УДК 007.681

Пархоменко І. І., Кривий Ю. О., Скробач А.Ю.

МЕХАНІЗМИ БЕЗПЕКИ В СИСТЕМІ БЕЗДРОТОВОГО ЗВ'ЯЗКУ З КОДОВИМ РОЗДІЛЕННЯМ КАНАЛІВ

В статті розглянуті принципи функціонування механізмів захисту інформації в мережах мобільного зв'язку, наведена оцінка їх ефективності. Детально розглянуто та проаналізовано архітектуру безпеки стандарту бездротовових мереж cdma2000. Наведено механізми забезпечення аутентифікації, цілісності та конфіденційності даних.

Ключові слова**:** cdma2000, шифрування, мобільний зв'язок, 3G, бездротові мережі.

*Вступ.*Застосування технологій на основі CDMA (Code Division Multiple Access, Множинний доступ із кодовим розподілом каналів) дає нові можливості користувачам послуг мобільного зв'язку якщо порівнювати з іншими технологіями. Переваги використання технології CDMA - висока швидкість передачі даних(для CDMA2000 до 3,1 Мбіт/с), набагато менша потужність випромінювання мобільних терміналів. Принципи, покладені в основу технології, забезпечують їй ще одну важливу перевагу. Стійкість до природних і штучним перешкод, спробам несанкціонованого доступу та іншим формам втручання є істотною особливістю CDMA.

Аналіз останніх досліджень та постановка проблеми. Питання безпеки стандарту CDMA розглянуті в джерелах [1, 2], причому в дослідженнях не розглядаються аспекти безпеки в мобільних мережах стандарту CDMA2000. *Актуальність* дослідження безпеки стандарту CDMA2000 невпинно росте, з постійним збільшенням користувачів цієї технології. *Метою* даної роботи є детальний огляд реалізації захисту інформації, що реалізований в 3G мережах стандарту CDMA2000.

Основна частина. В стандарті CDMA забезпечується високий ступінь захисту від активних і пасивних завад, шо дозволяє працювати при низьких значеннях відношень сигнал/шум. Розширення спектра сигналів дозволяє протидіяти навмисним штучним завадам. CDMA не є панацеєю від несанкціонованого доступу до даних, проте використання послуг мобільного зв'язку на основі CDMA гарантує появу набагато більших перешкод на шляху зловмисників в порівнянні з GSM. Узагальнена *архітектура безпеки* cdma2000 наведена на рис. 1, де процедури аутентифікації, забезпечення цілісності та шифрування виділені темно-сірим кольором, білим кольором і діагональної штрихуванням. Точковим візерунком позначені елементи UIM (User Interface Module), що відповідають за аутентифікацію. Алгоритми безпеки, які використовуються в cdma2000, показані в табл. 1. У cdma2000 передбачено використання як незнімного, так і знімного модуля ідентичності (removable) R-UIM. У цьому випадку оператор може використовувати власний набір відповідних алгоритмів. Процедура *аутентифікації* в cdma2000 подібна до двох етапної процедури аутентифікації в UMTS[3] з кількома вдосконаленнями. Зокрема, мова йде про необов'язкове доповненння процедури аутентифікації і ключового узгодження функцією f_{11}, генерування ключа K_{au} аутентифікації модуля UIM і функцією UMAC, яка перетворює за допомогою K_{au} тег аутентифікації повідомлення (див. рис. 1). Крім того, при передачі в мережу доступувектора аутентифікації цілісність і конфіденційність останнього забезпечується протоколом IPsec. Отримавши вектор аутентифікації, UIM ініціює виконання функції f_5, яка генерує ключ анонімності, і розшифровує SQN. Отримане значення використовується як вхід функції f_1, яка генерує параметр AUTN аутентифікації мережі. Після порівняння AUTN" і AUTN для обчислення RES, $K_{ш}$, $K_{д}$, і K_{au} виконуються функції f_2, f_3, f_4 і f_{11} відповідно. Потім значення RES передається в мережу для підтвердження дійсності абонента. Значення $K_{ш}$ і $K_{ц}$ передаються від UIM до терміналу, де вони далі використовуються для забезпечення конфіденційності і цілісності даних.

Конфіденційність обміну даними на ділянці від мобільної станції до контролера радіомережі забезпечується застосуванням стандарту шифрування AES [4] на основі симетричного блочного шифру Rijndael [5]. Останній зашифровує блоки даних довжиною 128-біт під управлінням 128-бітового ключа, довжина якого при необхідності може бути

зменшена. При шифруванні формуються блоки ключового потоку (рис. 1), що використовуються для потокового шифрування і розшифрування даних. Для забезпечення *цілісності* переданої інформації в системі використовується код аутентифікації повідомлення (Message Authentification Code - MAC), відповідальний за захист від навмисної модифікації. Довжина коду визначається важливістю повідомлення, але не може бути менше 32 біт. Для захисту повідомлень з найвищим пріоритетом використовується UMAC (universal hashing MAC), обчислення якого вимагає використання не тільки ключа цілісності $К_ц$, а й ключа аутентифікації $К_{au}$. Перевага UMAC в тому, що його обчислення може бути здійснено лише безпосередньо модулем ідентичності абонента UIM (рис. 1). У разі надання домашньої середовищем ключа аутентифікації $К_{au}$ у вигляді складової частини вектора аутентифікації мобільна станція визначає UMAC і поміщає його у відповідний пакет даних. Для хешування та перевірки достовірності використовується алгоритм хешування SHA-1.

Алгоритми (функції) безпеки cdma2000 Таблиця 1

Алгоритм	Призначення
f_0	Функція генерації випадкового числа
f_1	Функція аутентифікації мережі
f_2	Функція аутентифіуації користувача
f_3	Функція генерації ключа шифрування $К_ш$
f_4	Функція генерації ключа цілісності $К_ц$
f_5	Функція генерації ключа анонімності $К_а$
f_{11}	Функція генерації ключа аутентифікації UIM $К_{au}$
UMAC	Алгоритм аутентифікації UIM
ESP_AES	Алгоритм шифрування
EHMAC	Вдосконалений алгоритм забезпечення цілісності HMAC

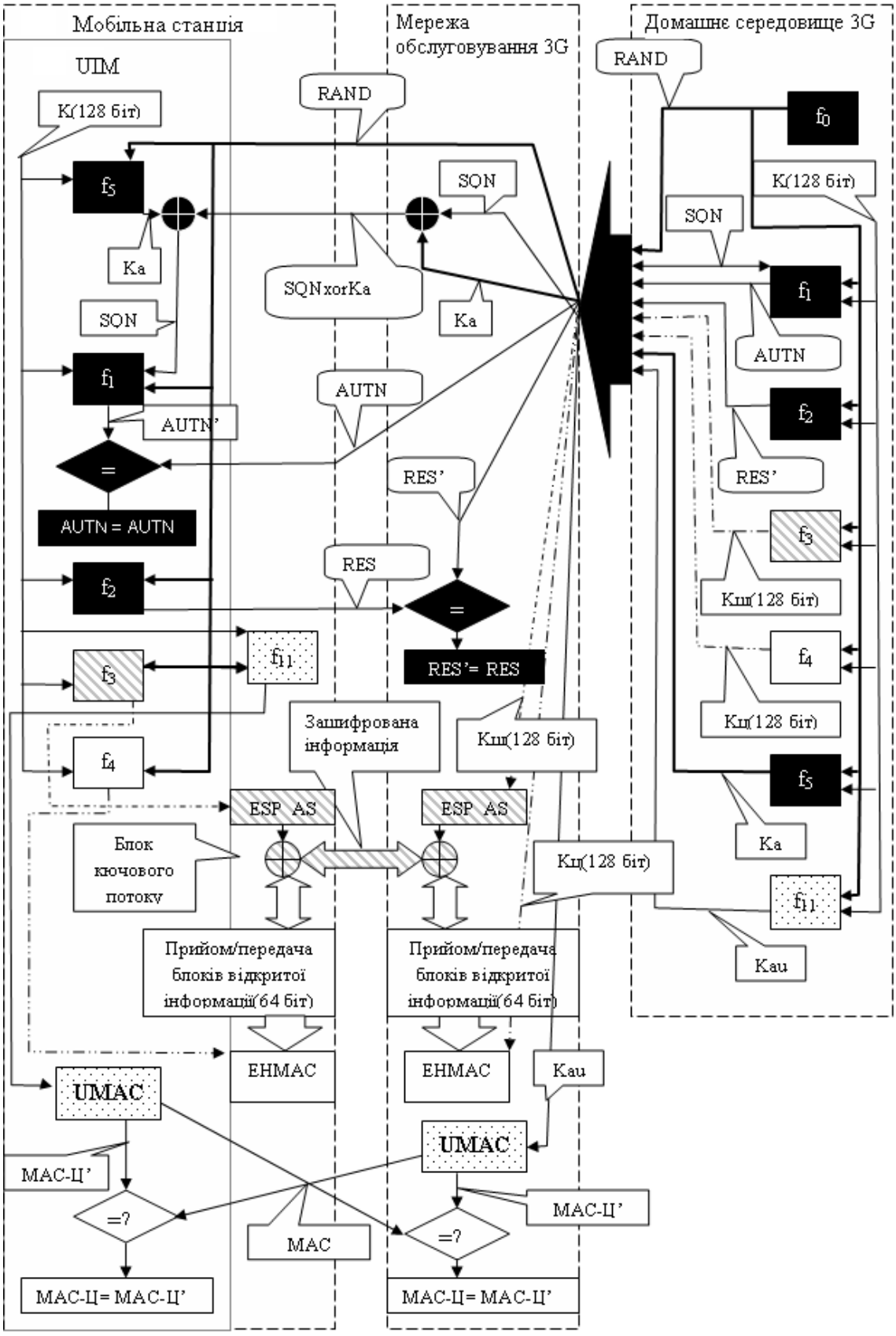

Рис.1. Узагальнена система безпеки cdma2000

Висновки. В системі сотового зв'язку cdma2000 реалізована достатньо потужна та продумана архітектура безпеки інформації, відкрита для подальшого вдосконалення. Перша перевага заключається в можливості використання як вбудованого так і змінного модуля ідентичності абонента - RUIM. Звідси випливає, що оператор може використовувати власний

набір криптографічних алгоритмів. Також використання RUIM виключає можливість використання втраченого терміналу, зменшує ймовірність викрадення і копроментування, забезпечує високий рівень конфіденційності інформації, що зберігається в модулі. Алгоритми безпеки cdma2000 повністю стандартизовані, та відповідають сучасним вимогам, адже використовується блочний шифр AES з розміром ключа 128 біт та протокол IPsec.

ЛІТЕРАТУРА

1. Шахнович И.В. Современные технологии беспроводной связи. — М.:Техносфера, 2006. – с.122-127.
2. Пархуць Ю.Л. Криптографічні механізми захисту інформації в мобільному зв'язку : зб. наук. праць / наук. ред. Кузнєцов Г.В.. — Київ : «Видавництво»., 2011. — 89 с.
3. Кривий Ю. О. Проблеми захисту інформації в мережах мобільного зв'язку третього покоління / Ю. О. Кривий, І. І Пархоменко. // Наукоємні технології. – 2009. – № 3 – С. 77–80.
4. J. Daemon and V. Rijmen, *AES Proposal: Rijndael*, AES Algorithm Submission, September 3, 1999.
5. Гепко И.А., Олейник В.Ф., Чайка Ю.Д., Бондаренко А.В. Современные беспроводные сети: состояние и перспективы развития. К: «ЕКМО», 2009. 672 с.
6. 3GPP2 S.R0032, Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP), version 1, Dec 2000.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Юдін О.К.