УДК 621.3

Ю.Л. Пархуць, В.Б. Дудикевич

Національний університет «Львівська політехніка», Львів

ТЕХНОЛОГІЯ КОДОВОГО РОЗДІЛЕННЯ КАНАЛІВ ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЇ АБОНЕНТА СТІЛЬНИКОВОЇ МЕРЕЖІ

У зв'язку із досить швидким розвитком стільникових мереж стандарту CDMA і одночасним вдосконаленням технологій несанкціонованого доступу до закритої інформації все більш актуальним стає питання забезпечення конфіденційності даних абонента. Розглядається принцип функціонування мобільних мереж, які побудовані на платформі CDMA, основна увага сконцентрована на технології множинного доступу з кодовим розділенням каналів, що дозволяє багатьом абонентам використовувати один пул радіоканалів і не пересікатися в розмовах. Наводиться детальний огляд процесу модуляції з використанням широкосмугових сигналів шляхом перемноження корисних бітів інформативного сигналу на псевдовипадкову послідовність коротких імпульсів, що дає можливість отримати сигнал, який займає значно ширший діапазон частот, ніж сигнал в інших стандартах мобільного зв'язку, при цьому зі значно нижчою інтенсивністю.

З метою визначення оптимального способу передачі конфіденційної інформації проводиться ґрунтовний аналіз основних методів розширення спектру корисного сигналу, а саме: методу прямого розширення спектру частот (DSSS-CDMA), багатоканального розширення спектру частот (MC-CDMA) і стрибкоподібної зміни частоти несучої (FHSS-CDMA). При прямому розширенні спектру застосовується математичний апарат псевдовипадкових послідовностей та двійкова фазова маніпуляція з фазовим зсувом на 180 градусів або квадратурно-фазова модуляція з одночасною передачею пари біт. Багатоканальне розширення застосовує кодові послідовності розділення абонентів, сформовані за допомогою ортогональних кодів Уолша. Особливість методики стрибкоподібної зміни частоти несучої полягає у розподілі всієї смуги частот на велику кількість каналів і постійного перелаштування частоти синтезатора з одного каналу на інший за псевдовипадковим законом. Результатом аналізу є порівняльна характеристика розглянутих методів акцентована на відмінностях застосовуваних механізмів перетворення сигналу та перевагах в ефективності захисту даних клієнта.

Проводиться оцінка технології множинного доступу з кодовим розділенням каналів, як засобу забезпечення конфіденційності інформації абонента на рівні радіо інтерфейсу. Наводиться принципи застосування процедур ідентифікації та аутентифікації користувачів із використанням потужних криптологічних механізмів, характерною особливістю яких є режим так званого «приватного зв'язку», що забезпечується за допомогою секретної маски у вигляді достатньо довгого ключа. Для підвищення рівня безпеки додатково можуть використовуватися скремблери у вигляді мініатюрних приставок до телефону або окремі криптосмартфони з вбудованим процесором для шифрування інформації. Пропонується подальший напрямок розробки клієнтоорієнтованих засобів захисту розвивати в рамках створення програмних аплікацій, що реалізують один із стійких криптографічних алгоритмів шифрування абонентських даних, що дозволить піднести на новий щабель рівень інформаційної безпеки в мережах мобільного зв'язку.