УДК 621.396

А.О. Москаленко[1], О.В. Федін[2]

[1] *Полтавський національний технічний університет імені Юрія Кондратюка, Полтава*
[2] *Академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів*

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІСНУЮЧИХ ТА ПЕРСПЕКТИВНИХ СИСТЕМАХ РУХОМОГО ЗВ'ЯЗКУ

В статті представлені результати порівняльного аналізу механізмів забезпечення інформаційної безпеки стандартів стільникового зв'язку другого та третього поколінь.

Ключові слова: *системи рухомого зв'язку, механізми забезпечення інформаційної безпеки, фрактальні структури.*

Вступ

Постановка задачі та її зв'язок із важливими науковими і практичними завданнями. Враховуючи ріст попиту Збройних Сил (ЗС) України на комунікаційні послуги, коли штатна система зв'язку не в змозі в повному обсязі вирішувати покладені на неї завдання, пошук шляхів вирішення даної проблеми наразі є пріоритетним завданням.

Аналіз науково-технічної політики розвинених країн свідчить, що головна її спрямованість проявляється у все більшій орієнтації на застосування нових інформаційних технологій, під якими розуміють сукупність методів, способів і засобів збирання, накопичення, зберігання, обробки, пошуку та надання інформації.

Обмеженість фінансування урядом Міністерства оборони України не дозволяє здійснити в короткі терміни повне переоснащення ЗС України новими зразками техніки зв'язку. Тому виникає завдання пошуку нових підходів щодо побудови системи зв'язку й автоматизації ЗС України [1].

Шляхи та напрямки розвитку системи зв'язку та автоматизації управління ЗС України доцільно визначати з урахуванням тенденцій розвитку систем військового зв'язку армій країн НАТО, а також тенденцій розвитку державних і комерційних мереж загального користування [1].

Аналіз останніх досліджень та публікацій. Аналіз зарубіжних публікацій про досвід армій країн НАТО щодо концепції використання транспортних можливостей систем стільникового зв'язку для забезпечення повсякденної діяльності збройних сил та їх участі в міжнародних миротворчих операціях, свідчить про доцільність її застосування.

Проте використання даної концепції можливе лише після проведення всебічного аналізу мобільних систем зв'язку. Одною з ключових характеристик сучасних систем, які застосовуються в інтересах оборонних відомств, є рівень забезпечення інформаційної безпеки.

Метою статті є дослідження механізмів забезпечення інформаційної безпеки в існуючих та перспективних системах рухомого зв'язку.

Основна частина

Важливим пріоритетом проектування системи стільникового зв'язку (ССЗ) є конфіденційність передачі інформації. Проте між базовою і мобільною станціями (БС та МС) інформація передається по радіоканалу, що, власне, може зробити доступним третій особі як сам факт передачі, так і її зміст.

Дослідження можливостей використання ССЗ для передачі інформації з обмеженим доступом становить великий практичний інтерес. Пошук відповідних організаційних та технічних рішень в більшості країн знаходиться в компетенції спецслужб. Але обладнання ССЗ, що на сьогодні використовується в Україні, розробляється і випускається за кордоном. Тому великий практичний інтерес становить аналіз потенційних можливостей відомих технологічних платформ мобільного зв'язку з позиції реалізації на їх основі перспективних механізмів безпеки.

Механізми забезпечення безпеки в GSM. Зараз в Україні, та й у всьому світі, найбільш масовими є мережі систем стільникового зв'язку стандарту GSM, розробленого Європейським інститутом стандартизації у сфері телекомунікацій (ETSI) на початку 90-х. У створенні схеми безпеки GSM, що мала надавати захист від несанкціонованого доступу, радіоперехоплення та прослуховування, приймали участь спецслужби країн блоку НАТО. В [2] визначено наступні механізми захисту системних та інформаційних ресурсів:

захист МС від несанкціонованого доступу за допомогою пароля;

ідентифікація МС за допомогою унікального міжнародного номера (IMSI);

аутентифікація абонента при кожному вході у зв'язок;

забезпечення конфіденційності інформації, що передається по радіоканалу, за рахунок шифрування;

секретність місцезнаходження абонента і напрямку його виклику.

Схема безпеки GSM базується на трьох алгоритмах: аутентифікації А3, шифруванні А5 та генеруванні криптоключа А8 (що являє собою односторонню функцію формування сеансового ключа для алгоритму А5 на основі фрагменту послідовності, що генерується А3). Перші два знаходяться в SIM-карті абонента (в ній також міститься IMSI та індивідуальний ключ аутентифікації і-го користувача Кі), а А5 – в спеціальному чипі МС.

Розглянемо наведені вище механізми більш детально. Виключення несанкціонованого доступу до SIM-карти реалізовано шляхом перевірки паролів без передачі в ефір (PIN і PUK-коди, що вводяться абонентом в МС перед її використанням).

Ідентифікація абонента при входженні в мережу здійснюється по IMSI, що передається на БС. Після цього йому присвоюється тимчасовий міжнародний ідентифікаційний номер (TMSI), який передається з БС на МС у зашифрованому вигляді. TMSI діє тільки у межах зони обслуговування абонента.

Процедура аутентифікації реалізується центром комутації мобільної мережі (ЦКММ) з боку БС та SIM-картою абонента з боку МС. При цьому виконуються такі дії (рис. 1):

МС надсилає БС запит про надання системних ресурсів;

ЦКМС генерує випадкове число RAND (128 біт) і відсилає його МС;

використовуючи RAND і ключ Кі, МС визначає відгук SRES (довжиною 32 біти) за допомогою алгоритму А3 і відсилає цей відгук на ЦКМС;

маючи всі дані про кожного абонента мережі, ЦКМС також обчислює SRES. При отриманні відгуку МС ці обидва значення порівнюються. Їх збіг призводить до встановлення з‘єднання, в іншому випадку зв‘язок з МС розривається.

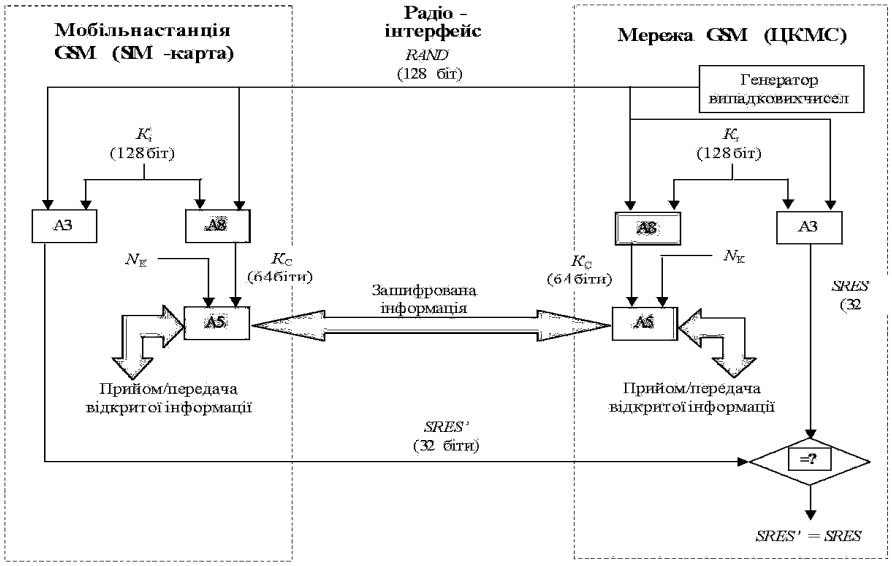

Рис. 1. Узагальнена схема ідентифікації і криптозахисту в мережі GSM

Конфіденційність передачі інформації в радіоканалі забезпечується її шифруванням у відповідності до алгоритму А5. У цьому випадку використовується ключ КС, що обчислюється (але не передається) одночасно з відгуком SRES (рис.1). Довжина КС на виході алгоритму А8 – 64 біти. Для перевірки ключа КС БС разом з RAND надсилає МС числову послідовність, пов‘язану в даний момент з діючим значенням КС. Після його перевірки МС отримує команду перейти в режим шифрування.

За допомогою А5 дані, що передаються, зашифровуються побітно. На вхід системи шифрування надходить номер кадру (NK) довжиною 22 біти і ключ КС (64 біти). Дві шифр-послідовності довжиною 114 біт формуються окремо від кожного кадру: одна для шифрування вихідного пакета даних, інша для розшифровування вхідного пакета. Номер кадру змінюється з кожним новим пакетом, а ключ КС – при кожному новому сеансі зв‘язку. Секретність місцезнаходження і напрямку виклику абонента досягається за рахунок використання TMSI, що передається абоненту в зашифрованому вигляді. При входженні в нову зону обслуговування абонент передає по радіоканалу не всю інформацію про себе, а лише TMSI і номер локальної зони, в якій його отримано. В новій локальній зоні БС дає запит старій БС на номер, присвоєний МС, та всю іншу інформацію про абонента з даними TMSI. Надалі абоненту присвоюється новий TMSI, так що в новій зоні абонент реєструється в мережі під псевдонімом.

Варто додати, що всі ці процедури визначено [2] в загальному вигляді, а їх деталі доступні лише вузькому колу людей із організацій-операторів GSM, що й досі залишається однією з найбільш засекречених комерційних таємниць. Тим не менше (а вірніше кажучи, завдяки цьому), вся історія експлу-

атації GSM супроводжується дискусіями навколо як дійсних, так і можливих випадків її компрометації.

Причин цьому, щонайменше, дві. Перша полягає в стратегії захисту системи, яка пов'язана із зберіганням в таємниці особливостей її реалізації. Як і слід було очікувати, широке розповсюдження МС поступово призвело до витоку інформації, і до середини 90-х стали відомі основні деталі А5. В ньому реалізовано поточний шифр на базі трьох лінійних регістрів зсуву. Довжини регістрів вибрано достатньо короткими – 19, 22 і 23 біти, що в сукупності формує 64-бітний сеансовий ключ шифрування. Теоретично сама по собі вкорочена довжина регістрів робить можливою «лобову» атаку шляхом перебирання вмісту двох перших регістрів (складність подібної процедури ≈ операцій 240). Після цього вміст третього регістра можна відтворити з вихідної шифрпослідовності (загальна складність дорівнює ≈ 245) [3].

Спецслужби, які приймали участь у розробці, одночасно були стурбовані неможливістю в подальшому за необхідності перехоплювати і дешифрувати інформацію, що передається. Прагнучи полегшити для себе це завдання, вони навмисне послабили стійкість шифру в алгоритмі А5, який застосовувався для захисту мовного каналу від прослуховування: в 64-бітному ключі використовуються тільки 54 біти, а 10 просто заміняються нулями. Таким чином, виникли два різновиди алгоритму А5: версія А5/1 з підсиленим шифром для «вибраних» країн і дещо слабша версія А5/2 для всіх інших. Для злому А5/2 прямим перебором достатньо знайти початкове заповнення керівного регістра довжиною 17 біт (складність 216), проаналізувавши два фрейми довжиною по 114 біт (перші два фрейми шифрпослідовності в GSM завжди відомі, оскільки зашифровуються при цьому тільки нулі). Злом такого шифру на персональному комп'ютері займає близько 15 мс [3].

Представник Smartcard Developer Association (SDA) не втримався від наступного коментаря щодо безпеки в GSM: « досвід показує, що розвідслужби, які стоять за всіма криптоалгоритмами GSM …компрометують будь-який і кожен компонент криптосистеми …лише тому, що можуть це зробити, а не тому, що їм це необхідно». Спеціалісти SDA називають наступні, з'ясовані ними, слабкі ланки в захисті GSM:

скомпрометовано ефективну довжину сеансового ключа. Зведення до нулів 10 біт в 64-бітному ключі, який А8 генерує для А5, означає навмисне послаблення системи безпеки приблизно в 1000 раз;

скомпрометовано схеми аутентифікації і генерування секретного ключа. Про слабкі сторони COMP128, які з'ясувались в 1998 р., учасникам проекту GSM MoU офіційно повідомили ще в 1989 р. – задовго до розповсюдження GSM. Проте група експертів з алгоритмів безпеки (SAGE) зберігала це в таємниці, тож деякі західні розвідслужби мають можливість клонувати телефони і вираховувати секретні ключі абонентів безпосередньо під час сеансу з'язку;

скомпрометовано «сильний» алгоритм шифрування А5/1. В шифрі з 64-бітним ключем виявлено ваду, яка призводить до зниження стійкості на 6 порядків (що практично відповідає стійкості еквівалентного шифру з 40-бітним ключем).

Крім того, шифрування в GSM здійснюється в каналі між мобільною і базовою станціями. Теоретично завжди існує можливість підключення безпосередньо до базової станції, після чого будь-яке шифрування взагалі стає відсутнім. При цьому не можна не зазначити, що взаємна аутентифікація між МС і БС відсутня, аутентифікується тільки МС, а точніше її SIM-карта. І нарешті, ще одним фундаментальним недоліком є те, що перешкодостійке кодування в GSM здійснюється до шифрування (рис. 2), що збільшує надмірність повідомлення, яке зашифровується, всупереч рекомендаціям класичної криптології [4].

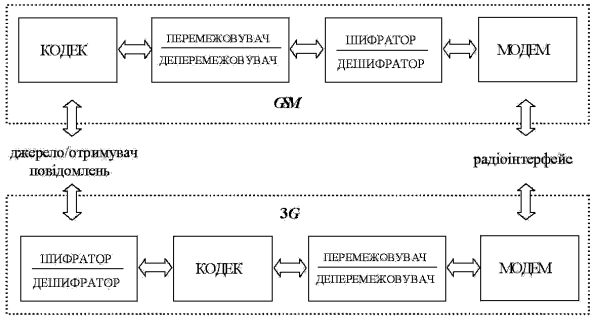

Рис. 2. Послідовність процедур кодування, перемежування, шифрування і модуляції в стандартах GSM і 3G

Наявність перерахованих недоліків робить GSM вразливою до різного роду атак, які спрямовані на порушення її інформаційної безпеки. Ілюзія безпеки в основному підтримувалась засекреченістю реалізації вищеназваних алгоритмів, не дивлячись на одне із основних положень криптології, яке каже: «криптостійкість алгоритму не може визначатися його засекреченістю» [4]. Приховування механізмів безпеки для систем широкого застосування – помилковий шлях, що не дозволяє аналізувати, своєчасно виявляти та виправляти слабкі сторони їх реалізації.

Механізми забезпечення безпеки в системах 3G. Зараз ведуться широкомасштабні роботи з розгортання ССЗ третього покоління, в яких реалізується суттєво відмінні і поки ще маловивчені схеми безпеки.

Для впровадження в Україні розглядаються дві радіотехнології покоління 3G: WCDMA UMTS, розроблена в межах проекту 3GPP, і cdma2000 (3GPP2). Обидві радіотехнології відповідають вимогам сумісності із системами 2G/2,5G та успадкували деякі їх особливості. Тож, не дивлячись на фундаментальні відмінності нових систем, в них застосовано вельми схожі схеми аутентифікації та розподілу ключів.

Алгоритмічне впровадження схем безпеки в 3G детально описано і визначено (табл. 1).

В ССЗ третього покоління використовується схема взаємної аутентифікації МС і мережі (рис. 3).

Таблиця 1

Основні алгоритми забезпечення безпеки в ССЗ покоління 3G

f0	Функція генерування параметрів виклику (Random challenge generating function)
f1	Функція аутентифікації мережі (Network authentication function)
f2	Функція аутентифікації абонента (User challenge-response authentication function)
f3	Функція генерування ключа шифрування (Cipher key derivation function)
f4	Функція генерування ключа перевірки цілісності (Integrity key derivation function)
f5	Функція генерування ключа анонімності (Anonymity key derivation function)

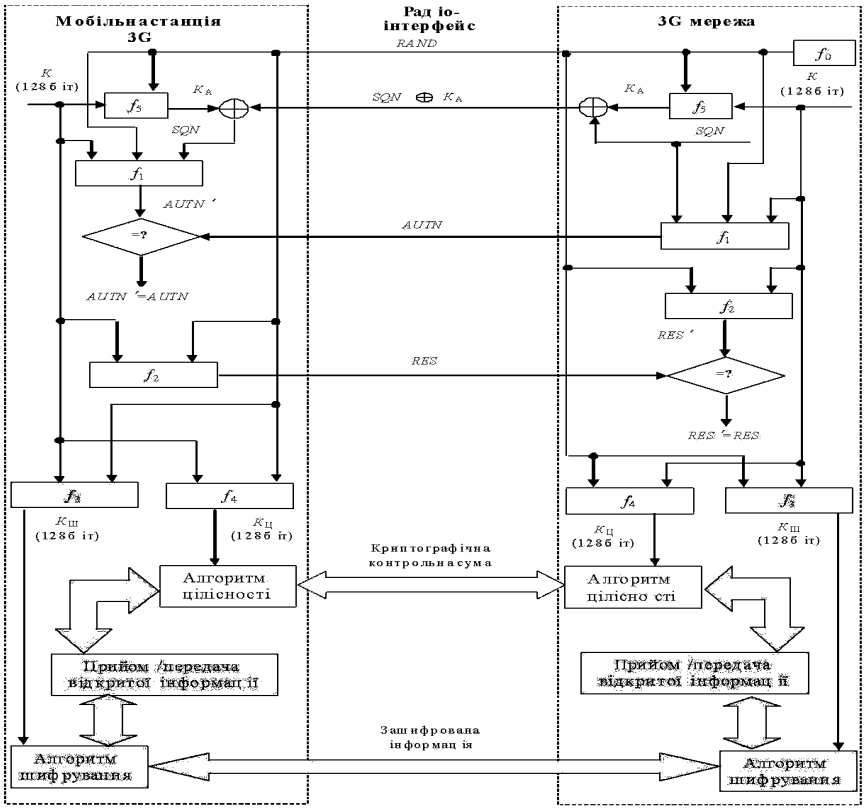

Рис. 3. Узагальнена схема ідентифікації та криптозахисту в системах 3G

Після отримання від МС запиту на обслуговування, мережа ініціює процедуру аутентифікації. Для цього центр аутентифікації мережі 3G генерує випадкове число RAND за допомогою функції f0, після чого переходить до генерування параметра аутентифікації AUTN, використовуючи функцію f1.

Крім вищезгаданого числа RAND для цього використовується попередньо розподілений довгостроковий секретний ключ К і номер переданої послідовності даних SQN (для ускладнення визначення місцезнаходження абонента він сумується за модулем 2 з ключем анонімності (anonymity key) КА, що генерується функцією f5). Потім "кортеж" параметрів RAND, SQN⊕КА й AUTN передається на МС через радіоефір. Для здійснення аутентифікації мережі в модулі ідентичності абонента, що міститься в МС, обчислюється AUTN'. Для цього, повторно сумуючи за модулем 2, обчислюється SQN⊕КА⊕КА=SQN, після чого за допомогою функції f1, кортежу К, прийнятого RAND і знайденого SQN визначається AUTN'. Далі МС, у випадку збігу обчисленого і прийнятого значень AUTN (AUTN'=AUTN), "визнає" мережу, а при розбіжності – відхиляє її.

Процедура аутентифікації МС мережею нагадує аналогічну процедуру в GSM. МС вираховує параметр RES за допомогою функції f2, на вхід якої надходять секретний ключ К і прийняте число RAND. Параметр RES передається в мережу, яка робить аналогічні обчислення, одержує RES' та порівнює його з RES. Якщо вони рівні, мережа "визнає" МС. Таким чином, у системах 3G передбачені процедури підтвердження достовірності як МС, так і безпосередньо мережі. Варто зазначити, що при розробці архітектури доступу в UMTS багато уваги звертається на забезпечення зворотної сумісності з GSM/GPRS. З погляду на безпеку, сумісність із системою-попередником, що має набагато слабший захист, вкрай небажана. Проте реалії ринку диктують свої закони.

Для забезпечення криптографічного захисту каналу мережа і МС генерують ключі шифрування та перевірки цілісності, кожен з яких довжиною 128 біт, використовуючи, відповідно, функції f3 і f4 (вхідними параметрами виступають числа RAND і K), після чого обидві сторони здійснюють потокове шифрування переданої інформації. Перевірка цілісності повідомлень проводиться шляхом формування й перевірки криптографічних контрольних сум.

Таким чином, першою і принциповою перевагою ССЗ покоління 3G є вільний доступ до інформації про алгоритмічні основи їхньої безпеки, що дозволяє вчасно вивчати й виправляти виявлені недоліки.

Другою перевагою практичного плану стала реалізація cdma2000 і UMTS схем взаємної аутентифікації. В GSM абонентський пристрій не був активним учасником процедури аутентифікації і не міг відхилити послуги мережі у випадку фрода. У системах 3G модуль ідентичності користувача зможе підтвердити або відкинути достовірність мережі, у якій абонент має реєструватися.

Третя важлива перевага 3G – впровадження сучасних і більш стійких алгоритмів шифрування та аутентифікації. Так, в cdma2000 за основу було взято розширений стандарт шифрування AES, відомий також як Rijndael [4]. У ньому використано блоковий шифр, який зашифровує 128-бітові блоки за допомогою 128-бітового ключа. За наявними оцінками, мінімальний порядок складності такого шифру щонайменше ≈ 287. У системі UMTS криптографічне ядро алгоритму шифрування ґрунтується на шифрі KASUMI, де 64-х бітові блоки даних зашифровуються вісьма ітераціями під управлінням ключа довжиною 128 біт (довжина ключа в GSM – 64 біти).

Четверта перевага, що здатна істотно вплинути на стійкість шифрування – більш раціональне, з погляду класичної криптографії, застосування перешкодостійкого кодування. Послідовність виконання кодування, перемежування, шифрування та модуляції в GSM і в ССЗ третього покоління показано на рис. 3 Застосування до шифрування перешкодостійкого кодування, завжди пов'язаного із внесенням надмірності у дані, що шифруються, здатне істотно полегшити криптоаналіз отриманого шифртексту. Можна навіть стверджувати, що в кінцевому результаті надання криптоаналітикам таких можливостей практично призвело до злому всієї системи безпеки стандарту GSM. З метою усунення зазначеного недоліку послідовність процедур кодування і шифрування в системах 3G була змінена (рис. 3).

Не менш важливою є ще одна перевага, що не належить до категорії схем забезпечення інформаційної безпеки мереж 3G, проте являється прямим наслідком системотехнічних особливостей розглянутих радіотехнологій. Використання в ССЗ 3-го покоління сигналів із розширенням спектра істотно ускладнює радіоперехоплення, а отже, фізичний доступ до інформації, що підлягає криптоаналізу.

Висновки

Таким чином, у схемі безпеки 3G були враховані основні недоліки стандарту GSM, у результаті чого було створено архітектуру безпеки, що базується на реальних загрозах і ризиках абонентів ССЗ. Не виключено, що реалізовані в них штатні механізми безпеки згодом можуть розглядатися як повноцінна ланка багаторівневої системи інформаційної безпеки при використанні ССЗ 3-го покоління для забезпечення повсякденної діяльності ЗС України та враховані при створенні сучасної автоматизованої системи управління військами та зброєю. Необхідний рівень конфіденційності зв'язку може гарантуватися при застосуванні додаткового абонентського шифрування в якості ще однієї ланки захисту.

Список літератури

1. Рудик В.В. Актуальні проблеми та напрямки розвитку системи зв'язку Збройних Сил України як складової частини системи управління військами (силами) / В.В. Рудик // Наука і оборона. – 2005. – № 2. – С. 22–28.

2. Security Management : Recommendation-GSM 12.03, version 3.0.0. – [Dated Nov. 15, 1988].

3. Biryukov A. The Real-Time Cryptanalysis of A5/2 / Alex Biryukov, Adi Shamir, David Wagner // Fast Encryption Software Workshop 2000, April 10, 2000. – New York City, 2000.

4. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М. : Binom, 2007. – 384 с.

Надійшла до редколегії 18.01.2013

Рецензент: канд. техн. наук Б.П. Томашевський Академія сухопутних військ ім. гетьмана Петра Сагайдачного, Львів.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СУЩЕСТВУЮЩИХ И ПЕРСПЕКТИВНЫХ СИСТЕМАХ ПОДВИЖНОЙ СВЯЗИ

А.О. Москаленко, О.В. Федін

В статье представлены результаты сравнительного анализа механизмов обеспечения информационной безопасности стандартов сотовой связи второго и третьего поколений.

Ключевые слова: *системы подвижной связи, механизмы обеспечения информационной безопасности, фрактальные структуры.*

INVESTIGATION OF MECHANISMS OF INFORMATION SECURITY IN CURRENT AND FUTURE MOBILE SYSTEMS

A.A. Moskalenko, A.V. Fedin

The article presents results of a comparative analyze the mechanisms information security standards cellular second and third generations.

Keywords*: mobile communication systems, mechanisms to ensure information security, the fractal structure.*