УДК 004.056

[1]Юдін О.К., д.т.н.,
[1]Ільєнко А.В., к.т.н.,
[1]Зюбіна Р.В.,
[2]Сергеєв-Горчинський О.О.

ЗАХИСТ КРИТИЧНОЇ МЕДИЧНОЇ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ GSM ТИПУ НА БАЗІ ЕЛІПТИЧНИХ КРИВИХ

[1]Національний авіаційний університет
[2]НТУУ «Київський політехнічний університет»
kszi@ukr.net
chunariova@gmail.com
ruslana.zubina@gmail.com
alysergeev@gmail.com

Проведено аналіз існуючих моделей організації віддаленого медичного обслуговування, що проводиться при відсутності можливості прямих консультацій лікаря у стаціонарних умовах. Визначено основні напрямки розвитку інформаційно-телекомунікаційних систем медичного призначення. Проведено дослідження організації захищеного каналу зв'язку між лікарем, хворим та лікарем-консультантом, що знаходиться в стаціонарних умовах шпиталю. Розроблено загальну структурно логічну та структурно-аналітичну модель системи захисту медичної інформації, яка передається через мережу GSM. Розроблено модель побудови безпровідного терміналу підтримки GSM зв'язку з вбудованою системою сучасного криптографічного захисту з використанням вдосконаленого протоколу Діффі-Хеллмана та протоколу AES-256 в режимі OFB для забезпечення надійної передачі конфіденційної медичної інформації на базі використання криптографії еліптичних кривих

Ключові слова: GSM, еліптичні криві, криптографічний захист, конфіденційність, критична медична інформація.

Вступ

Інформаційно-комунікаційні системи передачі даних стали важливою складовою передачі критичної медичної інформації для забезпечення кваліфікованої, спеціалізованої та оперативної медичної допомоги в умовах, що не дозволяють пацієнту проходити медичний огляд, обстеження чи лікування амбулаторно. Розглянуто атаки на інформаційні ресурси, які виникають в бездротовому каналі передачі даних. Поєднання телекомунікаційних систем та медичної інформатики надало можливість впровадження нового науково-практичного напрямку, який отримав назву – телемедицина [1]. В 1997 Всесвітньою Організацією Охорони Здоров'я було запропоновано таке визначення.: *телемедицина* – термін, який визначає діяльність і системи, пов'язані з наданням медичної допомоги на відстані за допомогою телекомунікаційних технологій, управління охороною здоров'я, які направлені на сприяння розвитку світової охорони здоров'я, здійснення епідеміологічного нагляду, а також навчання і проведення наукових досліджень в області медицини.

Концепція медичної сучасної телемедицини розвивається в наступних основних напрямках:

- наукові дослідження;
- надання навчальних послуг;
- надання медичних послуг.
- управління медичними структурами, тощо.

В цілому, телемедицину можна розділити на дві основних складових, а саме: медичну, до якої належать: особиста кар-

тка пацієнта, системи моніторингу стану пацієнта, аналогові та цифрові дані про стан людини, результати огляду та інше; телекомунікаційну – процес обробки, зберігання та передачі критичних медичних даних.

Мета

Метою статті є аналіз існуючих моделей організації віддаленого медичного обслуговування. Необхідно провести дослідження, що стосуються організації захищеного каналу зв'язку між лікарем, хворим та лікарем-консультантом, який знаходиться в стаціонарних умовах шпиталю, а також розробити загальну структурно логічну та структурно-аналітичну модель системи захисту медичної інформації на базі сучасних криптоалгоритмів.

Основні матеріали дослідження

В умовах передачі критичної медичної інформації між консультативним центром та місцем знаходження хворого виникає потреба організації безперервного та захищеного каналу зв'язку. По-перше це стосується організації системи захисту персональних даних пацієнта та інформації про стан його здоров'я, а по-друге такий підхід дозволить госпіталям мати первинну інформацію про стан хворого, ще до його прибуття і тим самим дасть виграш часу для підготовки та організацій процесу надання оперативної допомоги в критичних ситуаціях.

Нині на ринку існує лінійка мобільних телемедичних систем, наприклад *DiViSy TM21*, які мають можливість передавати, обробляти та накопичувати інформацію в різних формах її представлення. За допомогою вбудованих систем аудіо та відео моніторингу, такі комплекси дають змогу обробляти дані про стан пацієнта та налаштовувати відеоконференцзв'язок для надання консультативних послуг спеціалістам вузького профілю.

Сучасні мобільні телемедичні системи використовують такі канали зв'язку:

1. Супутникові (залежно від використовуваного супутника швидкість передачі інформації варіюється від 100 Кбіт/с до 4 Мбіт/с);
2. Radio Ethernet на дозволених частотах 2,4 ГГц, 5,25-5,35 ГГц та 5,7-5,8 ГГц;
3. Канали мобільного звязку *GSM* (9,6 Кбіт/с), *CDMA* (14400 Кбіт/с), *GPRS* (від 13 до 52 Кбіт/с) та інші;
4. Радіоканали ультракоротких хвиль (до 9,6 Кбіт/с);
5. Канали *Wi-Fi* мереж;
6. Інші спеціалізовані канали.

Під час використання телемедичної системи *DiViSy TM21* в залежності від потрібної якості зображення в режимі реального часу були отримані показники, представлені табл. 1.

Таблиця 1. Показники передачі телемедичної інформації в режимі реального часу

Стандарт кодування	Оціночна якість 8 Кбайт/кадр	Середня якість 16 Кбайт/кадр	Висока якість 64 Кбайт/кадр
GSM (9,6 Кбіт/с)			
MJPEG	1кадр/5 сек	1 кадр/10 сек	1кадр/40 с
Inmarsat Regional B-gan (до 100 Кбіт/с)			
MJPEG	1-1,5 кадр/с	1 кадр/2 с	1 кадр/5 с
MPEG4/H.263+	16 кадрів/с	10 кадрів/с	4 кадра/с

Під час роботи в другому режимі, відео, аудіо та телемедична інформація попередньо зберігається на жорсткому диску. Такий режим роботи надає можливість попередньо вибрати потрібний фрагмент запису для його передачу лікарю-консультанту.

Таблиця 2. Показники передачі телемедичної інформації в режимі попереднього запису

1 хвилина відео/ час передачі	**Оціночна якість**	**Средня якість**	**Висока якість**
GSM (9,6 кбіт/с)			
MJPEG	2 години	4 години	16 години
Inmarsat Regional B-gan (до 100 кбіт/с)			
MPEG2/4	3 Мбайта	6 Мбайт	24 Мбайта
Час передачі1 хвилини відео	4 хвилини	8 хвилин	30 хвилин
M-JPEG	8 Мбайт	18 Мбайт	70 Мбайт
Час передачі1 хвилини відео	12 хвилин	25 хвилин	90 хвилин

Як видно з табл. 2 , кодування відео при використанні *MPEG* 2/4 дозволяє досягти вищої швидкості передачі, однак кодування за допомогою *M-JPEG* є більш завадостійким.

Використання таких медичних комплексів у зоні прямої видимості досягає відстані передачі інформації до 30 км зі швидкістю до 11 МБ/с (реальна швидкість 6 МБ/с, *Radio Ethernet*). В гірській місцевості потрібно використовувати ретранслятори. Однак існують такі ситуації, коли використання швидкісних каналів зв'язку неможливе, тому доцільним є використання такого каналу зв'язку, який отримав найбільше поширення. Крім того, використання таких комплексів у віддалених районах та в надзвичайних ситуаціях не завжди є доцільний, тому і досі найпопулярнішим залишається використання мобільних пристроїв для передачі інформації про стан здоров'я хворого.

Як відомо, *Global System for Mobile communication (GSM)* на сьогодні є найпоширенішою технологією зв'язку у світі. У порівнянні з іншими видами зв`язку, *GSM* більш поширене завдяки щільному розташуванню приймачів сигналу, легкості використання та невисокої ціни пристроїв.

Проте дуже часто виникають проблеми, пов'язані із недоліками системи захисту. Адже доступ до конфіденційної інформації та прослуховування третьою особою можливе як для звичайних абонентів, так і для з'єднань державного значення. Зазвичай криптографічні алгоритми, що покладені в основу системи криптографічного захисту або не розголошуються, що вже свідчить про їх ненадійність [2], або мають низький ступінь захисту, тобто залежать цілком від довжини ключа, та стають повільнішими при його збільшенні, а це не є допустимим при обробці інформації в режимі реального часу.

На сьогодні використовують три види поточних алгоритмів для шифрування *GSM*. Всі вони відносяться до групи A5. Це потоковий шифр спеціально розроблений для захисту мережі *GSM*. A5 підключений на обох мобільних терміналах та базових станціях операторів мереж (рис.1). Алгоритм A5/1 був зламаний в 2009 році [3]. У 2010р. розроблена практична атака «Сендвіч», вона дозволяє атакуючому витягти 128-бітовий ключ [4].

Таким чином, стає нагальною потреба розробки моделі та пристрою, що дозволить забезпечувати криптографічно захищений зв'язок при підтримці *GSM*.

Розглянемо атаки, які виникають в бездротовому каналі передачі інформації. Атаки даного виду можуть бути пасивними – зловмисник прослуховує канал зв'язку між мобільним пристроєм і базовою станцією; або активними - на додаток до прослуховування, зловмисник вносить або надає вплив на вже циркулюючий трафік. Хоча можливості активних атак істотно знижені за рахунок використання криптографічного захисту переданої інформації, пасивні атаки, такі як аналіз трафіку і відслідкування місця розташування користувачів, все ще ймовірні.

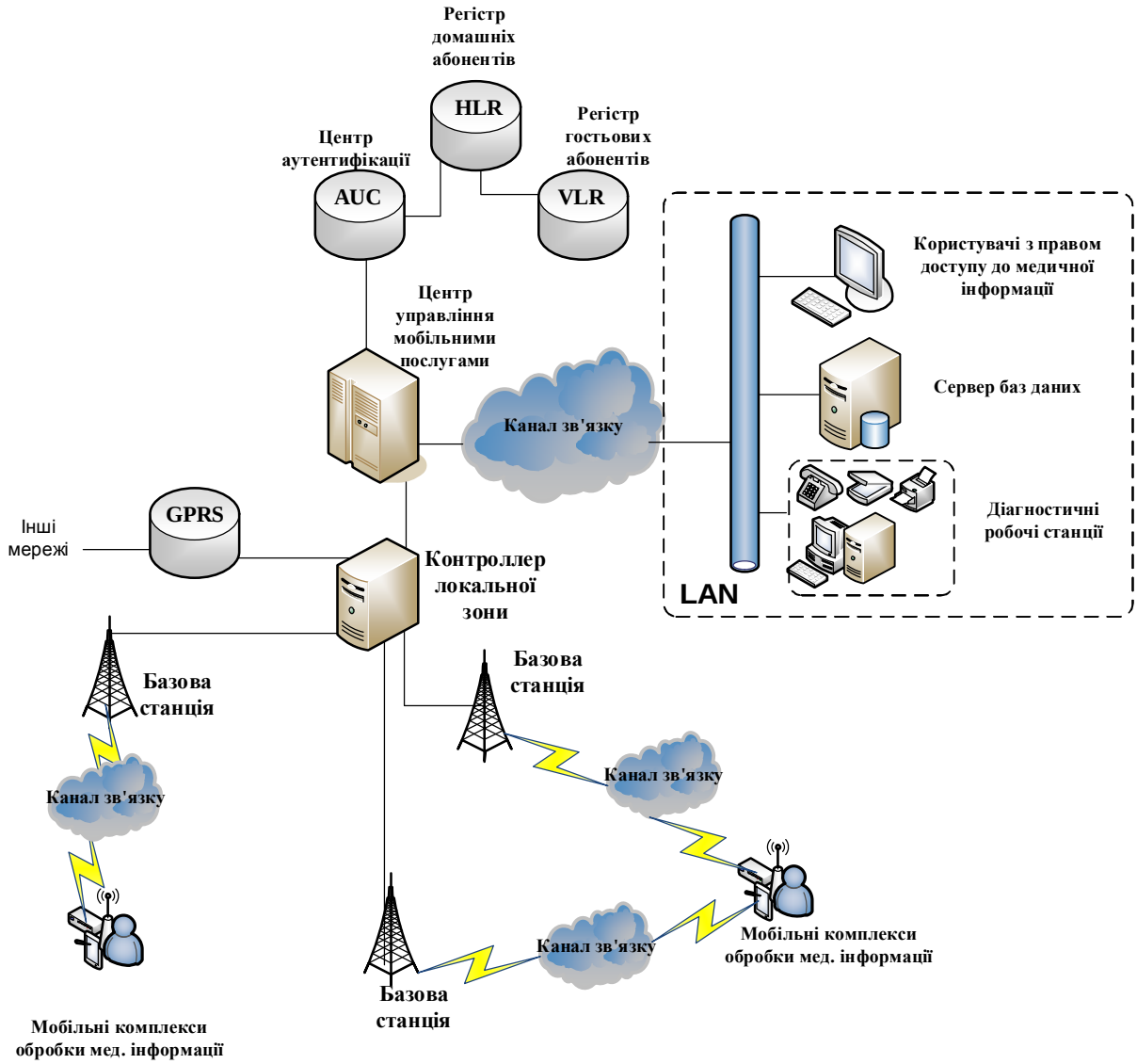

Рис.1 Структура інформаційно-телекомунікаційної мережі медичного призначення GSM типу

На рис. 2 представлено загальну схему системи захисту інформації, яка передається через мережу *GSM*.

Розглянемо підходи до створення закритих корпоративних мереж.

1. Технологія на базі мережі з комутацією пакетів.

Якщо захищене з'єднання організовується на базі мережі з комутацією пакетів (*GPRS, EDGE, 3G, 4G, Wi-Fi* и т.д.) з динамічним виділенням *IP- адрес*, то виникає необхідність в спеціальному сервері (*SIP*сервер), який забезпечує проходження по мережі викликів між абонентами та встановлення сеансу зв'язку. Часто для цього використовують протокол *SIP (Session Initiation Protocol)*.

Наявність *SIP* сервера – це пролом в системі захисту. А саме, в наслідок того, що сервер знаходиться на непідконтрольній території, користувач не зможе перевірити ПЗ серверу на наявність шпигунського програмного забезпечення та «поліцейских функцій».

Звичайно, можливо використання підключення без *SIP* сервера, зі статичними *IP*-адресами та встановлювати з'єднання безпосередньо між абонентами. Але таке підключення вельми проблематично з організаційної точки зору, до того ж, прив'язує абонента до одного провайдера послуги безпровідного зв'язку або до однієї *Wi-Fi* точки доступу.

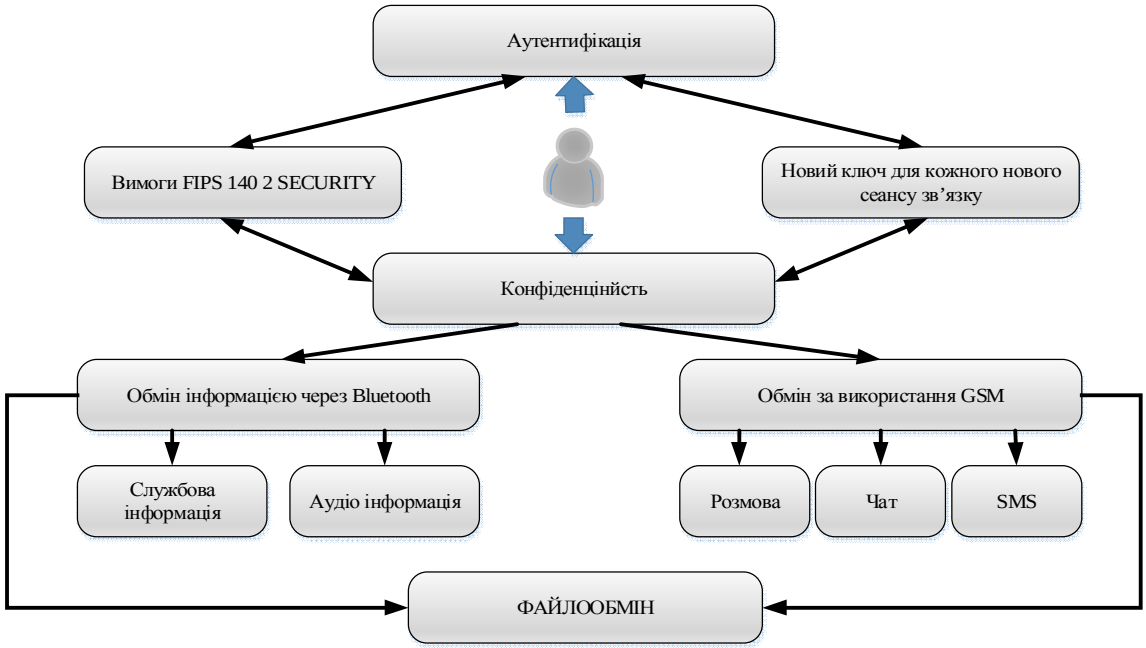

Рис.2. Схема моделі системи захисту

2. Технологія на базі мережі с комунікацією каналів.

З'єднання з комутацією каналів (*CSD*) має в цьому сенсі незаперечну перевагу, оскільки дозволяє абоненту використовувати підключення до будь-якого оператора безпровідного зв'язку та здійснювати захищене з'єднання безпосередньо без будь-якої участі третьої сторони.

На сьогодні використання протоколу *CSD* отримало нове дихання у зв'язку з масовим використанням технологій *M2M*.

Протокол *CSD* працює будь в якому місці, де є покриття *GSM* мережі. 3*G* та *Wi-Fi* істотно поступаються за цим параметром (зазвичай, це великі міста).

В якості алгоритмів криптографічного захисту запропоновано обрати сучасний блоковий шифр *AES* 256, що працює в режимі *OFB*. Такий вибір алгоритмів при програмно-апаратній реалізації дозволить здійснювати шифрування з надійністю високого ступеня в режимі реального часу та забезпечить вдалі результати під час передачі інформації по захищеному каналу. Адже режим *OFB* завдяки своїй структурі забезпечує локалізацію помилки, що отримана при шифруванні, в межах одного блоку, таким чином при дешифруванні помилки не впливають на все повідомлення.

Важливим аспектом організації системи захисту є процес автентифікації. Запропоновано використання посиленого алгоритму Діффі-Хеллмана за використанням еліптичних кривих.

Нехай над полем *F* задана еліптична крива у формі Монтгомері [5]:

$$By^2 = x^3 + Ax^2 + x,$$

де A, B $\in$ F та B(A2 − 4) ≠ 0

Точка *P = (x, y)* на еліптичній кривій у вигляді Монтгомері може бути представлена в Монтгомері координатах *P = (X: Z)*, де *P = (X: Z)*, проективні координати і $x = X / Z$ для $Z \neq 0$.

Визначено операцію додавання наступним чином:

$$P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2),$$

де $x_3 = B\left(\frac{x_2 - x_1}{y_2 - y_1}\right)^2 - A - x_1 - x_2$, $y_3 = \frac{(2x_1 + x_2 + A)(y_2 - y_1)}{x_2 - x_1} - \frac{B(y_2 - y_1)^3}{(x_2 - x_1)^3} - y_1$

Добуток визначається співвідношенням:

$$P_3 = 2 * P_1,$$

де $x_3 = \frac{\left(x_1^2 - 1\right)^2}{4x_1\left(x_1^2 + Ax_1 + 1\right)}$, $y_3 = \frac{\left(2x_1 + x_1 + A\right)\left(3x_1^2 + 2Ax_1 + 1\right)}{2By_1} - \frac{B\left(3x_1^2 + 2Ax_1 + 1\right)^3}{\left(2By_1\right)^3}$.

Протокол Діффі-Хеллмана, як відомо [6], є уразливим до атаки «Людина в середині», тому запропоновано використання його посилену модифікацію. А саме протоколу *HMQV* з вбудованою автентифікацією.

Розглянемо протокол у формі HMQV. Нехай Аліса має статичну ключову пару (W_a, w_a), де W_a її відкритий ключ і w_a її секретний ключ. Боб має статичну ключову пару (W_b, w_b) з відкритим та секретним ключами відповідно. Визначимо $\bar{R}$. Нехай $R = (x, y)$ буде точкою на еліптичній кривій зазначеного типу. Тоді

$$\bar{R} = \left(x \bmod 2^L\right) + 2^L,$$

де

$$L = \left\lceil \frac{\left(\log_2 n\right) + 1}{2} \right\rceil,$$

і n є порядок використовуваного генератора точки P. Таким чином, $\bar{R}$ є перші L бітів координати x для R. Визначимо кофактор h наступним чином:

$$h = \frac{|G|}{n},$$

де $|G|$ є порядок групи G, причому слід врахувати, що з технічних причин має виконуватися вимога: *gcd (n, h) = 1.*

Протокол має наступний вигляд.

1) Аліса створює ключову пару (R_a, r_a) генеруючи випадково r_a і обчислюючи $R_a = r_a * P$, де P - точка на еліптичній кривій (в нашому випадку у формі Монтгомері, з операціями додавання та добутку, що описані вище). Після цього вона посилає тимчасовий відкритий ключ $H(R_a)$ Бобу, де $H(R_a)$ значення хеш-функції.

2) Боб створює ключову пару (R_b, r_b) генеруючи випадково r_b і обчислюючи $R_b = r_b * P$. Після створення пари він посилає свій тимчасовий відкритий ключ $H(R_b)$ Алісі.

3) Аліса перевіряє, що тимчасовий відкритий ключ R_b належить групі G, а також те що R_b не є нульовим елементом. Після цього обчислює груповий елемент K_{ab}, як

$$K_{ab} = h * s_a * S_b,$$

де

$$s_a = (r_a + \bar{R}_a w_a) \bmod n,\ S_b = R_b + \bar{R}_b W_b.$$

Якщо $K_{ab} = 0$, Аліса відхиляє дані, що отримано від Боба. В іншому випадку, вона приймає обчислений результат, як загальний секретний ключ.

4) Боб перевіряє, що тимчасовий відкритий ключ R_a належить групі G, а також що R_a не є нульовим елементом. Обчислює груповий елемент K_{ba}, як

$$K_{ab} = h * s_b * S_a$$

де $s_b = (r_b + \bar{R}_b w_b) \bmod n,\ S_a = R_a + \bar{R}_a W_a$.

Якщо $K_{ba} = 0$, Боб відхиляє дані, що отримано від Аліси. В іншому випадку, він приймає обчислений результат, як загальний секретний ключ.

Саме використання хешування дозволяє зв'язати партнера з ключовим матеріалом. Таким чином, процес автентифікації стає вбудованим в протокол обміну ключами без використання цифрового підпису, який може ускладнювати протокол та вимагати значних витрат часу (при створенні цифрового підпису та при його верифікації).

Отже, використання мобільних медичних комплексів, як і мобільних терміналів в умовах надзвичайних ситуацій вимагає організації системи безпеки передачі критичної медичної інформації.

Тому у роботі розроблено модель побудови безпровідного терміналу підтримки *GSM* зв'язку з вбудованою системою сучасного криптографічного захисту для забезпечення надійної передачі конфіденційної медичної інформації між абонентами на базі використання криптографії еліптичних кривих.

Висновки

Проведено аналіз існуючих моделей організації віддаленого медичного обслуговування, що проводиться при відсутності можливості прямих консультацій лікаря у стаціонарних умовах. Визначено основні напрямки розвитку інформаційно-телекомунікаційних систем медичного призначення. Проведено дослідження організації захищеного каналу зв'язку між лікарем, хворим та лікарем-консультантом, що знаходиться в стаціонарних умовах шпиталю. Розроблено загальну структурно логічну та структурно-аналітичну модель системи захисту медичної інформації, яка передається через мережу *GSM*. Розроблено модель побудови безпровідного терміналу підтримки *GSM* зв'язку з вбудованою системою сучасного криптографічного захисту з використанням вдосконаленого протоколу Діффі-Хеллмана та протоколу *AES*-256 в режимі *OFB* для забезпечення надійної передачі конфіденційної медичної інформації на базі використання криптографії еліптичних кривих.

Список літератури

1. Юдін О., Курінь К. Дослідження взаємного впливу процедур шифрування та стиснення інформаційного повідомлення //Наукоємні технології. – 2010. – Т. 6. – №. 2. – С. 64-68.

2. Фергюсон Н., Шнайер Б. Практическая криптография. – М. и др. : ИД Вильямс, 2005.

3. Biryukov A., Shamir A., Wagner D. Real Time Cryptanalysis of A5/1 on a PC //Fast Software Encryption. – Springer Berlin Heidelberg, 2001. – С. 1-18.

4. Dunkelman O., Keller N., Shamir A. A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony //IACR Cryptology ePrint Archive. – 2010. – Т. 2010. – С. 13.

5. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. – М : URSS, 2006.

6. Diffie W., Hellman M. E. New directions in cryptography //Information Theory, IEEE Transactions on. – 1976. – Т. 22. – №. 6. – С. 644-654.

Статтю подано до редакції 09.12.2015