УДК 621.34

С.Г. Семенов[1], Р.В. Корольов[1], І.А. Ставицький[2]

[1] *Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*

АНАЛІЗ ТА ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ СТАНДАРТУ GSM

Проведений аналіз сучасних стандартів стільникового зв'язку та порівняльне дослідження засобів захисту інформації в телекомунікаційних мережах стандарту GSM. Виявлені основні складові сучасної системи захисту мережі зв'язку. Проілюстровані особливості процедур автентифікації й ідентифікації, а також забезпечення конфіденційності даних у мережах зв'язку стандарту GSM. Зроблено висновок про необхідність подальшого вдосконалення системи захисту інформації в телекомунікаційних мережах стандарту GSM.

Ключові слова: *телекомунікаційні системи і мережі, цифрові лінії зв'язку, стандарт GSM.*

Вступ

Постановка проблеми. Стрімкий розвиток цифрових засобів стільникового зв'язку, розширення спектру послуг та підвищення вимог до якості обслуговування обумовлюють розробку нових підходів щодо розподілення мережних ресурсів, управління та адміністрування в системах

мобільного зв'язку, вдосконалення сучасного мережного та комутаційного обладнання. Дослідження та порівняльний аналіз систем стільникового зв'язку показали, що сучасні абонентські вимоги забезпечуються підвищенням якості звуку, наданням нових послуг (передача даних, доступ до глобальних мереж, передача відеоінформації і т.ін.), поступовим збільшенням швидкості передачі даних (обладнання третього покоління (3G) – здійснюватиме відеозв'язок з абонентом або можливість перегляду мобільного телебачення зі швидкістю його передачі до 3,6 Мбіт/с, четвертого покоління (4G) зі швидкістю передачі даних до 1 Гбіт/с), а також впровадженням нових механізмів та засобів захисту інформації.

Дійсно, на сучасному етапі важко переоцінити важливість забезпечення основних послуг безпеки при веденні переговорів за допомогою засобів стільникового зв'язку в більшості сфер суспільної діяльності.

Аналіз вимог [1 – 3] щодо забезпечення безпеки інформації дозволив виявити основні складові сучасної системи захисту мережі зв'язку:

- коректна тарифікація послуг, що надаються;
- конфіденційність персональних даних;
- конфіденційність потоку навантаження;
- моніторинг дій користувачів і функціонування мережі;
- захист ресурсів мережі;
- управління системою захисту.

Забезпечення коректної тарифікації покликано захистити економічні інтереси дійових осіб і безпосередньо пов'язане з достовірністю ідентифікаторів користувачів і їх абонентського устаткування.

Слід зазначити, що перевірка достовірності об'єктів, що беруть участь в з'єднанні, є головним завданням системи захисту будь-якої мережі зв'язку.

Будь-яка система зв'язку повинна попередити зловмисне використання даних, що стосуються конкретних людей. Конфіденційність особистих даних має ключове значення для відомчих радіомереж правоохоронних органів. Але вона важлива також і для мереж загального користування у зв'язку з дотриманням законодавства з прав людини. Забезпечення конфіденційності персональних даних необхідне і для комерційних відомчих мереж професійного радіозв'язку, оскільки людський чинник є деколи критичним для захисту економічних інтересів відомства або компанії.

Зрозуміло, що конфіденційність персональної інформації досягається шляхом захисту бази даних абонентів і користувачів, а також за допомогою регулярної зміни паролів і позивних.

На підставі аналізу потоку навантаження, нехай навіть зашифрованого, можна одержати інформацію про структуру зв'язків конкретної особи або групи користувачів. Така інформація може представляти істотний комерційний або оперативний інтерес. Засоби забезпечення конфіденційності потоку навантаження потрібні в першу чергу для відомчих мереж служб безпеки. Одним із засобів забезпечення конфіденційності потоку навантаження є формування потоку заповнюючих (порожніх) повідомлень, що передаються по мережі.

Наявність різноманітних функцій і механізмів захисту стільникової мережі приводить до необхідності створення складної системи контролю і управління. Відповідні елементи є життєво важливими для безпеки і життєздатності мережі і тому самі є об'єктами підвищеної захищеності.

Аналіз сучасних стандартів стільникового зв'язку [1 – 4] показав, що в існуючих стандартах стільникового зв'язку (GSM, CDMA, UMTS ті ін.) застосовуються засоби забезпечення послуг безпеки (автентифікація, конфіденційність, цілісність і т.д.). Проте нині "вбудованого" захисту голосового трафіку вже недостатньо – перехопити розмову і передачу даних користувачами можна якщо не за допомогою спеціального обладнання, то за допомогою відомих і поширених електронних систем. Тому дуже важливою і, на жаль, поки що не розв'язаною проблемою є аналіз, розробка і застосування сучасних засобів захисту інформації. Дослідження показали, що найгостріше це питання стоїть у українських операторів мобільного зв'язку стандарту GSM.

Основна частина

Процедури автентифікації й ідентифікації у мережах зв'язку стандарту GSM. Дослідження сучасних засобів автентифікації й ідентифікації показали необхідність цих процедур у зв'язку з численними і різноманітними проявами особливого роду шахрайства – отримання несанкціонованого доступу до послуг стільникового зв'язку. Спочатку в аналогових системах стільникового зв'язку першого покоління процедура автентифікації мала простий вигляд: рухома станція передавала свій унікальний ідентифікатор (електронний серійний номер – Electronic Serial Number, ESN) і якщо такий відшукувався серед зареєстрованих у домашньому регістрі, то процедура автентифікації вважалася успішно виконаною. Така примітивна автентифікація залишала великі можливості для фроду, тому з часом і в аналогових системах, і тим більше в системах стільникового зв'язку другого покоління з використанням додаткових можливостей цифрових методів передачі інформації процедура автентифікації була значно удосконалена.

Ідея процедури автентифікації у цифровій системі стільникового зв'язку полягає у шифруванні деяких паролів-ідентифікаторів з використанням квазівипадкових чисел, які періодично передаються на рухому станцію з центру комутації, та індивідуального для кожної рухомої станції алгоритму шифрування. Таке шифрування з використанням одних і

тих самих початкових даних і алгоритмів проводиться як на рухомій станції, так і в центрі комутації (або в центрі автентифікації), і тому автентифікація вважається такою, що закінчилася успішно, якщо обидва результати збігаються.

У стандарті GSM процедура автентифікації пов'язана з використанням модуля ідентифікації абонента (Subscriber Identity Module – SIM), званого також SIM-картою (SIM-card) або смарт-картою (smart-card). Модуль SIM – це знімний модуль, що встановлюється у відповідне гніздо абонентського апарату.

Модуль SIM містить персональний ідентифікаційний номер абонента (Personal Identification Number – PIN), міжнародний ідентифікатор абонента мобільного зв'язку (International Mobile Subscriber Identity – IMSI), індивідуальний ключ автентифікації абонента Ki, індивідуальний алгоритм автентифікації абонента A3, алгоритм обчислення ключа шифрування A8.

Для автентифікації використовується зашифрований відгук (signed response) S, що є результатом застосування алгоритму A3 до ключа Ki і квазівипадкового числа R, яке рухома станція отримує від центра автентифікації через центр комутації. Алгоритм A8 використовується для знаходження ключа шифрування повідомлень.

Унікальний ідентифікатор IMSI для поточної роботи замінюється тимчасовим ідентифікатором TMSI (Temporary Mobile Subscriber Identity – тимчасовий ідентифікатор абонента мобільного зв'язку), який присвоюється радіотелефону при його першій реєстрації у конкретному регіоні, що визначається ідентифікатором LAI (Location Area Identity – ідентифікатор області місцеположення), і анулюється при виході апарату за межі цього регіону.

Ідентифікатор PIN – це код, відомий тільки абонентові, який має служити захистом від несанкціонованого використання SIM-карти, наприклад при її втраті. Після трьох невдалих спроб набору PIN-кода SIM-карта блокується, а блокування може бути знято або набором додаткового коду – персонального коду розблокування (Personal unblocking key – PUK), або за командою з центру комутації.

Процедуру автентифікації у стандарті GSM схематично показано на рис. 1.

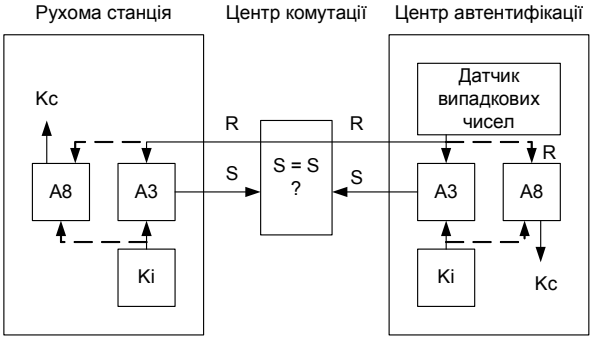

Рис. 1. Структурна схема проведення процедури автентифікації у стандарті GSM

Пунктиром позначені елементи, що не відносяться безпосередньо до процедури автентифікації, але використовуються для знаходження ключа шифрування Кс. Таким чином, апарат функціонуватиме, якщо він не ідентифікований у "чорних" списках і автентифікований.

Процедура забезпечення конфіденційності даних у мережах зв'язку стандарту GSM. Ключ шифрування. Для забезпечення конфіденційності інформації, яка передається по радіоканалу, вводиться наступний механізм захисту. Усі конфіденційні повідомлення повинні передаватися у режимі захисту інформації. Алгоритм формування ключів шифрування (A8) зберігається в модулі SIM. Після прийому квазівипадкового числа *R* рухома станція обчислює відгук *S* і ключ шифрування Кс, використовуючи Ki та алгоритм A8 (рис. 2):

$$Kc=Ki\,[R].$$

Ключ шифрування Кс не передається по радіоканалу. Як рухома станція, так і мережа обчислюють ключ шифрування, який використовується іншими мобільними абонентами. У інтересах забезпечення безпеки обчислення Кс відбувається у SIM-картці.

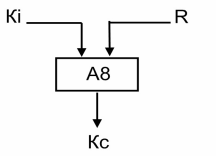

Рис. 2. Процедура обчислення ключа шифрування

Не дивлячись на те, розробники мобільних систем стандарту GSM достатньо велику увагу приділяють розробці і впровадженню засобів захисту інформації; попит на нові, сучасні засоби, що забезпечують основні послуги безпеки, не зменшується. Останнім часом з'явилися багато нових, перспективних напрямів в розробці і впровадженні програмних і апаратних засобів захисту інформації. На рис. 3 наведена класифікація сучасних програмно-апаратних засобів захисту інформації стандарту GSM.

Висновки

Проведений огляд процедур забезпечення безпеки інформації в мережах стільникового зв'язку GSM показав перспективність розвитку у цьому напрямку. Так, в порівнянні із стільниковими системами першого покоління, у яких були невеликі можливості з точки зору безпеки та, як наслідок, значні збитки від шахрайської діяльності, система GSM має багато особливостей в плані забезпечення безпеки, які розроблені для того, щоб надати абонентам і операторам зв'язку більш високий рівень захищеності від загроз. Проте, скоріш за все, із приходом зв'язку третього та четвертого покоління (3G, 4G)

існуючі стандарти забезпечення конфіденційності доведеться модифікувати або розробляти нові, тому

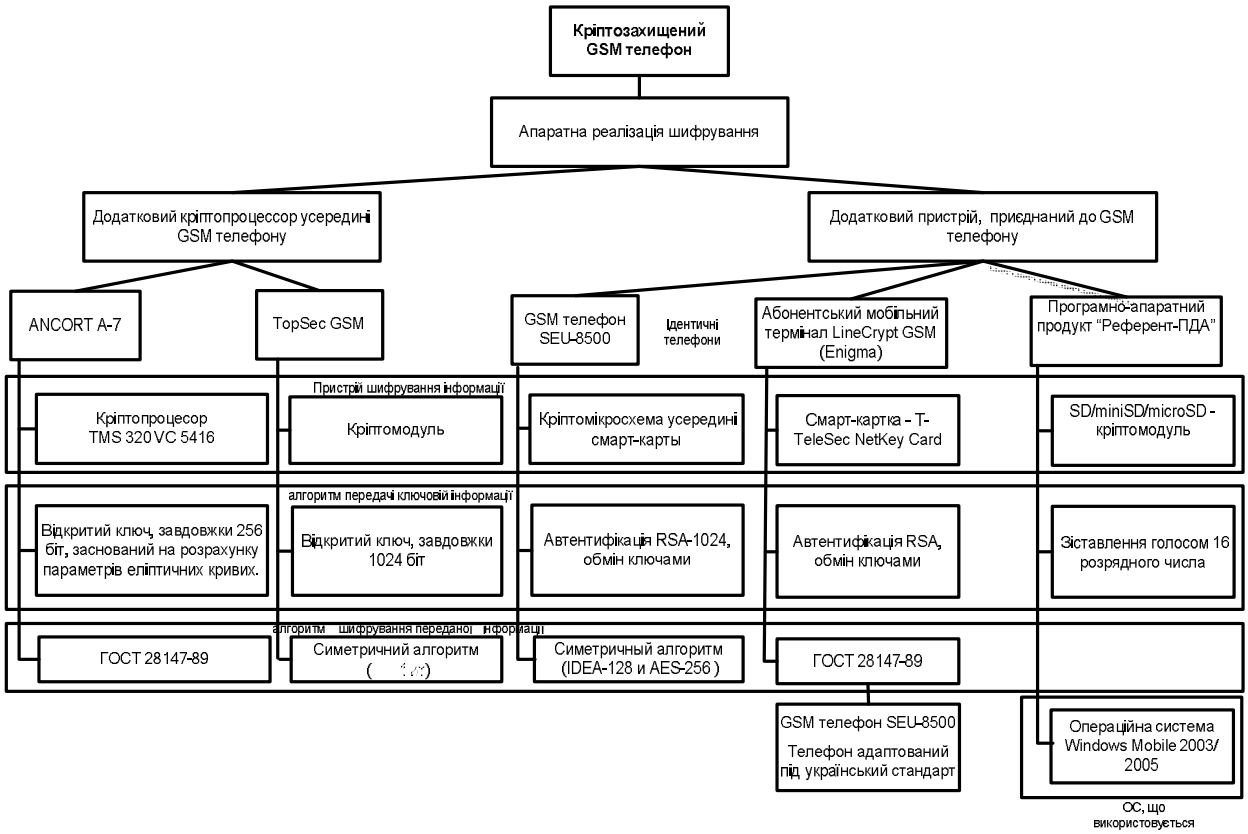

Рис. 3. Класифікація сучасних програмно-апаратних засобів захисту інформації стандарту GSM

що у стандартах 3G, 4G та GSM використовуються принципово різні технології множинного доступу до мережі (множинний доступ із кодовим розподіленням – CDMA і множинний доступ із розподіленням у часі – TDMA відповідно).

Список літератури

1. Величко В.В. Передача данных в сетях мобильной связи третьего поколения / В.В. Величко. – М.: Горячая линия – Телеком, 2005. – 332 с.

2. Жуков С. Хакинг мобильных телефонов / Сергей Жуков. – М.: Бук_пресс, 2006. – 224 с.

3. Громаков А.Ю. Стандарты и системы подвижной радиосвязи / А.Ю. Громаков. – М.: Эко-Трендз, 1998. – 239 с.

4. Афанасьев В.В. Защита информации в сетях сотовой подвижной связи / В.В. Афанасьев, В.Н. Максименко, Н.В. Волков. – М.: Горячая линия – Телеком, 2007. – 360 с.

Надійшла до редколегії 30.03.2010

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський національний технічний університет сільського господарства ім. П. Василенка, Харків.

АНАЛИЗ И СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ СТАНДАРТА GSM

С.Г. Семенов, Р.В. Королев, И.А. Ставицкий

Проведен анализ современных стандартов сотовой связи и сравнительное исследование средств защиты информации в телекоммуникационных сетях стандарта GSM. Обнаружены основные составляющие современной системы защиты сети связи. Проиллюстрированы особенности процедур аутентификации и идентификации, а также обеспечения конфиденциальности данных в сетях связи стандарта GSM. Сделан вывод о необходимости последующего совершенствования системы защиты информации в телекоммуникационных сетях стандарта GSM.

Ключевые слова: *телекоммуникационные системы и сети, цифровые линии связи, стандарт GSM.*

AN ANALYSIS AND COMPARATIVE RESEARCH OF FACILITIES OF DEFENCE OF INFORMATION IS IN NETWORKS OF TELECOMMUNICATIONS OF STANDARD OF GSM

S.G. Semenov, R.V. Korolyov, I.A. Stavitskiy

The analysis of modern standards of cellular connection and comparative research of facilities of defence of information is conducted in the networks of telecommunications of standard of GSM. Found out the basic constituents of the modern system of defence of communication network. The features of procedures of authentification and authentication, and also providing of confidentiality of information, are illustrated in communication of standard of GSM networks. A conclusion is done about the necessity of subsequent perfection of the system of defence of information in the networks of telecommunications of standard of GSM.

Keywords: *systems of telecommunications and networks, digital flow lines, standard of GSM.*