Карпінський В. Моделювання захищеного безпровідного передавання інформації в сенсорній мережі / Карпінський В., Антош Б., Яремчук Т. // Вісник ТНТУ. — 2011. — Том 17. — № 2. — С.196-202. — (математичне моделювання. математика. фізика).

УДК 004.94

В. Карпінський[1]; Б. Антош[2]; Т. Яремчук[3]

[1]Тернопільський національний технічний університет імені Івана Пулюя
[2]Університет в Бєльську-Бялій, Польща
[2]Тернопільський національний економічний університет

МОДЕЛЮВАННЯ ЗАХИЩЕНОГО БЕЗПРОВІДНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В СЕНСОРНІЙ МЕРЕЖІ

Резюме. *Розроблено комп'ютерну програму для моніторингу за прийомами (хопами), що здійснюються мікроелектронними пристроями в безпровідній сенсорній мережі. За допомогою розробленої комп'ютерної програми проведено моделювання захищеного безпровідного передавання динамічного стрибкоподібного коду та виявлено характерні особливості функціонування сенсорної мережі.*

Ключові слова: *безпека, безпровідна передача, моделювання, сенсорна мережа.*

V. Karpinskyi, B. Antosz, T. Yaremchuk

MODELING OF SECURITY WIRELESS INFORMATION TRANSMISSION IN SENSOR NETWORKS

The summary. *Was developed a computer program for hops monitoring over microelectronic devices in wireless sensor network. Via this computer program was held modeling (simulation) of secure wireless transmission of wireless and were found characteristic features of sensor network functioning.*

Key words: *security, wireless transmission. modeling, sensor network*

Постановка проблеми в загальному вигляді та аналіз досліджень. Поле діяльності в галузі систем безпеки та контролю доступу є досить широким, включаючи вибрані на ринку технології розробки консольної бібліотеки для обслуговування мікроконтролерів при застосуванні модуля USART (Universal Synchronous/Asynchronous Receiver/Transmitter – універсальний синхронний/асинхронний приймач/передавач) із шифрувальною підпрограмою. Відповідно до припущення, система повинна бути сучасною, перспективною та, що найважливіше, впровадженою на практиці, перевіреною та діючою. Подібну систему запатентувала фірма Microchip. Вона базована на динамічному чи стрибкоподібному коді (hopping code) система KeeLoq [1]. Ця система використовується в багатьох галузях та є однією з найпоширеніших апаратних рішень, що ґрунтується на регістрі зсуву з нелінійною функцією. Згадана функція є стандартною складовою, яка використовується в радіозв'язку та картах доступу як найменш уразлива для криптоаналітичних атак у порівнянні зі стандартною лінійною функцією в поєднанні з регістром зсуву. Інші системи, в яких застосовуються нелінійні функції, це – Achterbahn, Grain, Trivium, VEST.

Одностороннім системам притаманні два істотні недоліки: код, який передається передавачем, загалом відомий і кількість комбінацій є відносно низькою. З цієї причини ці пристрої можуть бути уразливі щодо несанкціонованого доступу [2]. Тому надійною буде система, в якій вищезгадані недоліки усунуті. До такого рішення належить змінно-кодова система KeeLoq, в якій передбачена велика кількість можливих комбінацій коду [3, 4]. З метою безпеки також повинна виконуватися друга умова – система не може вдруге реагувати на цей самий трансльований код [5]. Односторонній зв'язок у рамках технології KeeLoq запропонував доктор наук Ф.

Брувер з компанії Nanoteq Ltd., а систему шифрування розробив професором Ґ. Кун. У подальшому її реалізував у мікросхемі доктор наук В. Сміт з компанії Nanoteq Ltd. У середині 80-х років система KeeLoq набула стрімкого розвитку після купівлі ліцензії на нього компанії Microchip Technology Inc. Відтоді ця система набула великої популярності завдяки своїй надійності, а також низькій вартості таких мікросхем, як NTQ105/106/115/125D/129D та HCS101/2XX/3XX/4XX/5XX. Їх застосовують у більшості безпровідних систем контролю доступу фірми Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Clifford, Shurlok, Jaguar.

Формування цілей статті (постановка завдання). До цілей статті належить удосконалення придатної функціонуючої системи моделювання безпечної комунікації в безпровідній сенсорній мережі (БСМ) в галузі електронної охорони об'єктів.

Моделювання безпечного безпровідного передавання інформації

Об'єкт досліджень. Система моделювання безпечної комунікації в БСМ на підставі системи KeeLoq грунтується на двох пристроях – шифраторі HCS410 та дешифраторі HCS500 [6]. З урахуванням технічної документації на вищезазначені засоби розроблено метод організації та оптимізації процесу моделювання захищеного безпровідного передавання інформації шляхом її шифрування та розшифрування. Розроблена комп'ютерна програма на мові C# разом із нижченаведеним описом зможуть бути придатними для наукових та інженерних працівників, а також становити дидактичний матеріал для студентів, які хочуть ознайомитися з технологією динамічного коду KeeLoq. Комп'ютерна програма надалі іменується KeeLoq Dumping Console.

Реальним фізичним досліджуваним засобом для моделювання є прототипна плата, побудована на базі 16-бітного мікроконтролера PIC24FJ128 (рис. 1) [7]. До інтерфейсів під'єднані схеми шифратора і дешифратора KeeLoq. Зазначений мікроконтролер моніторує їх через розміщену в своїй пам'яті програму.

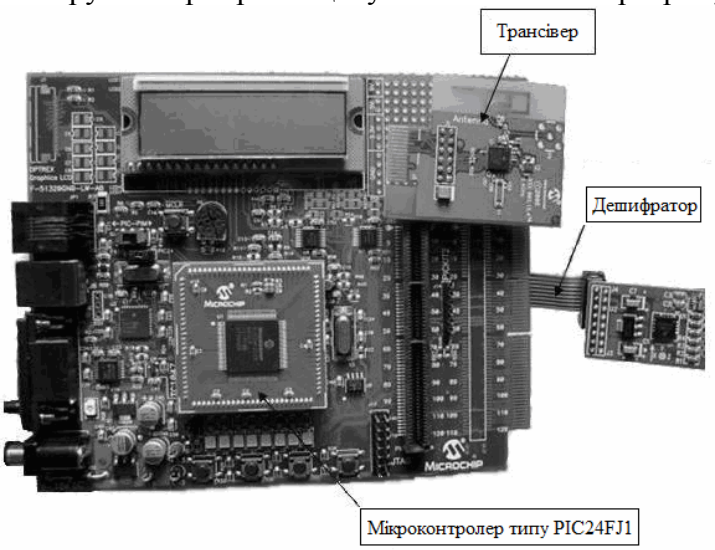

Рисунок 1. Система KeeLoq з дешифратором HCS500 на прототипній платі PIC24FJ128

Генерування та ініціалізація змінних. При першому введенні в дію мікроелектронного пристрою HCS410, отже, вже у фазі виготовлення, він програмується спеціальним всадом, що містить програму машинною мовою. Серед записуваних до мікроконтролера даних знаходиться така інформація, як код виробника (записується до пам'яті ROM) і серійний номер (записується до пам'яті EEPROM). Код виробника є однаковий для всіх пристроїв даного виробника або для партії пристроїв, які повинні між собою співпрацювати. Завдяки спеціальним алгоритмам інтегральна

мікросхема генерує ключ шифрування та ініціювальне зерно SEED, яке потрібне для узгодження передавача з приймачем [8]. Алгоритм генерування ключа з серійного номера та коду виробника – це алгоритм, розроблений виробником і відомий лише йому.

Важливу роль відіграє пам'ять EEPROM, яка, не зважаючи на свої невеликі габарити, достатня для завантаження найважливіших даних. До них належать: 28/32-бітний серійний номер, який є унікальним для кожної окремої мікросхеми; 64-бітне ініціювальне зерно чи зародок (seed); 64-бітний ключ шифрування, що згенерований під час виробництва; 16-бітний лічильник синхронізації та опції конфігурації.

Лічильник синхронізації становить базу до кожного нового передавання. Достатньо зміни на один біт і значно змінюється весь трансльований код. Після кожного натиснення клавіші на пульті керування лічильник інкрементується, тобто збільшується на один.

У програмі-симуляторі відразу ж після ввімкнення всі поля порожні. Їх можна також вигенерувати через меню „Program->Reset". Клікаючи по черзі „Generate Manufacturer Code", а потім „Generate Serial Number", заносяться до віртуальної пам'яті EEPROM пульта бінарні значення, які в процесі виготовлення надає фірма-виробник. Функція „Generate Master Key" ініціює виконання згідно з опрацьованим виробником ускладненим алгоритмом процесу, в результаті чого отримується ключ шифрування. Додатково лічильник синхронізації встановлюється в половині свого діапазону, бо це має місце для випадку мікрочипа HCS410.

Режим навчання. Мікроелектронний пристрій HCS410 у режимі навчання, а отже, після натиснення, наприклад, комбінації клавіш, замість типового слова із динамічним кодом передає в ефір ініціювальне зерно SEED [8].

У програмі-симуляторі режим „Learn Mode" приймача задіюється кнопкою. В цей момент програма очікує на передавач, на надання ініціювального зерна SEED. Кнопкою „Send SEED" на пульті керування дозволяється висилання зерна і тим самим на спарювання пульта керування з приймачем. Дані пульта керування перетворюються приймачем і запам'ятовуються в його пам'яті EEPROM (рис. 2-4).

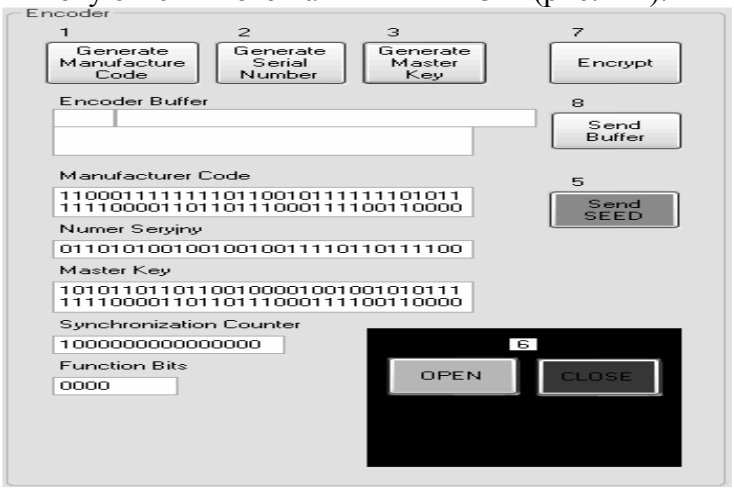

Рисунок 2. Знімок екрана № 1 авторської програми

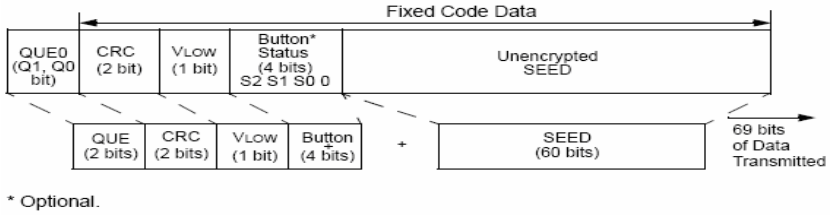

Рисунок 3. Структура слова ініціювального зерна

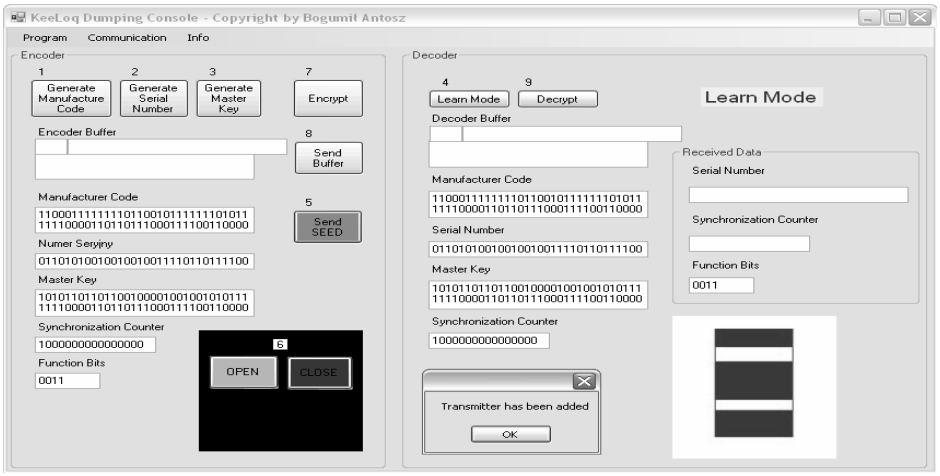

Рисунок 4. Знімок екрана № 2 авторської програми

Шифрування. Стан лічильника синхронізації, біти функції та різницеві значення шифруються за допомогою ключа шифрування в 32-бітний криптоблок. Такий блок дозволяє отримати приблизно 4 трильйони змін динамічного коду. 32-бітний криптоблок, пов'язаний з серійним номером і функціональними бітами, утворює фрейм інформації, що передається до дешифратора. Зміна лічильника синхронізації на 1 біт впливає на ~50 % зміну стрибкоподібного коду.

Режим стрибкоподібного коду. Мікросхема HCS410 вмикається після викриття сигналу короткого замикання на кнопці, вичікуючи потім приблизно 30 мс на повернення кнопки до вихідної позиції. Підготовлена інформація, тобто зашифрована до вигляду динамічного коду, надається в ефір. Кожного разу після натиснення кнопки висилається інша інформація. Натиснення та притримування кнопки спричиняє передавання однієї і тієї ж самої інформації доти, аж поки кнопка не вивільниться або не мине призначений час. Надаваний передавачем код не повториться через приблизно 65000 наступних циклів, що випливає з величини лічильника синхронізації. Додавання залишкових бітів може бути використане дешифратором для розширення кількості комбінації до 192000. Якщо під час передавання однієї попередньої рамки натиснеться на іншу кнопку, то комунікація переривається. Якщо ж натиснеться комбінація клавіш та якщо ця сама комбінація буде натиснена до 2 секунд від першого випадку, то надавання переривається й розпочинається нове передавання. В таблиці 1 наведено функції, які можна передати [8].

Таблиця 1

Функції передавання

	LC0	S2	S1	S0	Comments
1	0	0	0	1	Normal Code Hopping transmission
2	0	0	1	0	Normal Code Hopping transmission
3	0	0	1	1	Delayed seed transmission if allowed by SEED and TMPSD/Normal Code Hopping transmission
4	0	1	0	0	Normal Code Hopping transmission
5	0	1	0	1	Normal Code Hopping transmission
6	0	1	1	0	Normal Code Hopping transmission
7	0	1	1	1	Immediate seed transmission if allowed by SEED and TMPSD/Normal Code Hopping transmission
8	1	0	0	0	Transponder mode

Формат передавання даних. Кожному передаванню даних передує преамбула та заголовок, а завершується воно визначеною паузою мовчання між наступною трансляцією. Відразу ж за заголовком надається інформація – 69 бітів, що містять 32 біти зашифрованих даних та решту незакодовану 37-бітну частину (рис. 5) [8].

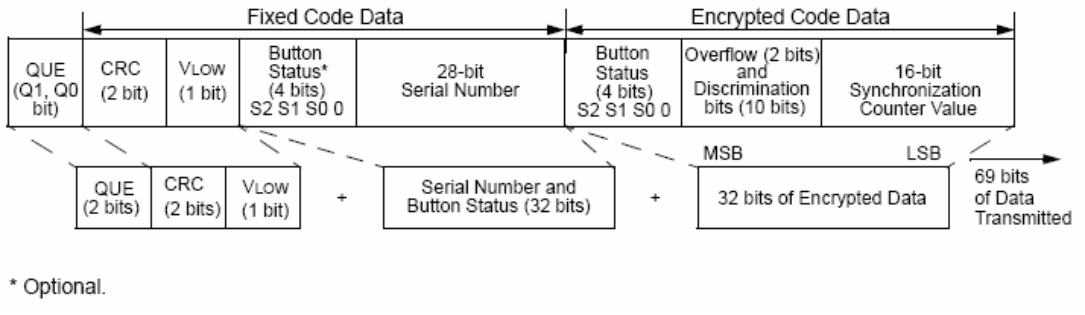

Рисунок 5. Структура слова динамічного коду

У програмі-симуляторі шифрування відбувається після натиснення кнопки „Encrypt". Йому повинен передувати вибір відповідної функції щляхом натиснення кнопки OPEN/CLOSE. Такий підхід зумовлений тим, що ця функція разом із зашифрованою частиною та серійним номером передається до віртуального буфера пульта керування для досягнення кращого представлення всього процесу.

Рисунок 6. Знімок екрана № 3 авторської програми

Розшифрування. Моделювання процесу розшифрування здійснено із використанням компатибільного з мікроелектронним засобом HCS410 дешифратора HCS500. Для того, щоб такий мікрочип міг розшифрувати отриману від передавача інформацію, повинен містити запрограмований такий самий код виробника в пам'яті ROM. Завдяки отриманому в процесі навчання зерну SEED від передавача, можна згенерувати (відповідний для нього) ключ шифрування, потрібний для розшифрування, та такий самий, як пульт керування.

Відібрана інформація містить такі дані: біти, що відповідають за розрізнення функції до виконання, біт серійного номера та зашифровану частину до вигляду динамічного коду. Передусім перевіряється серійний номер пристрою, з якого отримано рамку, з актуально записаними в пам'яті дешифратора серійними номерами. Потім, якщо серійний номер співпадає, настає розшифрування інформації. Внаслідок цього, замість динамічного коду в регістрі CSR, з'являється стан лічильника синхронізації та інша інформація від шифратора, яка після порівняння активізує функції системи.

Перебіг операцій у чергових ітераціях алгоритму розшифрування зводиться до наступного. За допомогою нелінійної функції NLF (Non-Linearp-Function) генерується один з п'яти бітів, що містяться в регістрі зсуву CSR. Цей вихід з'єднаний через функцію виключної диз'юнкції XOR з двома бітами регістра CSR і одним ключем шифрування (master key). Наприкінці кожного циклу вміст регістра ключа шифрування

в пам'яті RAM зсувається на один біт вліво, так само як і регістра CSR. Найбільш значущий біт регістра CSR відкидається, а місце найменш значущого біта регістра CSR займає результат операції XOR. Процес розшифрування вимагає 528 таких циклів взаємодії. Це означає, що лише після 528 змін у регістрі CSR з'явиться розшифрована інформація. Нелінійна функція NLF необхідна до усунення будь-якої лінійної залежності, що може з'явитися в розшифрованій інформації.

За допомогою кнопки „Send Buffer" пульта керування передається його вміст до буфера приймача. Оскільки в пам'яті приймача наявні вже дані щодо пульта керування, які отримані в процесі навчання, то можна приступити до декодування отриманої інформації. Це настає після натиснення кнопки „Decrypt", завдяки чому почергово перевіряється відібраний у буфері серійний номер, декодований зі стрибкоподібного коду стан лічильника синхронізації, який повинен бути більший від попередньо відібраного в правильній комунікації. В подальшому, якщо ці умови витримуються, реалізується відібрана функція, чому передує висвітлення повідомлення про правильний процес декодування. Після виконання функції лічильник синхронізації, який записаний у пам'яті дешифратора, збільшується на 1.

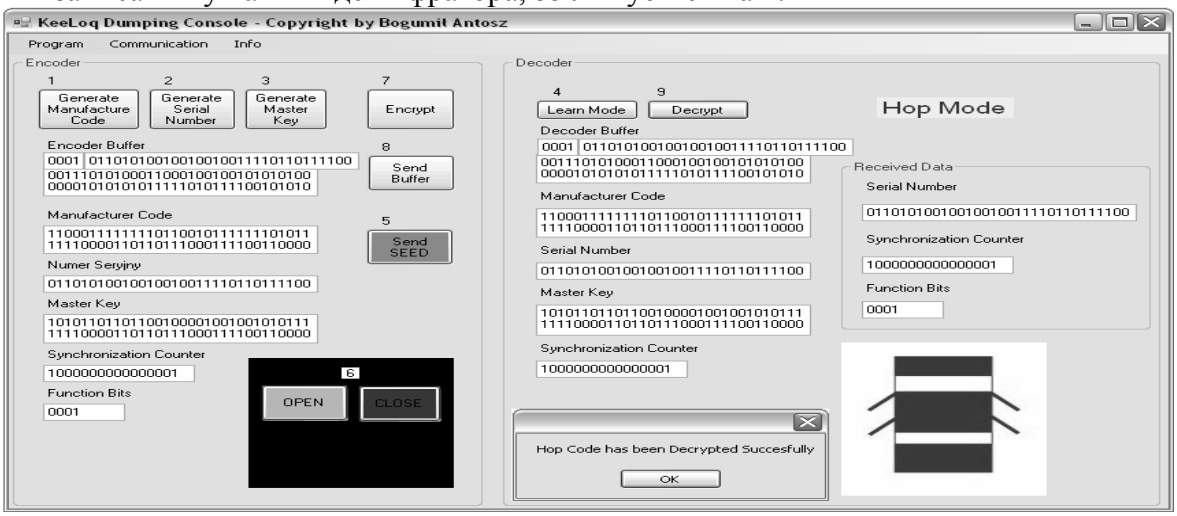

Рисунок 7. Знімок екрана № 4 авторської програми

Висновки з даної роботи і перспективи подальших досліджень у даному напрямку. Утворено підгрунтя для виконання готової діючої системи захищеного доступу. Розроблену комп'ютерну програму KeeLoq Dumping Console – при використанні комунікації з мікроконтролерем через модуль USART або порт USB – можна застосовувати для спостереження та моніторингу за черговими переприйомами (чи хопами – hop), що надаються та приймаються обговореними мікроелектронними пристроями серії HCS. Завдяки використанню програми контролю цих засобів через розміщений на прототипній платі засіб керування PIC24F, а також по'єднанню його з розробленою авторською комп'ютерною програмою, можливий детальний аналіз наступних фреймів трансляції.

Розвинена комп'ютерна програма KeeLoq Dumping Console надається оснащенню з можливістю вибору мікроелектронних пристроїв шифратора/дешифратора для самостійного визначення функції та алгоритмів, що призначені, приміром, для генерування ключів.

Завдяки проведеному за допомогою розробленої комп'ютерної програми моделюванню виявлено характерні особливості функціонування системи безпровідного передавання динамічного стрибкоподібного коду KeeLoq. Отримані результати можуть послужити дидактичним джерелом у роботах над створенням апаратно та програмно комплексної системи безпечного доступу.

Література

1. Aleman E. KEELOQ™ with AES Microcontroller-Based Code Hopping Encoder / E. Aleman, M. Stuckey // DS01265A: Microchip Technology Inc., 2009. – 12 p.
2. Bogdanov A. Cryptanalysis of the KeeLoq block cipher [Електронний ресурс] / A. Bogdanov // Cryptology ePrint Archive, Report 2007/055. – Режим доступу: http://eprint.iacr.org/
3. Courtois N. T. Algebraic and Slide Attacks on KeeLoq / N. T. Courtois, G. V. Bard, D. Wagner // Fast Software Encryption – 15th International Workshop: FSE 2008, February 10-13, 2008: Proceedings. – Lausanne, Switzerland. – Lecture Notes in Computer Science (LNCS). – Vol. 5086: Springer, 2008. – Pp. 97-115. – ISBN: 3-540-71038-8.
4. Courtois N. T. Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq / N. T. Courtois, G. V. Bard, A. Bogdanov // Tatra Mt. Mathematical Publications. – 2008. – N 41. – Pp. 167–188.
5. A Practical Attack on KeeLoq / Indesteege S., Keller N., Dunkelman O. [et al.] // The Theory and Applications of Cryptographic Techniques – Advances in Cryptology : 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2008, April 13-17, 2008: Proceedings. – Istanbul, Turkey. – LNCS. Vol. 4965: Springer, 2008. – Pp. 1–18. – ISBN 978-3-540-78966-6.
6. Microchip: AN642 [Електронний ресурс]: Code Hopping Dekoder / S. Dawson. – Режим доступу: http://www.KeeLoq.boom.ru/decryption.pdf
7. 101 SMR [Електронний ресурс]: 16-bit Microcontroller Seminar. – Режим доступу: http://www.ekiert.com/technical/16bit_seminar_2007.pdf
8. Microchip [Електронний ресурс]: 16-bit Microcontrollers and Digital Signal Controllers / Product Family / PIC24F MCU. – Режим доступу: http://www.microchip.com/ParamChartSearch/chart.aspx?branchID=8181&mid=14&lang=en&pageId=75

Отримано 30.03.2011