УДК № 621.317.73

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ СТАНДАРТУ CDMA.

Корнилюк М.І.
Науковий керівник – доц. , к.т.н Барась С.Т.

Настільки бурхливий розвиток і величезна популярність галузі особливо гостро поставили перед розробниками стандартів стільникового зв'язку і устаткування питання надійної аутентифікації користувачів і безпеки передачі інформації.

Протоколи, що забезпечують безпеку передачі інформації в CDMA-IS-41 мережах, є одними з кращих в індустрії. Крім того сам CDMA стандарт за своєю побудовою робить перехоплення сигналу і його розшифрування дуже складним і дорогим завданням доступним, фактично, лише державним спецслужбам.

CDMA використовує стандартизований алгоритм шифрування CAVE (Cellular Authentification and Voice Encryption) для генерації 128 бітного підключа SSD (Shared Secret Data).

SSD складається з двох частин: SSD_A, використовуваної для створення аутентифікаційного цифрового підпису, і SSD_B, використовуваної при генерації ключів для шифрування голосових даних і службових повідомлень.

Як було вже сказано, для аутентифікації абонента в CDMA мережі використовується допоміжний ключ SSD_A генерований CAVE алгоритмом з A-key, ESN і RANDSSD.

Секретний ключ A-key є перепрограмований, у разі його зміни інформація на мобільному телефоні і в HLR/AC повинний бути синхронізований.

Private Long Code Mask не шифрується інформацію, вона просто замінює відомі величини, використовувані в кодуванні CDMA сигналу секретними величинами, відомими тільки мобільному телефону та мережі. Таким чином підслуховування розмов без знання Private Long Code Mask є надзвичайно складним завданням.

CDMA мережу підтримує призначення мобільному телефону тимчасового ідентифікатора мобільного абонента TMSI (Temporary Mobile Station Identifier) для його представлення в процесі передачі інформації по ефіру між мобільним телефоном і мережею.