наземных системах радиомониторинга при многоканальном приеме / А.С. Вершинин, Е.П. Ворошилин, В.П. Денисов // Доклады ТУСУРа. – 2010. – № 2 (22), часть 2. – С. 32– 35.

4. Мархакшинов А. Л. Корреляционное измерение навигационных параметров в сейсмической системе охраны / А.Л. Мархакшинов, М.А. Райфельд, А.А. Спектор // Научный вестник НГТУ. – 2010. – № 3 (40). – С. 161– 166.

Надійшла 27.11.2012 р.
Рецензент: д.т.н. Шинкарук О.М.

УДК 004.056

В.Ю. КОРОЛЬОВ, В.В. ПОЛІНОВСЬКИЙ
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ

ТАЙМЕРНЕ КОДУВАННЯМ З ВИКОРИСТАННЯМ ПРИХОВАНОГО КАНАЛУ АВТЕНТИФІКАЦІЇ СТОРІН ДЛЯ УКРАЇНСЬКОГО КЛЮЧА-АВТЕНТИФІКАТОРА

Представлено систему автентифікації користувачів інформаційних систем на базі українського ключа-автентифікатора (УАК). Запропоновано нову таймерну систему передачі інформації з обмеженим доступом з використанням прихованого каналу автентифікації відправника.

Ключові слова: український ключ-автентифікатор, таймерне кодування, комбінаторна модель.

Presented system for authenticating users of information systems based on Ukrainian-key authenticator (UAC). A new timer system classified information transmission with the use of covert channel sender authentication is described.

Keywords: Ukrainian-key auth timer encoding combinatorial model.

Вступ. Сьогодні кіберзлочинність стала складовою загальносвітового організованого кримінального бізнесу, а у ЗМІ постійно поступають повідомлення про злам і крадіжку як корпоративних, так і персональних даних. Тому надійність комп'ютерної безпеки займає найперші позиції у переліку вимог до інформаційних систем. Суттєва кількість випадків несанкціонованого доступу пов'язана з недосконалістю систем автентифікації і протоколів передачі секретних даних. Отже, сучасні складні інформаційні і технічні системи потребують постійного вдосконалення системи автентифікації користувачів і системи передачі інформації з обмеженим доступом.

Постановка задачі. Відомі методи автентифікації мають технічні та експлуатаційні недоліки [1-4]. Більшість способів ідентифікації права доступу до об'єктів та ідентифікаторів передбачають використання постійного коду. Очевидно, що надійність таких способів умовна, особливо у випадку крадіжки та несанкціонованого копіювання або втрати користувачем ідентифікатора і тому потребують вдосконалення. Запропонована система дозволяє отримати кращі технічні і експлуатаційні показники. Ця стаття є продовженням циклу робіт [1-12] з захисту складних технічних систем і інформаційних джерел на базі таймерних методів персоналізації.

Аналіз останніх досліджень і публікацій.

Виділення раніше не вирішених частин проблеми. Як було показано у попередніх публікаціях [1– 13] відомі способи автентифікації мають наступні недоліки:

- використання невеликої кількості кодових комбінацій;
- використання двійкової системи запам'ятовування коду, що не зовсім зручно пересічному користувачеві;
- код, набраний на ідентифікаторі, досить легко зчитати (підгледіти) третіми особами будь-якими оптичними пристроями реєстрації інформації (фото, відео) під час користування ідентифікатором;
- використання багатозначних кодів (порядку 10– 14 знаків), які не просто запам'ятовувати пересічному користувачеві.

Перелічені недоліки доводиться компенсувати організаційними методами безпеки організації, що ускладнює її роботу і потребує додаткового навчання та регулярних тренувань працівників.

Формулювання цілей статті. Запропонована система дозволяє вирішити технічну задачу, яка полягає у створенні більш досконалого способу автентифікації і введення кодової інформації та створенні автентифікатора зі зчитувачем кодової інформації для здійснення цього способу.

Технічним результатом є збільшення ємності кодової інформації за рахунок зміни форми автентифікатора, збільшення кількості положень секретних елементів відносно зчитувача з одночасним збільшенням кількості видів секретних елементів, а також підвищення зручності користування автентифікатором за рахунок впровадження 10– 12-значної літерно-цифрової системи запам'ятовування коду та зменшення довжини коду до 4-8 знаків.

Визначена задача та технічний результат досягаються завдяки набиранню коду на механічному носії кодової інформації, у нашому випадку на автентифікаторі, шляхом вибіркового обертання секретних елементів з кодовими символами на визначений кут навколо осі, згідно з винаходом [13] та періодичній зміні форми автентифікатора, що є додатковою зовнішньою ознакою коду. Завдяки переліченим

особливостям нового способу автентифікації створено нові механічних носії секретного коду з кращими безпековими і експлуатаційними характеристиками та системи передачі дачі даних з захистом.

Виклад основного матеріалу

Спосіб автентифікації і введення кодової інформації

Механічний носій кодової інформації і зчитувач кодової інформації (контрольний пристрій, рідер) реалізують спосіб введення кодової інформації, що включає набір коду на автентифікаторі шляхом вибіркового обертання секретних елементів з кодовими символами на відповідний кут. Від інших способів автентифікації запропонований відрізняється тим, що користувачі додатково здійснюють періодичну зміну коду шляхом зміни форми автентифікатора згідно з регламентом безпеки.

Автентифікатор зі зчитувачем кодової інформації

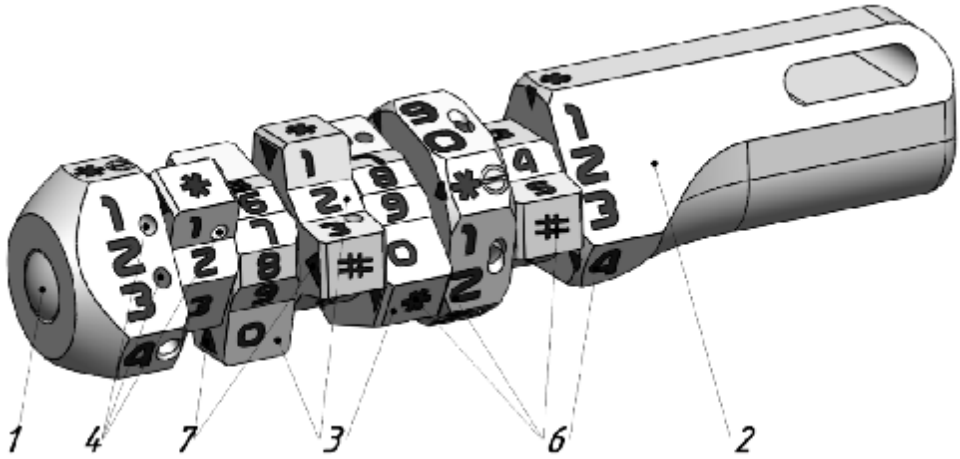


Рис. 1. Автентифікатор (УАК – Український Автентифікатор-Ключ)

На рис. 1. Наведено загальний вигляд автентифікатора. УАК містить секретні елементи з кодовими символами 3 і 6, що встановлені на осі з можливістю повороту 6, елементи взаємної фіксації 7, що розміщені на торцях (полюсах) секретних елементів. Конструктивно секретні елементи виконані у вигляді багатогранників (пластин) 3, а елементи фіксації виконані у вигляді виступів та відповідних їм отворів. При цьому кількість отворів 4 дорівнює кількості фіксованих положень секретного елемента. Кодові символи 6 нанесені з краю пластин по різні боки від стрижня і виконані у вигляді перфорацій, прорізів або виступів. Габарити пластин відповідають розмірам отвору контрольного пристрою. Торці пластин, що контактують між собою, мають елементи взаємної фіксації, а весь набір пластин підпружинений 2 уздовж осі стрижня.

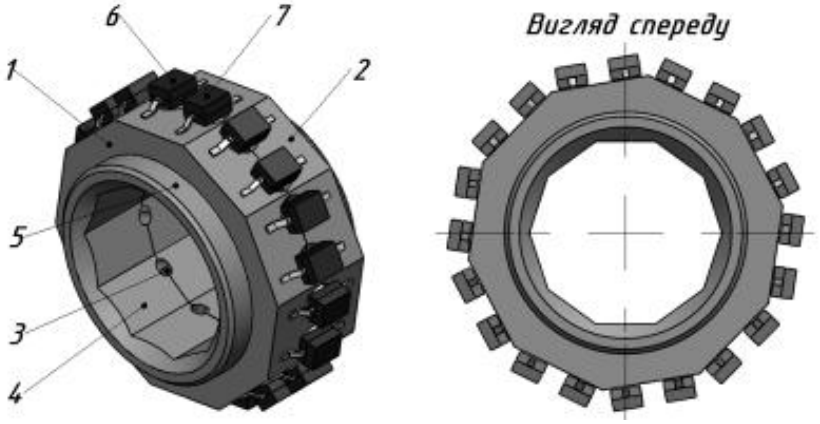


Рис. 2. Зчитувач УАК

При проходженні автентифікатора через шахту починається робота зчитувача (рис. 2). Зчитувач кодової інформації з автентифікатора містить корпус, в якому виконана шахта для проходження автентифікатора 4, і є канали 5 для проходження оптичного, акустичного або електромагнітного сигналу. В даній роботі розглянуто зчитування за допомогою оптопар. Сукупність частково або повністю закритих, відкритих випромінювачів 7 (світловий діод) при проходженні крізь них секретного елемента автентифікатора утворює певну кодову комбінацію елемента у відповідному положенні на автентифікаторі.

Множина кодових комбінацій секретних елементів автентифікатора (рис. 3) у певних положеннях утворюють вихідну кодову послідовність автентифікатора (I-XII), яку можна змінювати наприклад завдяки повороту секретних елементів 11 навколо осі автентифікатора 3. У випадку встановлення невірності коду доступ до об’єкта залишається перекритим (не відбувається) і може спрацьовувати сигналізація.

Комбінаторна модель УАК і рідера

Зчитування пластини УАК включає реєстрацію передньої форми багатогранника, кількості і просторового розташування отворів та тильної форми. Відповідно маємо, як мінімум, три групи зчитаних сигналів від оптопар, які відображають послідовність реєстрації форм багатогранної пластини та отворів у ній. Для того, щоб показати як з сигналів отримати секретний код, введемо поняття інформаційний зріз (ІЗ). ІЗ – це впорядкована інформація, яку отримують при зчитуванні форми пластини УАК або розташування і кількості отворів на гранях УКА, кількість якої дорівнює числу оптопар. Рис. 4 ілюструє відповідність між зчитаною інформацією і пластиною УАК. Видно, що мінімальна кількість інформаційних шарів для пластини дорівнює трьом, хоча може бути доповнена до будь-якої кількості, яка є експлуатаційно раціональною.

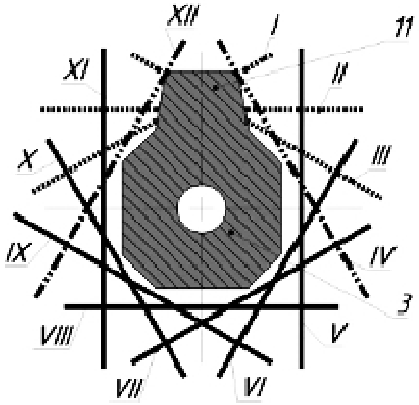


Рис. 3. Багатогранник УАК і траєкторії променів між оптопарами

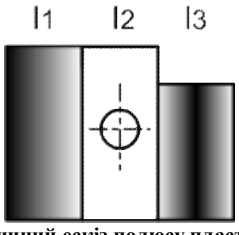


Рис. 4. Схематичний ескіз полюсу пластини УАК (вид згори). I_1, I_2, I_3 – інформаційні зрізи

Розрахуємо кількість комбінацій для форм пластини УАК (інформаційні зрізи I_1, I_3). Очевидно, що кількість комбінацій для форми визначається кількістю унікальних сигнальних відкликів від оптопар і для симетричних пластин кількість комбінацій зменшується пропорційно до числа осей симетрії у фронтальній площині. Отже, маємо формулу:

$$V_c = \left[\sum_{i=1}^{Z} G_i \times \frac{P_i}{S_i}\right]^M$$

де G_i – кількість пластин з означеним числом полюсів, P_i – кількість полюсів, S_i – кількість осей симетрії у пластини у фронтальній площині, Z – загальна кількість пластин всіх видів, M – експлуатаційна кількість пластин ключа.

Таким чином, для прикладу, УАК з 12 і 10 граней, що містить тільки однакові за конфігурацією пластини, з 8 і 14 пластинами маємо таку кількість комбінацій по визначенню форми:

$$(2*12 + 1*6 + 1*3)^{14} = 39^{14} \approx 2^{22},\ (2*12 + 1*6 + 1*3)^{8} = 39^{8} \approx 2^{13},$$
$$(2*10 + 1*5 + 1*2)^{14} = 27^{14} \approx 2^{20},\ (2*10 + 1*5 + 1*2)^{8} = 27^{8} \approx 2^{11}.$$

Виходячи з принципу роботи рідера і ключа робимо висновок, що послідовність реєстрації оптопарами отворів одного інформаційного зрізу в пластині не суттєва, а важлива тільки їх кількість і розташування на гранях. Такій постановці задачі відповідають сполучення у комбінаториці, тобто нас не цікавить порядок елементів у комбінаціях, а тільки їх склад. Скористаємось наступним означенням для сполучень: *k*-сполученнями з *n*-елементів називають всі можливі *k*-розстановки, складені з цих елементів, і які відрізняються одна від одної складом, а не порядком елементів. Отже, кількість комбінацій отворів у пластинах УАК, зареєстрованих оптопарами, визначається співвідношенням:

$$C_N^k = \frac{N!}{(N-k)!\,k!}$$

де k – кількість отворів у пластині УАК, N – загальна кількість оптопар.

Максимальна кількість комбінацій для УАК

Для ключа з M пластин кількість комбінацій визначається наступним добутком:

$$\prod_{i=1}^{M} C_N^{k_i}$$

де k_i – кількість активних пар для пластини. Відомо, функція сполучень C^k_N подібна до перевернутої параболи, симетрична і має один максимум в точці $N/2$. Тому максимальна кількість комбінацій для ключа буде в тому випадку, коли всі пластини нададуть значення $k = N/2$. При цьому максимальна кількість комбінацій для ключа з M-пластин дорівнює:

$$\left[C_N^{N/2}\right]^M = \left[\frac{N!}{\left(\frac{N}{2}!\right)^2}\right]^M$$

Мінімальну кількість комбінацій, рівну одиниці, дають вироджені конфігурації пластин – без отворів або з кількістю отворів рівною кількості оптопар. Для УАК з вироджених пластин кількість комбінацій дорівнює числу пластин – M. Експлуатаційно раціональній **мінімальній кількості комбінацій** відповідає пластина з одним отвором або пластина с кількістю отворів рівною $N - 1$. Для обох випадків кількість комбінацій для УАК з M пластин дорівнює N^M.

Розрахуємо кількість комбінацій, яку можна ввести в рідер пластинами різної форми. При введенні одної пластини у рідер кількість комбінацій відповідає сумі сполучень від всіх конфігурацій отворів для пластини. Скориставшись відомим у комбінаториці співвідношенням отримуємо:

$$C^0_N + C^1_N + C^2_N + \ldots + C^{N-1}_N + C^N_N = 2^N.$$

Методика розрахунку кількості комбінацій для ключа і рідера

З метою розрахунку кількості комбінацій кодуючу конструкцію багатогранника УАК можна розділити на форму пластини і форму з отворами. Вибір такого розділу обумовлений стадіями процесу реєстрації зміни конфігурації світлового поля всередині рідера по мірі проходження пластин УАК вздовж шахти. Дійсно, спочатку стан світлового поля змінюється тільки формою пластин (багатогранників) (етап 1), а потім, по мірі руху ключа в глиб шахти, через отвори у пластині проходять промені (етап 2). Отже, в результаті реєстрації процесу проходження пластини вздовж рідера маємо два стани для елемента УАК: затемнення променів формою, реєстрація променів, що проходять через отвори в пластині. Таким чином, при реєстрації коду з пластини УАК отримуємо одну кодову комбінацію від форми пластини-багатогранника і одну кодову комбінацію від пластини з отворами. Для варіантів конструкції пластин, що представляють собою декілька послідовних співвісних рядів з отворами в різних формах, виконаних як одна монолітна деталь (складений багатогранник), розрахунок кількості комбінацій зводиться до обчислення кількості комбінацій для кожної елементарної пластини.

Визначення кількості комбінацій для ключа і рідера

1) У конструкції складеного сегмента виділяють прості структури (елементарні багатогранники: форма пластини і пластина з отворами «перфорована пластина»). Якщо багатогранник не складений, див. п.2.

2) Для простого багатогранника ключа форма – одна група комбінацій і перфорована форма – одне сполучення комбінацій. Для рідера – форма ключа дає кількість (симетричних) поворотів, а перфорована пластина дає сполучення комбінацій.

3) Загальна кількість кодових комбінацій для ключа – це добуток всіх кодових комбінацій від перфорованих пластин і форм пластин. Оскільки форма пластини і пластина з отворами є єдиною конструкційною (збірною) одиницею – деталлю і разом вони дають незалежні кодові комбінації, відповідно, то кількість кодових комбінацій суммується, а не перемножується, як у випадку окремих ІЗ:

$$UAK = \prod_{i=1}^{M}\left(C_N^{k_i} + \frac{q_i}{2 \cdot S}\right)$$

де C^{ki}_N – кількість комбінацій, що задається отворами конкретного (встановленого) i-го сегмента, q_i – кількість поворотів сегмента з отворами, котрі дають унікальні кодові комбінації. Кількість унікальних комбінацій для форм сегментів з поперечними осями симетрії скорочується вдвічі від кількостей осей симетрії – S для полюсів форми. Загальна кількість кодових комбінацій рідера ключа (повна кількість усіх кодових станів системи) – сума всіх комбінацій для форми сегмента і сума всіх сполучень для пластин, тобто:

$$R = \left[\sum_{i=1}^{N}\left(C_N^{k_i} + \overline{q_i}\right)\right]^M = \left[2^N + \sum_{i=1}^{N}\overline{q_i}\right]^M \approx 2^{N*M}.$$

$$C^{Nstart}_N + \ldots + C^{N-1}_N + C^N_N = 2^N - (C^0_N + C^1_N + C^2_N + \ldots + C^{Nstart-1}_N)$$

$$R = \left[\sum_{i=1}^{N}\left(C_N^{k_i} + C_N^{q_i}\right)\right]^M = \left[2^{N+1} - \sum_{i=1}^{N_{Start_i}-1} C_N^{g_i}\right]^M \approx 2^{N*M}.$$

M – кількість сегментів, N – кількість оптопар, k_i – кількість променів, q_i – кількість поворотів, котрі задають незалежні комбінації для форм сегментів, C^{qi}_N – кількість комбінацій для пропущених формою променів. N_{Start} – мінімальна кількість променів, що перекриваються формою з однією особливістю, g_i – кількість променів, що перекриваються формою, причому їх менше ніж $N_{Start,}$ C^{gi}_N – кількість віртуальних комбінацій для затриманих (затемнених, перерваних, перекритих) формою променів. Зрозуміло, що кількість комбінацій, які дають отвори у пластинах значно більша від кількості комбінацій, які дають форми багатогранника. Отже, для системи **рідер-УАК** з ключем, що складається з M пластин **кількість комбінацій** становить $2^{M\times N}$. Оскільки, результат зчитування пластини описується станом 10– 12 оптопар, то довжина вихідного коду рідера у бітах дорівнює добутку кількості комбінацій на число оптопар. Зведемо отримані результати у табл. 1.

Таким чином, кількість комбінацій для УАК-системи перевищує вимоги криптографічних стандартів захисту інформації, що рекомендують довжини ключів автентифікації у 256 біт. Суттєво збільшений об’єм секретної інформації вимагає прискорення передачі, оскільки стандартні периферійні пристрої використовують низько швидкісні канали передачі даних.

Таблиця 1

Наближена до ступеня 2 кількість комбінацій та довжина коду для УАК і рідера при 10/X і 12/XII оптопарах (N) для одного (для двох введень) та для 8 і 14 пластин (M).

Кількість пластин УАК	Максимум рідера				Максимум ключа				Раціональний мінімум рідера і ключа			
	X		XII		X		XII		X		XII	
8	2^{80}	800	2^{96}	1153	2^{64}	640	2^{79}	951	2^{27}	270	2^{29}	545
	2^{160}	1600	2^{192}	2307	2^{128}	1280	2^{158}	1930	2^{53}	530	2^{57}	1089
14	2^{140}	1400	2^{168}	2218	2^{112}	1120	2^{138}	1665	2^{46}	460	2^{50}	953
	2^{280}	2800	2^{336}	4037	2^{223}	2230	2^{276}	3302	2^{93}	930	2^{100}	1906

Трійкове кодування

Як було показано вище, завдяки новій конструкції УАК і рідера кількість комбінацій було збільшено на понад 20 порядків двійкового ступеня у порівнянні з ВІК [13]. Зрозуміло, що виконані вдосконалення конструкції сегментів УАК і рідера виключають застосування найдешевших моделей контролерів, оскільки зросла технічна складність системи. Тому після зчитування кодової комбінації УАК, стиску даних і їх шифрування, пропонується використати вільні ресурси контролерів для обчислення таймерних модифікацій стандартних алгоритмів кодування з метою підвищення скритності і захищеності передачі секретних даних від рідера до персонального комп'ютера (ПК).

Одним із основних способів підвищення скритності передачі даних є зменшення часу їх пересилання. За означенням, двійковий потік даних УАК після шифрування є випадковим (у відповідності до криптографічних стандартів) і тому не може бути стиснутий алгоритмами архівації з метою скорочення часу передачі пакетів даних.

Покажемо, що трійкова система забезпечує найменшу відносну кількість цифр для представлення чисел серед позиційних арифметико-розрядних систем. Нехай потрібно відобразити усі десяткові цілі числа від 0 до N у новій системі. Позначимо основу нової позиційної системи числення через b, тоді знайдемо m – число розрядів (цифр у новій позиційній системі числення), що містяться у числі $N = 10^n - 1$.

Маємо $b^m > 10^n - 1 \geq b^{m-1}$ або $b^m \geq 10^n > b^{m-1}$

Оскільки $\lg a^p = p \lg a$,

тоді $m \lg b \geq n > (m-1) \lg b$,

Розділимо нерівності на $\lg b$ і запишемо у вигляді

$m \geq n/\lg b > m-1$,

Отже, m є першим цілим числом не меншим за $n/\lg b$.

Фізичне позиційне представлення числа, яке відображає одну цифру у розряді назвемо арифметико-розрядним імпульсом. Всього маємо $m \cdot b$ арифметико-розрядних імпульсів, тобто $b \times [\, n / \lg b + 1 \,]$. Для того, щоб знайти b – мінімальну кількість імпульсів, треба знайти мінімум функції аргументу b:

$$g(b) = \min_{b=2;\,3;\,4\ldots} b \cdot [\, n/\lg b + 1 \,] \approx b\,(n / \lg b).$$

Оскільки n – параметр, то дослідження зводиться до пошуку мінімуму функції $f(b) = b/\lg b$, аргументом якої є змінна b – нова основа позиційних арифметико-розрядних систем. Якщо число n велике, що характерно для ключів сучасної криптографії, то мінімум досягається при $b = 3$ (табл. 2), тобто трійкова позиційна система потребує найменшої кількості цифр для позначення чисел, а значить і арифметико-розрядних імпульсів.

Таблиця 2

Результати обчислень функції f (b) для різних значень аргументу b

b	*2*	*3*	*4*	*5*	*6*
f (b)	*6,64*	*6,29*	*6,64*	*7,15*	*7,71*

Наступні значення для $f(b)$ ще більші, наприклад, $f(10) = 10$. Таким чином, для розрядно-позиційних представлень чисел має місце наступне твердження. Найменше відносне число цифр на представлення досягається при $b = 3$. Видно також, що для $b = 2$ і $b = 4$ загальне число цифр не на багато більше; у цьому сенсі малі основи позиційної системи числення мають перевагу.

Розрахунки кількості кодових імпульсів, необхідних для передачі UAK-Ключа.

УАК-ключем можна вводити різне число біт (табл. 1) за одне зчитування рідером залежно від поставлених завдань безпеки технічних систем. Тому, в розрахунках будемо виходити з довжини ключа, котра забезпечує стандартизовану кількість двійкових кодових комбінацій для алгоритмів симетричного шифрування, яку вважається не можливо подолати прямим перебором, тобто рівну 2^{256}. Зрозуміло, що всі отримані висновки справедливі і для шифрованих пакетів даних.

Розрахуємо кількість позиційних розрядів 2^{256} для представлення цього числа у трійковій системі, тобто знайдемо логарифм за основою 3 від 2^{256}. Для цього скористаємося відомою формулою перетворення основи логарифмів:

$$\log_A B = \log_C B / \log_C A \qquad (1)$$

У нашому випадку необхідно знати, який показник ступеня трійки дає 2^{256}, тому скористаємося формулою (1) у вигляді:

$$\log_3 2^{256} = \log_2 2^{256} / \log_2 3 \approx 162 \text{ [імпульси]}.$$

Відносне скорочення кількості імпульсів при передачі криптографічного ключа 2^{256} дорівнює відношенню кількості двійкових розрядів (бітів) для передачі числа у двійковій системі до кількості трійкових розрядів (тритів), які потрібні для передачі числа у трійковій системі:

$\log_2 2^{256} /[\log_2 2^{256} / \log_2 3] = \log_2 3 \approx 1.5850$.

Таким чином, представлення чисел у трійковій системі дозволяє скоротити тривалість передачі коду на *58,5 %*, завдяки суттєво чому покращується скритність передачі секретної інформації.

Загальний вигляд імпульсних діаграм для трійкового кодування

Відомо, багато варіантів трійкового кодування [14], які було розроблено для різних застосувань у теорії обчислень та створення спеціалізованих комп'ютерів. Для задач скритної передачі інформації кодові імпульси мають бути мінімальної тривалості і простої прямокутної форми рис. 5.

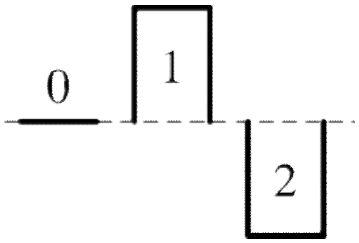


Рис. 5. Форми кодових імпульсів для трійкового кодування

Запропоноване представлення тритів аналогічне до біполярного двійкового кодування (AMI – Alternate Mark Inversion) [15,16], тому спектр (рис. 6) і характеристики завадозахищенності аналогічні до AMI-кодування.

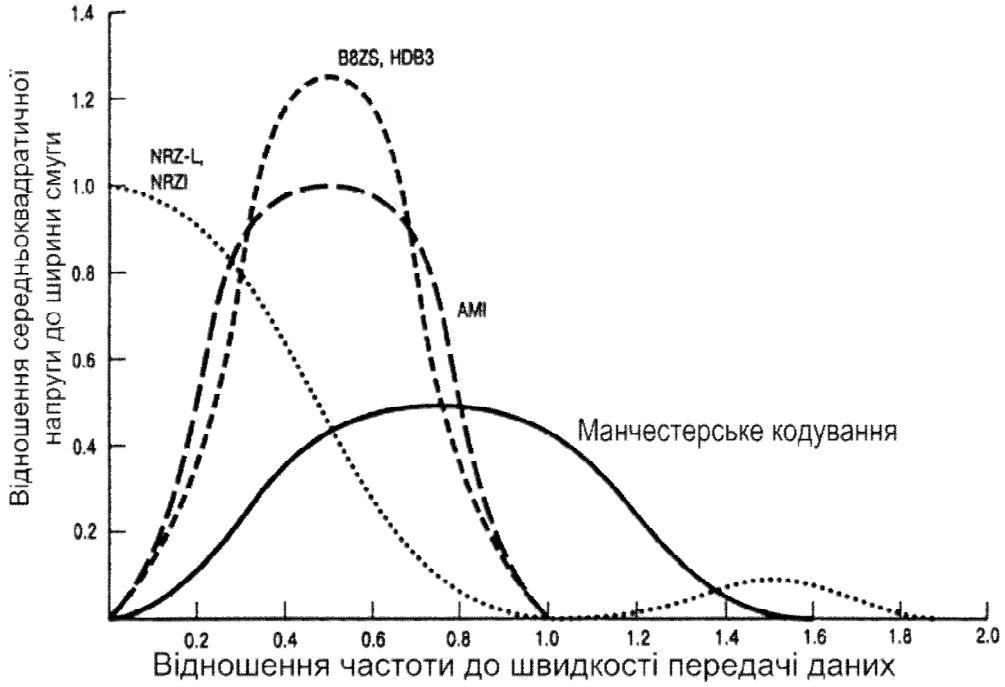


Рис. 6. Спектральна густина для схем кодування. Розшифровка позначень: B8ZS (bipolar with 8-zeros substitution) – біполярне кодування з заміщенням восьми нулів, HDB3 (high density bipolar-3 zeros) – кодування високої щільності з трьома нулями, NRZ-L – кодування без повернення до нульового рівня, NRZI – кодування без повернення до нуля з інверсією на одиницях

Порівняємо за швидкістю виникнення похибок (рис. 7) бінарне кодування (NRZ – Non Return to Zero) та біполярне кодування (AMI).

Зрозуміло, що у випадку використання трійкового кодування приймач має віднести отриманий сигнал до одного з трьох рівнів, а не до двох, як у бінарному кодуванні (NRZ). Внаслідок чого, при однаковій імовірності виникнення помилок трирівневий (трьохзначний) сигнал вимагає приблизно на 3 дБ більше потужності ніж двозначний сигнал (рис. 7). Іншими словами, при заданому відношенні сигнал-шум (С/Ш) швидкість появи помилок при бінарному кодуванні менша ніж при трійковому кодуванні, що є платою за прискорення передачі даних. Отже, застосування трійкового кодування дозволяє скоротити час передачі на *58,5 %*, але для отримання аналогічних до NRZ показників швидкості виникнення помилок амплітуду сигналу потрібно збільшити в 2 рази.

Передача коду від рідера УАК до комп'ютера здійснюється у екранованому кабелі на відстань приблизно 0,5 – 1,2 м в офісному приміщенні, а живлення контролера буде здійснюватись від USB-порта, який забезпечує напругу до 2,5 [В], тому проблем з заглушенням сигналу завадами не виникатиме. Отже, за характеристиками завадозахищенності в даних умовах експлуатації кодування NRZ не має суттєвої переваги перед AMI.

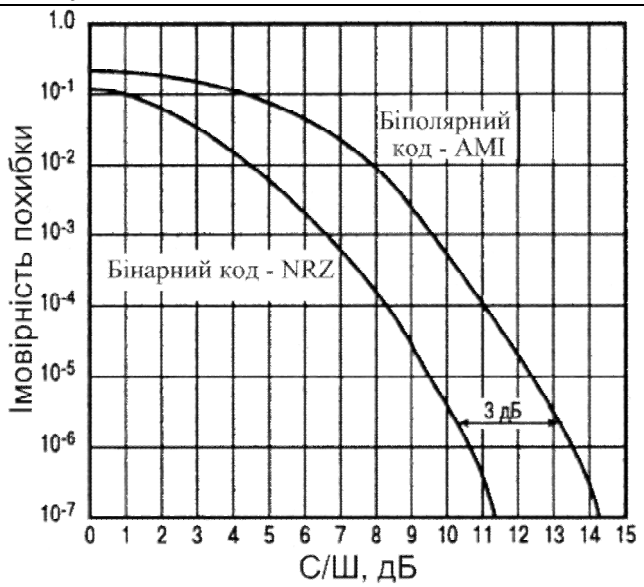


Рис. 7. Теоретична швидкість виникнення похибок при бінарному (NRZ) і біполярному кодуванні (AMI)

Таймерне кодуванням на базі трійково-двійкової передачі даних з прихованим каналом автентифікації

В даному підрозділі представлено алгоритм трійкового кодування з двійковим прихованим каналом передачі автентифікаційної інформації відправника. Оскільки, запропоноване кодування полягає у зміні тривалості сигнальних посилок, то воно є різновидом таймерного (широтно-імпульсного) кодування.

Побудова прихованого двійкового каналу передачі автентифікаційної інформації

Ідея створення таємного каналу полягає в скороченні або подовженні тривалості трійкових імпульсів по лівому і/або правому фронтам, яка відображає прихований двійковий біт у трійковому таймерному кодовому імпульсі (рис. 8). Сама автентифікація будується на стандартизованих криптографічних алгоритмах, типу SHA-256. Технічно розпізнавання вставки біта в імпульс трита на стороні приймання здійснюється за рахунок застосування прецизійних синхронізуючих генераторів і цифрових частотомірів, тактова частота яких повинна бути в 2– 4 рази вище робочої частоти передачі даних для трійкового імпульсу. Очевидно, що ширина смуги пропускання лінії передачі сигнальних посилок також збільшуються згідно до тактової частоти генератора опорної частоти.

Якщо частота генератора синхронізації вище частоти передачі тритів у два рази, один трит може нести тільки один біт. Якщо частота генератора синхронізації вище в чотири й більш раз, то один три може нести два біти. Зрозуміло, що можлива й зворотна реалізація, коли біти передають ключ, а трити – автентифікаційні дані.

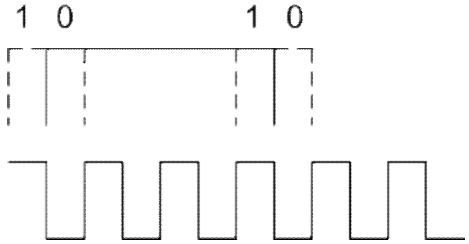


Рис. 8. Ілюстрація принципу вставки бітів в імпульси тритів

Узагальнений протокол передачі ключа в трійковій системі з прихованим каналом передачі автентифікаційних даних можна реалізувати в наступній послідовності

1) Синхронізація сторін джерела (передавача) і приймача; передача команд ініціалізації (за протоколом).

2) Перетворення ключа (симетричного або асиметричного) із двійкової системи в трійкову.

3) Розрахунки криптографічної функції хешування від ключа й ідентифікатора джерела.

4) Формування імпульсів тритів із вбудованими бітами за алгоритмом посвідчення відправника.

5) Передача від джерела до приймача даних по екранованому кабелю з лінією синхронізації.

6) Приймання даних.

7) Декодування тритів і добування автентифікаційних бітів.

Алгоритм посвідчення відправника (АПВ) ґрунтується на додаванні даних у двійковий код з метою організації прихованого каналу передачі інформації для перевірки автентичності відправника секретного коду.

Пропонуються два варіанти кодування в прихованому каналі:

а)"Триплет цілком" (ТЦ). ТЦ код дозволяє вбудувати в один таймерний імпульс три двійкові біти відразу.

б)"Бітова розрядка" (БР). БР код дозволяє вбудувати в один таймерний імпульс один двійковий біт.

Очевидно, що ТЦ має меншу скритність ніж БР, особливо коли частота таймерних імпульсів мало відрізняється від частоти генератора тактових імпульсів. Зрозуміло, що з позиції ймовірності виявлення схованого каналу передачі даних тривалість вбудованих імпульсів коду ТЦ і БР повинна бути мінімальною з можливих, щоб забезпечити максимально можливу скритність.

На рис. 9 наведені діаграми імпульсів, що пояснюють принципи їх кодування. Крім скорочення або збільшення тривалості таймерного імпульсу можливо й кодування по амплітуді.

На рис. 9 наведено діаграми для БР-кодування. Видно, що можливі чотири варіанти добавок в імпульси по лівому й правому фронтам (цифрами показано приклади додавання прихованих біт).

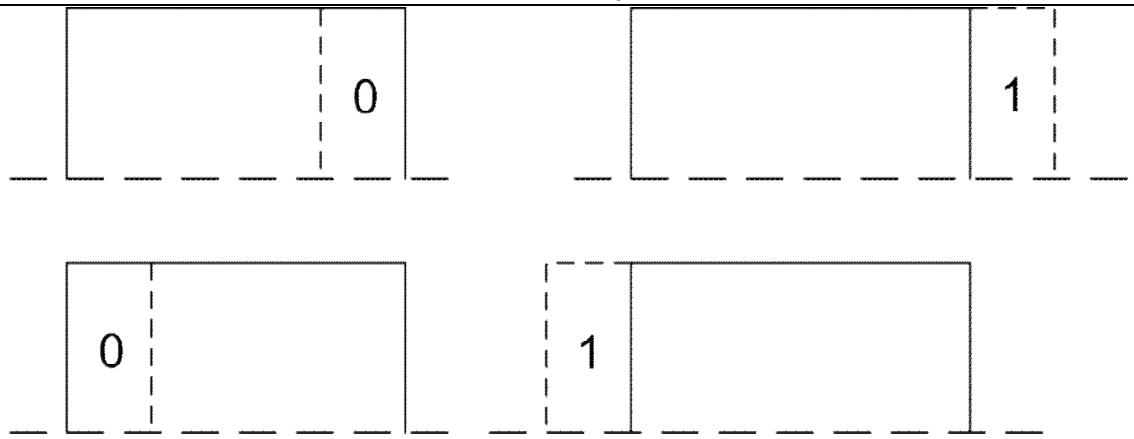


Рис. 9. Діаграми для імпульсів БР-кодування

Алгоритм кодування для таємного каналу (АКТК) представляє собою послідовне застосування генераторів випадкових чисел або вилучення значень із попередньо сформованих таблиць випадкових цифр для вибору алгоритму кодування і його параметрів. По суті, АКТК є спрощеним потоковим шифром. Передбачається, що Виконавчий контролер, завдяки використанню прецизійного генератора тактової частоти, здатний гарантовано розпізнати зміни у довгих таймерних імпульсах, на яких побудовано ТЦ або БР кодування.

Зазначимо, що АКТК може бути у подальшому вдосконалено, що дасть змогу поліпшити показники надійності й таємності для доповнення і поліпшення розробленого в Інституті кібернетики протоколу передачі інформації з підвищеним ступенем захисту передачі пакетів даних [1,11,12].

АКТК припускає циклічне виконання наступних кроків:

1) Вибір БР або ТЦ схеми кодування.

2) Запуск генератора вибору номера імпульсу, в якому будуть вбудовані біти даних.

3) Запуск генератора вибору фронту вбудовування бітів для БР або вибір трійки бітів для ТЦ.

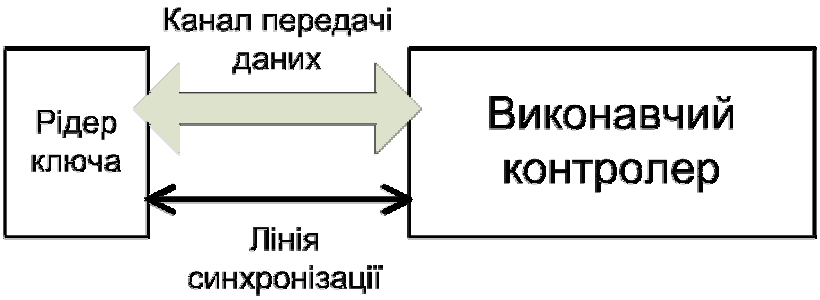


Рис. 11. Структурна схема обміну даними і синхронізації між рідером ключа й виконавчим контролером

Передбачається, що Виконавчий контролер (рис. 11), завдяки використанню прецизійного генератора тактової частоти, здатний забезпечити надійне розпізнавання зміни тривалості таймерних імпульсів, на яких побудовано ТЦ кодування. Алгоритм таємного каналу (АТК) приведено в узагальненому виді, тому нюанси ТЦ не розглядаються. Бітовий вектор даних, які засвідчують відправника (контролер зчитувача ключа), складається із частини внутрішнього секретного ключа зчитувача ключа і УАК, переданого у Виконавчий контролер. Видача імпульсів здійснюється через стандартний таймерний вихід Виконавчого контролера.

У випадку коли декілька трійковових імпульси йдуть підряд двійкові імпульси додаються або на початок, або в кінець групи, якщо цим не ускладнюється синхронізація передачі даних.

Висновки з даного дослідження

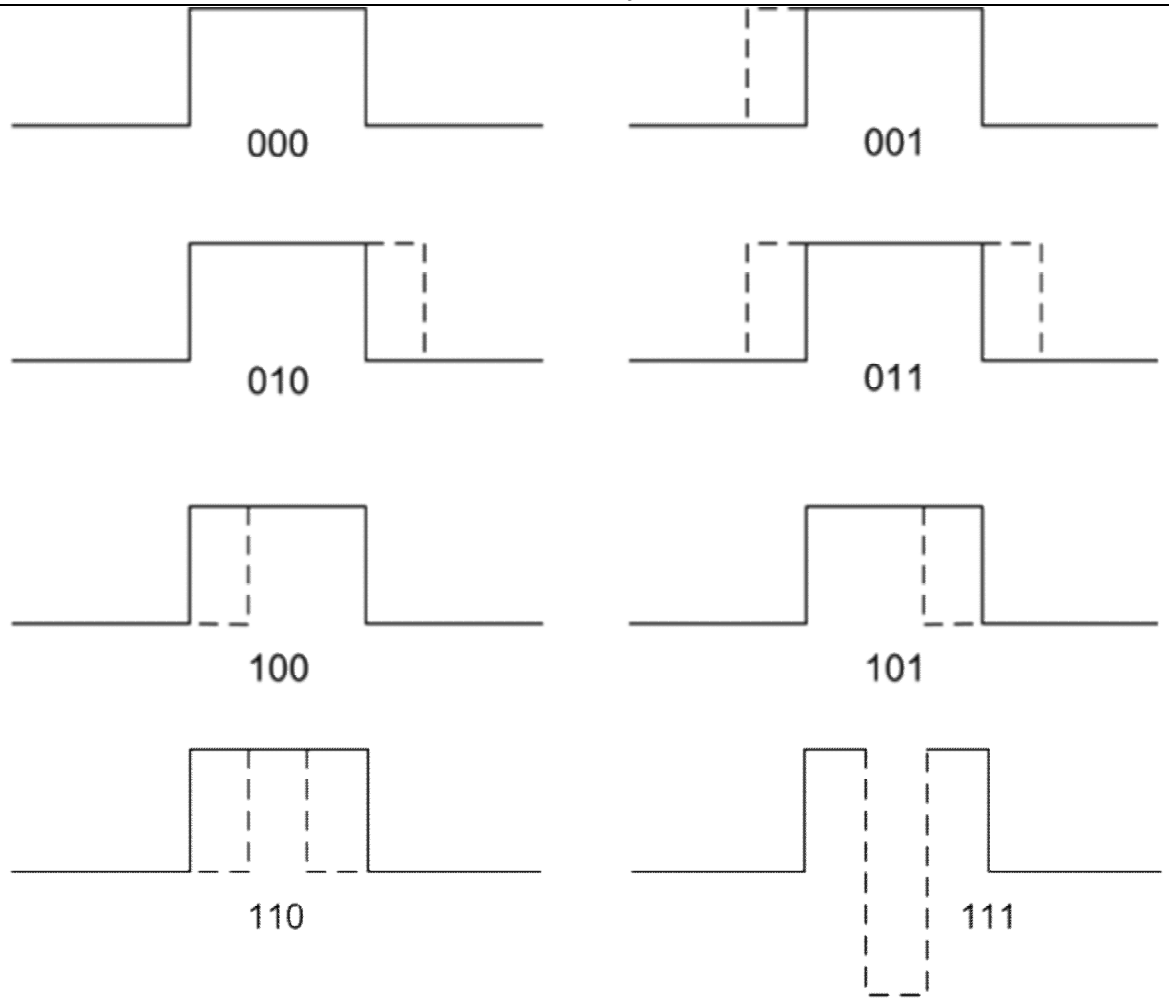
1) Запропоновано нову таймерну трійкову систему кодування з двійковим прихованим каналом автентифікації на базі AMI-кодування.

2) Показано, що нова система дозволяє прискорити передачу даних на 58,5 % причому потрібна смуга пропускання не перевищує ширину спектра для бінарних кодів типу NRZ.

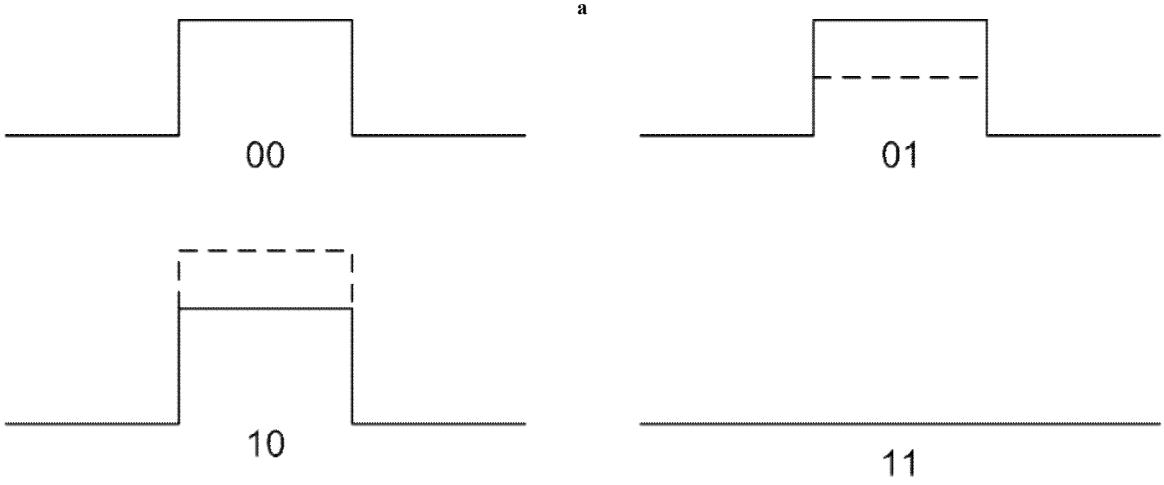
3) Аналіз завадозахищенності доводить, що запропонована система автентифікації, передачі службової та секретної інформації для комп'ютерних систем працездатна в умовах сучасних офісних приміщень.

4) Розроблено комбінаторну модель ключа автентифікатора та представлено інженерну методику обчислення кількості комбінацій для різних конфігурацій ключа.

5) Розраховані максимум і мінімуми кодової ємності ключа, а також УАК рідера доводять, що представлена система захищеної передачі інформації відповідає за кодовою ємністю сучасним криптографічним стандартам.



а



б

Рис. 10. Діаграми імпульсів для ТЦ-кодування

Література

1. Корольов В.Ю. Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним захистом інформації / Корольов В.Ю., Поліновський В.В // Математичні машини і системи. – 2009. – № 4. – С. 96 – 105.

2. Корольов В.Ю. Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень / Корольов В.Ю // Математичні машини і системи. – 2012. – № 2. – С. 60– 69.

3. Королёв В.Ю. Алгоритмизация дистанционного распознавания ВІК-кода / Корольов В.Ю // Электронное моделирование. – 2008. – № 2. – С. 19– 28.

4. Бардаченко В.Ф. Персонализация мобильных телекоммуникационных и вычислительных средств методом оптической регистрации ВІК-кода / Бардаченко В.Ф., Корольов В.Ю., Полиновский В.В., Герасименко В.А., Коновалов Д.Н // Управляющие системы и машины. – 2008. – № 2. – С. 46 – 53.

5. Королёв В.Ю. Синтез портабельных информационных сервисов для флеш-накопителей / Корольов В.Ю., Полиновский В.В // Управляющие системы и машины. – 2008. – № 6. – С. 28 – 33.

6. Корольов В.Ю. Тенденції розвитку портабельних програмних систем / Корольов В.Ю., Поліновський В.В., Герасименко В.А // Вісник Хмельницького національного університету. – 2009. – № 1. – С. 233 – 241.

7. Бардаченко В.Ф. Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа / Бардаченко В.Ф., Корольов В.Ю // Управляющие системы и машины. – 2007. – № 1. – С. 53 – 61.

8. Корольов В.Ю. Персоналізація віртуальних обчислювальних ресурсів і інформаційних джерел в сервісно-орієнтованих архітектурах / Корольов В.Ю // Вісті академії інженерних наук України. – 2007. – № 4 (34). – С. 13 – 20.

9. Корольов В.Ю. Персоналізація мобільних телекомунікаційних засобів методом дистанційного розпізнавання ВІК-коду / Корольов В.Ю., Поліновський В.В., Герасименко В.А // Вісник Вінницького політехнічного інституту. – 2007. – № 5 (74). – С. 137 – 142.

10. Корольов В.Ю. Аналіз способів вводу ВІК-коду для контролю доступу до ПК локальної мережі / Корольов В.Ю // Вісник Хмельницького національного університету. – 2007. – № 6. – С. 212 – 220.

11. Корольов В.Ю. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора / Корольов В.Ю., Поліновський В.В., Малікова О.В // Вісник Хмельницького національного університету. – 2008. – № 3. – С. 175 – 181.

12. Корольов В.Ю. Криптогенератор з використанням перетворення шумів слабострумних електронних кіл / Корольов В.Ю., Поліновський В.В // Вісник Черкаського Державного Університету. Серія технічні науки. Інформаційні технології, обчислювальна техніка і автоматика. – 2009. – № 2. – С. 14 – 18.

13. Пат. UA 89745 Україна, МПК (2009) E 05B 19/00. Спосіб автентифікації і введення кодової інформації та автентифікат зі зчитувачем кодової інформації для його здійснення / В.В. Поліновський, О.М. Ходзінський та ін. – Заявл. 06.08.2009; опубл. 25.02.2010, Бюл. № 4.

14. Троичная система счисления [Електронний ресурс]. – Режим доступу : http://ru.wikipedia.org/wiki/Троичная_система_счисления

15. Столлингс В. Компьютерные системы передачи данных / Столлингс В. – М. : Издательский дом "Вильямс", 2002. – 928 с.

16. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – М. : Издательский дом «Вильямс», 2003. – 1104 с.

Надійшла 2.11.2012 р.
Рецензент: д.т.н. Гуляницький Л.Ф.

УДК 519.6: 531.4

Ю.А. РУДЯК
ДВНЗ «Тернопільський державний медичний університет імені І.Я. Горбачевського МОЗ України»

МАТЕМАТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДУ ДИФУЗНОГО ПОВЕРХНЕВОГО РОЗСІЮВАННЯ

У роботі математично обґрунтовано експериментально-розрахунковий оптичний метод, який використовує ефект дифузного поверхневого розсіювання. Ефект базується на перерозподілі величин інтенсивностей дзеркальної та дифузних складових розсіяного поверхнею об'єкта світлового потоку при локальній зміні його кривизни. Розглянуто варіанти експериментальної реалізації методу, коли зондуюче випромінювання є поляризованим та неполяризованим. Одержано формули для розв'язання лінійних та двомірних задач механіки. Метод може бути застосований для прозорих та непрозорих об'єктів з дифузно-розсіювальною поверхнею.

Ключові слова: оптичні методи, дифузне поверхневе розсіювання, деформації, поверхні.

In this article the experimental design optical method which uses a diffuse surface scattering effect is presented and mathematically grounded. The effect is based on the redistribution of the intensity value of mirror and diffuse components of the scattered object surface flux at a local change its curvature. We examined the experimental implementation of the method, when the probe radiation is polarized and unpolarized. The formulas for the solution of linear and two-dimensional problems of mechanics are obtained. The method can be used for transparent and opaque objects with diffuse scattering surface.

Keywords: optical methods, diffuse surface scattering, deformation of the surface.

Вступ

Оптичний ефект дифузного поверхневого розсіювання зв'язує локальну малу зміну кривизни поверхні деформованого об'єкту з перерозподілом інтенсивностей дзеркальної та дифузних складових розсіяного поверхнею об'єкта світлового потоку. У роботі наведено дані, які математично описують даний ефект для лінійних та двомірних об'єктів. Також розглянуто два випадки експериментальної реалізації методу дифузного поверхневого розсіювання (МДПР), коли зондуюче випромінювання є поляризованим та