УДК 621.396.2

О.М. Кащук, М.Є. Фриз, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ЗАХИСТ ТА ШИФРУВАННЯ ДАНИХ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ GSM

O.M. Kashchuk, M.Y. Fryz, Ph.D Assoc. Prof.

PROTECTION AND ENCRYPTION DATA IN A MOBILE COMMUNICATION SYSTEM GSM

GSM (від *Groupe SpécialMobile*, пізніше перейменована в Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного сотового зв'язку, з розділенням частотного каналу по принципу TDMA і середнім ступінем безпеки.

Сотові системи зв'язку першого покоління, такі як NMT, TACS і AMPS, мали не великі можливості в плані безпеки, і це призвело до суттєвого рівня шахрайської діяльності, яка шкодить і абонентам і мережевим операторам. Безліч інцидентів великого значення висунуло на перший план чутливість аналогових телефонів до підслуховування ліній радіозв'язку. Система GSM має безліч особливостей у плані безпеки, які розроблені, щоб надати абонентові й мережному оператору більший рівень захисту від шахрайської діяльності. Механізми аутентифікації гарантують, що тільки добросовісним абонентам, які мають добросовісне обладнанням, тобто не вкрадене або нестандартне, буде надано доступ до мережі. Як тільки зв'язок було встановлено, інформація в лінії зв'язку передається в зашифрованій формі, щоб уникнути підслуховування. Найпростіший рівень захисту проти шахрайського використання мобільного телефону - особистий ідентифікаційний номер (PIN-код), призначений для захисту проти шахрайського використання украдених SIM карт. В SIM карті PIN код має вигляд від чотирьох-до восьми-значного числа. Користувач може мати можливість відключення цього рівня захисту. SIM-картка також може зберігати другий чотирьох-, восьми-розрядний десятковий код, відомих як PIN2, щоб захистити певні можливості, які є доступними для абонента. Як тільки PIN-код, і якщо потрібно - PIN2, введені правильно, об'єкт технічної експлуатації (main tenance entity) буде мати доступ до даних, збереженим в SIM карті.

Як тільки справжність абонента була перевірена, таким чином захищаючи і абонента і мережевого оператора від впливу шахрайського доступу, користувач повинен бути захищений від підслуховування. Це досягається шляхом шифрування даних, переданих по радіо-інтерфейсу, з використанням другого ключа Kc і секретного алгоритму A5. Kc генерується в ході перевірки автентичності, використовуючи Ki, RAND і секретний алгоритм A8, який також зберігається в SIM карті. Подібно до алгоритму A3, A8 не унікальний, і він може також бути обраний оператором. Ключі Kc для кожного користувача обчислюються в AuC домашньої мережі і передається в VLR в складі набору триплетів, де кожному триплети і, відповідно - ключу Kc, присвоюється номер ключа - CKSN. У деяких реалізаціях A3 і алгоритми A8 об'єднані в єдиний алгоритм A38, який використовує RAND і Ki, щоб згенерувати Kc і SRES. На відміну від A3 і A8, які, можливо, різні для кожного індивідуального оператора, A5 буде вибирається зі списку з 7 можливих варіантів.

Література

1. Берлин А.Н. «Курс Сотовые системы связи Лекция №3 Многостанционный доступ с кодовым разделением и сети GSM» -: Видавництво Вильямс 2011 р., 376 с., ISBN n/a