УДК 004.056

В.В. ПОЛІНОВСЬКИЙ[*], В.Ю. КОРОЛЬОВ[**]

ВІТЧИЗНЯНИЙ КЛЮЧ ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ, ОПИС, АНАЛІЗ ТА ПРОПОЗИЦІЇ ВИКОРИСТАННЯ

[*]Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна
[**]Інститут комп'ютерних технологій Університету «Україна», Київ, Україна

Анотація. *Представлено вітчизняний ключ для автентифікації користувачів, опис, аналіз та пропозиції щодо використання засобу автентифікації користувачів інформаційних систем на базі українського ключа-автентифікатора (УАК). Запропоновано нову таймерну систему передачі інформації з обмеженим доступом з прихованим каналом автентифікації відправника.*
Ключові слова: *український ключ-автентифікатор, таймерне трійкове кодування.*

Аннотация. *Представлены отечественный ключ для аутентификации пользователей, описание, анализ и предложения по использованию средства аутентификации пользователей информационных систем на базе украинского ключа-аутентификатора (УАК). Предложена новая таймерная система передачи информации с ограниченным доступом со скрытым каналом аутентификации отправителя.*
Ключевые слова: *украинский ключ-аутентификатор, таймерное троичное кодирование.*

Abstract. *The national key for users' authentication is presented. Description, analysis and suggestions for the usage of authentication of users of information systems based on the Ukrainian authentication key (UAK) are given. A new timer transmission system with limited access and buried channel of sender identity authentication is suggested.*
Keywords: *Ukrainian authentication key, triple timer coding system.*

1. Вступ

Сьогодні майже всі корпоративні та приватні інформаційні системи працюють з використанням тих чи інших засобів автентифікації користувачів, у той же час у ЗМІ постійно поступають повідомлення про злам і крадіжку як корпоративних, так і персональних даних. Тому надійність комп'ютерної безпеки у переліку вимог до інформаційних систем займає найперші позиції. Суттєва кількість випадків несанкціонованого доступу пов'язана з недосконалістю засобів автентифікації і протоколів передачі секретних даних. Отже, сучасні складні інформаційні і технічні системи потребують постійного вдосконалення засобів автентифікації користувачів з надійною системою передачі інформації з обмеженим доступом.

Аналіз існуючого стану. У 1998 р. був розроблений ключ-ідентифікатор Бардаченка (ВІК) – перший і єдиний вітчизняний механічний ідентифікатор користувача, пристрої зчитування якого можуть вбудовуватися в будь-які технічні системи, що потребують ідентифікації користувачів. На його основі було реалізовано низку серійних продуктів і товарів. Зокрема, такі:

– апаратно-програмний комплекс «Персоналізація» з використанням пристрою «Миша персоналізована» (МОП–3), яка дає можливість здійснювати дешевий та ефективний захист комп'ютерних ресурсів, розмежування прав доступу, ідентифікацію та автентифікацію користувача, захист конфіденційних даних, запобігати несанкціонованому доступу, але в той же час може працювати як стандартна миша. Використовується для роботи в операційних системах Windows 2000/XP/2003;

– рідер для ключа ВІК, розроблений під основні порти комп'ютерної техніки, і використовується для ідентифікації й автентифікації користувача та персоналізації комп'ютерної техніки шляхом зчитування кодової комбінації з ключа ВІК;

– кодовий електронно-механічний замок «Кобра», основним принципом роботи якого є таймерна електронно-кодова система. Електронний ключ замка забезпечує більш ніж 1 млрд кодових комбінацій.

За сукупністю характеристик МОП-3 та Рідер ВІК здобули звання «Товар року–2007». Отримано також позитивний експертний висновок Національного банку України на використання зазначених пристроїв персоналізації у банківських установах.

Постановка задачі. Відомі методи автентифікації мають технічні та експлуатаційні недоліки [1–8]. 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. Вище згадувалося про ключ-ідентифікатор Бардаченка (ВІК), який за аналізом [1, 5, 7] є кращим за цілу низку існуючих ідентифікаторів і дозволяє вирішити більшість задач по персоналізації комп’ютерної техніки. Але прогрес невпинний і ключового простору ключа ідентифікатора Бардаченка (2^{14} кодових комбінацій, 2^{28} – при подвійному введенні) вже недостатньо для надійної ідентифікації та автентифікації користувачів.

Дана робота є продовженням циклу статей [1–8] з захисту складних технічних систем і інформаційних джерел на базі таймерних методів персоналізації.

2. Основна частина

Запропонований вітчизняний механічний ключ-автентифікатор, ключовий простір якого складає вже не 2^{14}, як у попередника, а 2^{192} (це при використанні стандартної комплектації) або більше. За своїми характеристиками цей ключ-автентифікатор (УАК) унікальний не лише в Україні, а й в усьому світі. Слід розглянути його більш детально.

Ключ складається з об'ємних секретних елементів (рис. 1), які можуть мати будь-яку форму та містять кодові отвори, фіксатори й кодові символи, що допомагають користувачеві запам'ятати обраний код у цифро-буквеному вигляді. Все це надає змогу вручну змінювати кодову послідовність та значно полегшує процес набирання і запам'ятовування її.

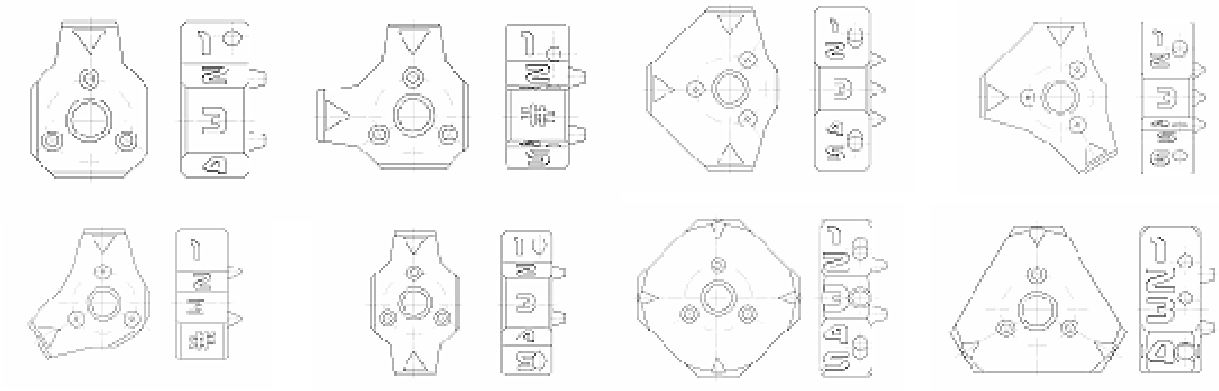

Рис. 1. Секретні елементи ключа різних форм

Така будова ключа надає низку переваг:

1. Кодові канали. На відміну від свого попередника, ключ-автентифікатор має об'ємні секретні елементи, в яких може бути кілька кодових каналів (рис. 2). За їх допомогою відбувається зчитування кодової комбінації та подальша генерація пароля.

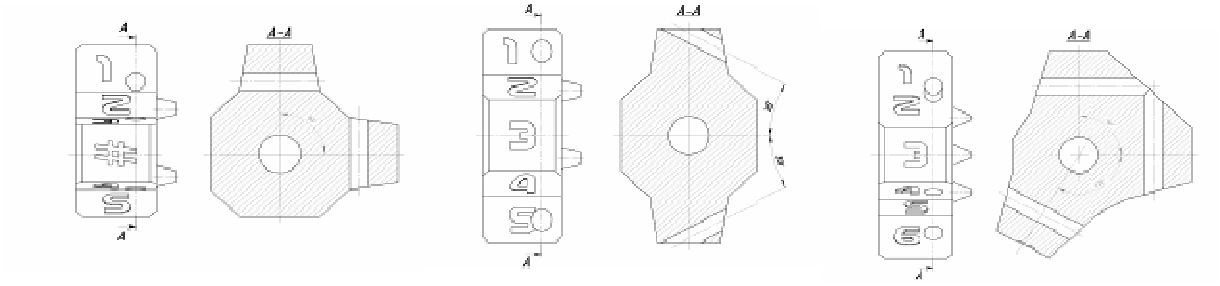

Рис. 2. Варіанти розташування кодових каналів елемента

2. Можливість перекривання певних отворів. На деяких секретних елементах є спеціальні гвинти, за допомогою яких можна перекривати певні канали (рис. 3). Завдяки цьому, значно розширюється кількість можливих кодових комбінацій.

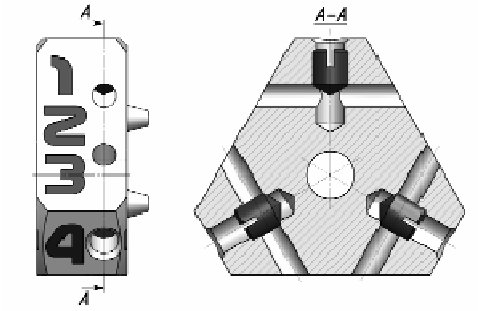

Рис. 3. Можливість перекривання каналів елемента

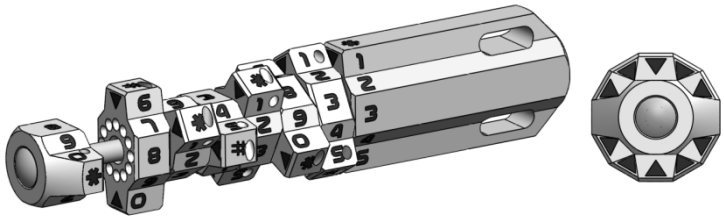

Рис. 4. Обертання секретних елементів ключа-автентифікатора навколо осі

3. Фіксатори та кодові символи. На кожному секретному елементі ключа є спеціальні виступи-фіксатори й кодові символи. Вони дозволяють фіксувати кут секретного елемента при повороті відносно інших елементів (рис. 4). На кожній грані елемента нанесені символи, що дозволяють легко запам'ятовувати положення сегмента та допомагають користувачеві безпомилково встановлювати потрібний код.

4. Різноманітність форм. Форма елементів може бути різна (рис. 5): трикутник, чотирикутник, п'ятикутник та інші багатогранники різного вигляду, навіть асиметричні.

а) б)

Рис. 5. Автентифікатор, що складається з двополюсних (а) та триполюсних (б) секретних елементів

5. Вибір кількості та форми. Користувач на власний розсуд може обирати, скільки секретних елементів міститиме ключ та в якому порядку вони будуть розташовані, якої форми будуть ці елементи, кількість та кут кодових отворів (рис. 6). Він також може самостійно обирати, чи потрібно йому перекривати кодові отвори гвинтами (формуючи, напри-

клад, довгостроковий ключ) чи ні. Відтак кожен ключ буде унікальним і матиме власний набір кодових комбінацій.

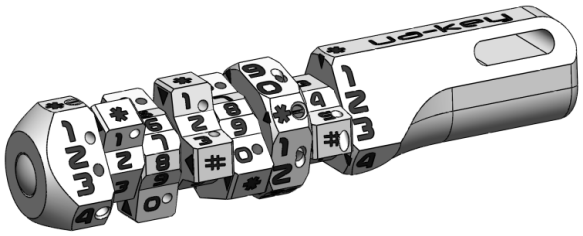

Рис. 6. Автентифікатор, що складається з різних за формою секретних елементів

6. При викраденні ключа злодій не отримає доступ до паролів користувача, оскільки тільки користувач знає правильне положення секретних елементів, а підібрати код перебиранням майже неможливо.

7. Універсальність застосування ключа. Користувач без будь-яких спеціальних пристроїв може вручну швидко змінювати загальну кількість, послідовність та положення секретних елементів. За допомогою одного ключа можна задавати безліч різних паролів та працювати з необмеженою кількістю пристроїв, що мають вбудований зчитувач кодової комбінації (миша для роботи з комп'ютером, сейф, дверний замок тощо).

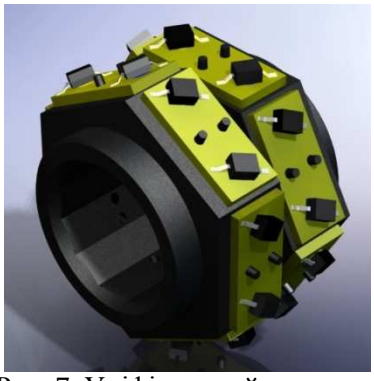

Рис. 7. Уніфікований зчитувач на 12 сегментів може зчитувати складні комбінації ключа з різним набором сегментів

8. Уніфікований зчитувач UA-Key. Нашим колективом було розроблено два унікальних пристрої зчитування (рис. 7) для всіх можливих ключів UA-Key (ключів, що мають різну довжину, сегменти неоднакової форми та типу з різними кутами розміщення секретних каналів). Конструкцію зчитувача вдосконалено, тепер зчитувач ключа-автентифікатора може складатись із довільної, мінімально необхідної кількості зчитувальних елементів, зчитувати різні види ключів-автентифікаторів, мати декілька ступенів зчитування та властивість простого монтажу.

3. Комбінаторна задача для сегмента 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. На рис. 8 проілюстровано 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 експлуатаційно раціональна.

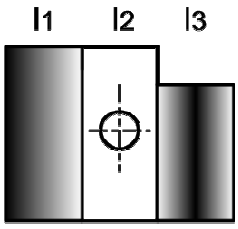

Рис. 8. Схематичний ескіз полюса пластини УАК (вид згори). I_1, I_2, I_3 – інформаційні зрізи

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 таку 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 пластині у фронтальній площині, Z – загальна кількість пластин усіх видів, M – експлуатаційна кількість пластин ключа.

Таким чином, для УАК з 12 і 10 граней, з 8 і 14 пластин маємо таку кількість комбінацій:

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

Виходячи з принципу роботи рідера і ключа, робимо висновок, що послідовність реєстрації оптопарами отворів у пластині не суттєва, а важливі 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 таким означенням для сполучень: k-сполученнями з n-елементів називають всі можливі k-розстановки, складені з цих елементів і які відрізняються одна від однієї 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.

4. Максимальна кількість комбінацій для УАК

Для ключа з M пластин кількість комбінацій визначається таким добутком:

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

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

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

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 з 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 однієї пластини у рідер кількість комбінацій відповідає сумі сполучень від усіх конфігурацій отворів для пластини. Скориставшись відомим у комбінаториці співвідношенням, отримуємо

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

Отже, у системі рідер-УАК з ключем, що складається з M пластин, довжина коду становить

$$V = \left[2^N + \sum_{i=1}^{Z} G_i \times \frac{P_i}{S_i}\right]^M \times (10 \div 12) \quad \approx 2^{N*M} \times (10 \div 12)\ [bit].$$

Зведемо отримані результати у табл. 1.

Таблиця 1. Довжина коду у бітах для УАК і рідера при 12 оптопарах для одного (для двох уведень)

Кількість пластин УАК	Максимум рідера	Максимум ключа (приблизно)	Раціональний мінімум УАК і рідера (приблизно)
8	1153 (2307)	951 (1930)	545 (1089)
14	2218 (4037)	1665 (3302)	953 (1906)

Таким чином, кількість комбінацій для УАК-системи перевищує вимоги криптографічних стандартів захисту інформації, що рекомендують довжини ключів автентифікації 128–256 біт.

5. Трійкове кодування ключів шифрування для підвищення скритності передачі секретної інформації

Як зазначено вище, завдяки новій конструкції УАК і рідера, кількість комбінацій було збільшено до близько 14 порядків двійкового ступеня у порівнянні з ВІК [1, 5, 7]. 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 з криптографічними стандартами) 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. Усього 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:

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

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 таке 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.

6. Розрахунки кількості кодових імпульсів, необхідних для передачі UAK-ключа

UAK-ключем можна вводити різне число біт (табл. 1) за одне зчитування рідером в залежності від поставлених завдань безпеки технічних систем. Тому у розрахунках будемо виходити з довжини ключа, що забезпечує стандартизовану кількість двійкових кодових комбінацій для алгоритмів симетричного шифрування, яку, вважається, неможливо 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), потрібних 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 чому суттєво покращується скритність передачі секретної інформації.

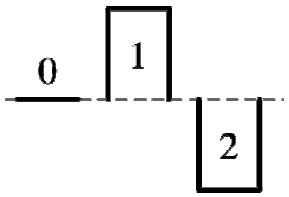

Рис. 9. Форми кодових імпульсів для трійкового кодування

Загальний вигляд імпульсних діаграм для трійкового кодування

Відомо багато варіантів трійкового кодування [9], які було розроблено для різних застосувань у теорії обчислень та створення спеціалізованих комп'ютерів. Для задач скритної передачі інформації кодові імпульси повинні бути мінімальної тривалості і простої прямокутної форми (рис. 9).

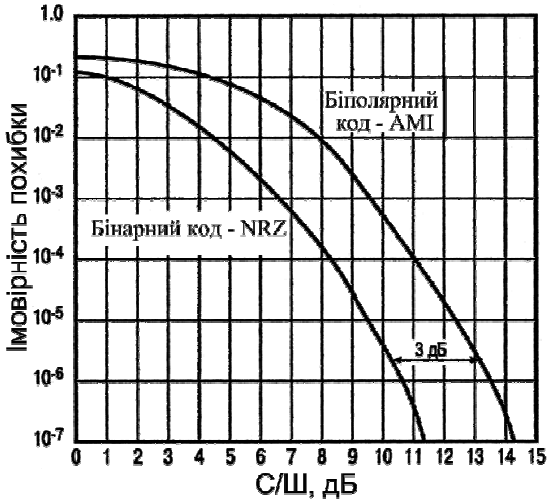

Рис. 10. Теоретична швидкість виникнення похибок при бінарному (NRZ) і біполярному кодуванні (AMI)

Запропоноване представлення тритів аналогічне до біполярного двійкового кодування (AMI – Alternate Mark Inversion) [10, 11], тому спектр і характеристики завадозахищеності згідно до AMI-кодування (рис. 10).

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

Зрозуміло, що у випадку використання трійкового кодування приймач відносить отриманий сигнал до одного з трьох рівнів, а не до двох, як у бінарному кодуванні (NRZ). Внаслідок чого, при однаковій імовірності виникнення помилок трирівневий (тризначний) сигнал (рис. 9) вимагає приблизно на 3 дБ більше потужності, ніж двозначний (рис. 10). 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 дозволило 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 в 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 завадозахищеності в даних умовах експлуатації кодування NRZ не має суттєвої переваги перед AMI.

7. Таймерне кодування на базі трійково-двійкової передачі даних з прихованим каналом автентифікації

У 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 у скороченні або подовженні тривалості трійкових імпульсів по лівому і/або правому фронтам, яка відображає прихований двійковий біт у трійковому таймерному кодовому імпульсі (рис. 11). Сама автентифікація будується на стандартизованих криптографічних алгоритмах типу SHA-256.

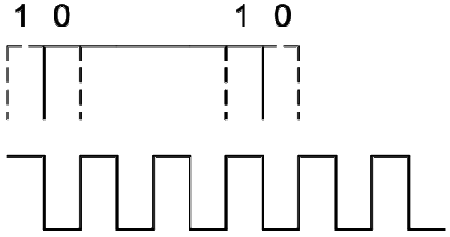

Рис. 11. Ілюстрація принципу вставки бітів в імпульси тритів

Технічно розпізнавання вставки біта в імпульс трита на стороні приймання буде здійснюватися 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 збільшується згідно з тактовою частотою 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 більше разів, то один трит може нести два біти. Зрозуміло, що можлива й зворотна реалізація, коли біти передають ключ, а трити – автентифікаційні дані.

Узагальнений протокол передачі ключа в трійковій системі з прихованим каналом передачі автентифікаційних даних

1) Синхронізація сторін джерела (передавача) і приймача; передача команд ініціалізації.
2) Перетворення ключа (симетричного або асиметричного) із двійкової системи в трійкову.
3) Розрахунки криптографічної функції хешування (SHA-256) від ключа та ідентифікатора джерела.
4) Формування імпульсів тритів із вбудованими бітами.
5) Передача від джерела до приймача даних по екранованому кабелю з лінією синхронізації.
6) Приймання даних.
7) Декодування тритів і добування автентифікаційних бітів.

Некриптографічний алгоритм посвідчення відправника (НАПВ). НАПВ ґрунтується на додаванні даних у двійковий код з метою організації прихованого каналу передачі інформації для перевірки ідентичності відправника секретного коду.

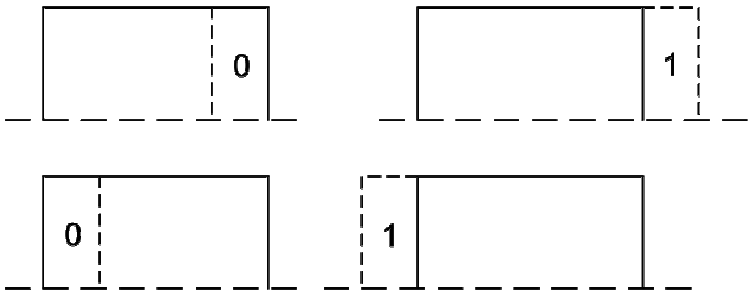

Рис. 12. Діаграми для імпульсів БР-кодування

На рис. 12 наведено діаграми для БР-кодування. Видно, що можливі чотири варіанти добавок в імпульси по лівому й правому фронтам (цифрами показано приклади додавання прихованих біт).

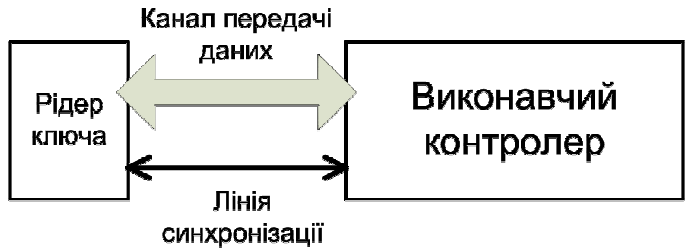

Рис. 13. Схема обміну даними і синхронізації між рідером ключа й виконавчим контролером

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

Передбачається, що виконавчий контролер (рис. 13), завдяки використанню прецизійного генератора тактової частоти, здатний забезпечити надійне розпізнавання зміни тривалості таймерних імпульсів, на яких побудовано БР-кодування. Алгоритм таємного каналу (АТК) приводиться в узагальненому виді, тому нюанси БР 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.

АТК припускає циклічне виконання таких кроків:

1) Ініціалізації протоколу обміну даними за допомогою БР-схеми кодування.
2) Запуск генератора вибору номера імпульсу, в який будуть вбудовані біти даних.
3) Вибір бітів для БР.

8. Висновки

Запропонований вітчизняний механічний ключ-автентифікатор за своїми характеристиками є досить унікальним, ефективним і в той же час універсальним пристроєм. При цьому варто зазначити, що позитивним є і той факт, що зчитування для всіх можливих ключів UA-Key, а саме ключів, що мають різну довжину, сегменти неоднакової форми та типу з різними кутами розміщення секретних каналів, можна зчитувати одним універсальним зчитувачем.

Комбінаторний аналіз вітчизняного механічного ключа-автентифікатора показує, що кількість комбінацій для УАК-системи перевищує вимоги криптографічних стандартів захисту інформації, що рекомендують довжини ключів автентифікації 128–256 біт.

Було представлено алгоритм трійкового кодування з двійковим прихованим каналом передачі автентифікаційної інформації відправника. Запропонований алгоритм дозволяє здійснити кодування ключів шифрування для підвищення скритності передачі секретної інформації.

Крім того, оскільки запропоноване кодування полягає у зміні тривалості сигнальних посилок, то воно є різновидом таймерного (широтно-імпульсного) кодування і, у свою чергу, це дозволяє збільшити швидкість передачі секретної інформації.

Все це дозволяє створювати сучасні універсальні системи автентифікації користувачів з підвищеним рівнем захисту секретної інформації.

СПИСОК ЛІТЕРАТУРИ

1. 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 / Поліновський В.В., Ходзінський О.М. та ін.; заявл. 06.08.09; опубл. 25.02.10, Бюл. №4.
2. Корольов В.Ю. Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним захистом інформації / В.Ю. Корольов, В.В. Поліновський // Математичні машини і системи. – 2009. – № 4. – С. 96 –105.
3. Корольов В.Ю. Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень / В.Ю. Корольов // Математичні машини і системи. – 2012. – № 2. – С. 60 – 69.
4. Королёв В.Ю. Алгоритмизация дистанционного распознавания ВІК-кода / В.Ю. Королёв // Электронное моделирование. – 2008. – № 2. – С. 19 – 28.
5. Персонализация мобильных телекоммуникационных и вычислительных средств методом оптической регистрации ВІК-кода / В.Ф. Бардаченко, В.Ю. Королёв, В.В. Полиновский [и др.] // Управляющие системы и машины. – 2008. – № 2. – С. 46 – 53.
6. Королёв В.Ю. Синтез портабельных информационных сервисов для флеш-накопителей / В.Ю. Королёв, В.В. Полиновский // Управляющие системы и машины. – 2008. – № 6. – С. 28 – 33.
7. Бардаченко В.Ф. Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа / В.Ф. Бардаченко, В.Ю. Королёв // Управляющие системы и машины. – 2007. – № 1. – С. 53 – 61.
8. Корольов В.Ю. Криптогенератор з використанням перетворення шумів слабострумних електронних кіл / В.Ю. Корольов, В.В. Поліновський // Вісник Черкаського державного університету. Серія технічні науки. Інформаційні технології, обчислювальна техніка і автоматика. – 2009. – № 2. – С. 14 – 18.
9. Троичная система счисления [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Троичная_система_счисления.
10. Столлингс В. Компьютерные системы передачи данных / Столлингс В. – М.: Издательский дом "Вильямс", 2002. – 928 с.
11. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

Стаття надійшла до редакції 01.11.2012