечує комерційну якість дешифрування інформації і гарантує досить високу стійкість приховування вмісту.

За принципом дії розрізняють аналогові скремблери з перетвореннями у частотній області, з перетвореннями у часовій області і комбіновані [3]. Створення скремблеру на основі частотних перетворень передбачає інвертування частотного спектру повідомлень. Перевагою цього є відсутність окремих каналів синхронізації передавача і приймача, або застосування власно синхронізованих сигналів.

Таким чином створено структуру аналогового скремблеру, що містить аналоговий комутатор, вхідний смуговий фільтр, балансний модулятор, суматор балансного модулятора з фільтром низьких частот, тактовий генератор і дільник – формувач частоти несучого сигналу. При цьому частотно – інвертований сигнал виділяється з нижньої бічної смуги спектру балансного перетворювача звукового сигналу з надзвукової несучої. Одночасно запропонована схема побудови забезпечує як скремблювання, так і дескремблювання повідомлень, за допомогою послідовного виконання двох циклів інверсії. Також система характеризується відсутністю синхронізації кодеру і декодеру.

Досить невисока вартість скремблера дозволяє створити «мережу» серед постійних абонентів або всередині корпоративного керівництва для ведення повністю «закритих» переговорів в межах цієї мережі.

Література

1) Кісельов Є.М. Дослідження кодерів цифрових даних на основі скремблерів / Є.М. Кісельов, О.І. Нагасць // Елементи, прилади та системи електронної техніки (ЕПСЕТ-18). Elements, devices and systems of electronic technique (EDSET-2018). Матеріали першої міжнародної науково-практичної конференції. / Запорізька державна інженерна академія. – Запоріжжя: ЗДІА, 2018 – С. 88 – 89

2) Кісельов Є.М. Використання моделювання поточкових шифрів у лабораторному практикумі з дисципліни «Засоби захисту інформації у мережах ЕОМ» / Є.М. Кісельов // Збірник доповідей учасників 7 Всеукраїнської н.-метод. конф. «Кредитно-модульна система підготовки фахівців». – Запоріжжя, 2007. – С. 262 - 263

3) Методы и средства сокрытия данных путем скремблирования — Национальная библиотека им. Н. Э. Баумана : веб-сайт. URL: <https://ru.bmstu.wiki/%D0%9C%D0%B5%D1%82%D0%B4%D1%> (дата звернення: 26.10.2019)