Представлено вітчизняний ключ для автентифікації користувачів, – опис, аналіз та пропозиції використання засобу автентифікації користувачів інформаційних систем на базі українського ключа-автентифікатора (УАК). Створено математичну реляційну модель системи автентифікації користувачів інформаційних систем на базі УАК. Побудовано комбінаторну модель ключа та зчитувача. Представлено загальну методику розрахунку кількості комбінацій і довжин коду. Показано, що система УАК-зчитувач дозволяє отримати довжину коду, яка відповідає криптографічним стандартам.

УДК 004.056

В.Ю. КОРОЛЬОВ, В.В. ПОЛІНОВСЬКИЙ,
О.М. ХОДЗІНСЬКИЙ

МАТЕМАТИЧНА МОДЕЛЬ УКРАЇНСЬКОГО КЛЮЧА-АВТЕНТИФІКАТОРА

Вступ. У сучасних інформаційних системах дані зберігаються і передаються в електрон-ному виді. Скорочення капітальних витрат обумовлює перехід комерційних і громадських організацій до хмарних обчислень, тобто повну або часткову відмову від власних серверних інфраструктур. Проте всі переваги використання комп'ютеризованих систем зв'язку та зберігання й розподіленої обробки даних можливі лише тоді, коли гарантується безпека доступу, зберігання та передачі інформації.

Сьогодні кіберзлочинність стала складовою загальносвітового організованого кримінального бізнесу, а до засобів масової інформації (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 й технічні системи та їх математичні моделі потребують постійного вдосконалення системи автентифікації користувачів і системи передачі інформації з обмеженим доступом.

Аналіз існуючого стану проблеми. В 1998 р. розроблено 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 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, запобігти несанкціонованому доступу, але водночас, 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 та автентифікації користувача та персоналізації комп'ютерної техніки шляхом зчитування кодової комбінації з ключа ВІК.

Постановка задачі. Відомі методи автентифікації мають технічні та експлуатаційні недоліки [1 – 9]. Більшість способів ідентифікації мають права доступу до об’єктів та ідентифікаторів, передбачаючих використання постійного коду. Очевидно, що надійність таких способів умовна, особливо у випадку крадіжки та несанкціонованого копіювання або втрати користувачем ідентифікатора й тому потребують удосконалення.

Вище згадувалося про ВІК, який за аналізом [1 – 9] є кращим за цілу низку існуючих ідентифікаторів та дозволяє вирішити більшість задач з персоналізації комп’ютерної техніки. Але прогрес невпинний, і ключового простору ВІК (2^{14} кодових комбінацій, 2^{28} – при подвійному введенні) вже недостатньо для надійної ідентифікації та автентифікації користувачів інформаційних систем та джерел. Відомий також ряд механічних аналогів за окремими показниками до запропонованої конструкції [1]. Проте їх загальним недоліком є недостатня комбінаторна ємність для використання в сучасних системах захисту інформації та автентифікації користувачів.

Запропонована система дозволяє отримати кращі технічні й експлуатаційні показники, що доводиться математичним моделюванням. Ця стаття є продовженням циклу робіт [1 – 9] із захисту складних технічних систем й інформаційних джерел на базі таймерних методів персоналізації.

Виділення раніше не вирішених частин проблеми. Як показано в попередніх публікаціях [1 – 9] 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 та ціль роботи. Запропонована система дозволяє вирішити технічну задачу, яка полягає у створенні більш досконалого способу автентифікації та введення кодової інформації і 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 щодо зчитувача з одночасним збільшенням кількості видів секретних елементів, а також підвищення зручності користування автентифікатором за рахунок впровадження 10-ти – 12-ти 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 [1] та періодичній зміні форми автентифікатора, що є додатковою зовнішньою ознакою коду. Завдяки переліченим особливостям нового способу автентифікації створено нові механічні носії секретного коду з кращими безпековими й експлуатаційними характеристиками та системи передачі даних з захистом.

Спосіб автентифікації і введення кодової інформації. Механічний носій кодової інформації та 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 до регламенту безпеки.

УАК – це механічний носій кодової інформації, який використовується разом зі зчитувачами цієї інформації та представляє собою спосіб ідентифікації й автентифікації для пристроїв, за допомогою яких визначається право доступу до будь-яких об’єктів і систем.

До таких способів і пристроїв висуваються наступні вимоги: надійний захист об’єктів від несанкціонованого доступу; надійність і простота конструкції; надійний і простий спосіб застосування, зрозумілий звичайному користувачу будь-якого віку та будь-якого рівня підготовки.

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 УАК унікальний не лише в Україні, а й за її межами. Розглянемо його більш детально.

Ключ складається з об'ємних секретних елементів (рис. 1), які можуть мати будь-яку форму й містять кодові отвори, фіксатори та кодові символи, що допомагають користувачеві запам'ятати обраний код у цифро-буквенному (символьному) вигляді. Весь набір пластин підпружинено вздовж осі стрижня. Все це надає змогу вручну змінювати кодову послідовність та значно полегшує процес набирання та запам'ятовування її. Крім того, така різноманітність форм дозволяє збільшити на порядки кількість комбінацій ключа.

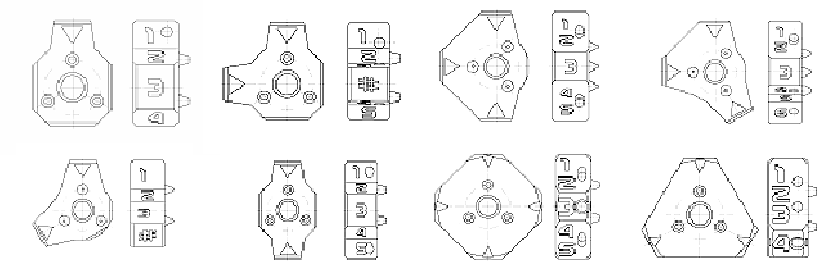


РИС. 1. Секретні елементи ключа різних форм

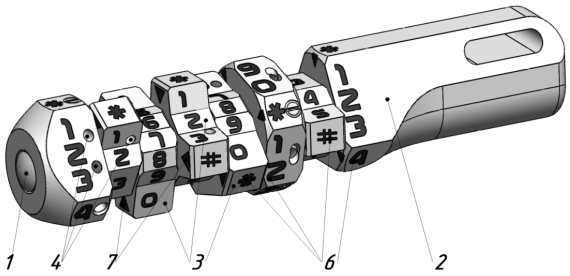


РИС. 2. Автентифікатор (УАК)

На рис. 2 показано 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 з різних сторін від стрижня та 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 підпружнений 2 уздовж осі стрижня.

При проходженні автентифікатора через шахту починається робота зчитувача (рис. 3). 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. 4) 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.

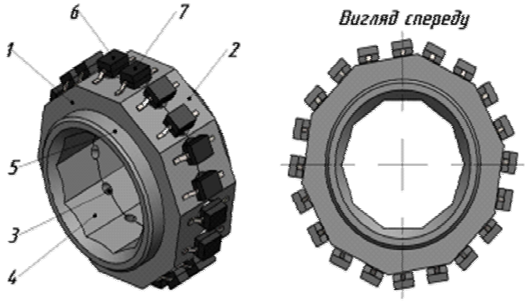


РИС. 3. Зчитувач УАК

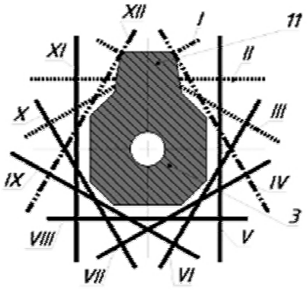


РИС. 4. Багатогранник УАК і траєкторії променів між оптопарами

Зрозуміло, що процес реєстрації конфігурації УАК можна представити як декартовий добуток [10 – 12]: $K = A \times C$, де A – множина лексиграфічно впорядкованих номерів оптопар; C – множина конфігурацій УАК; K – впорядкована сукупність (кортеж) освітлених і затемнених оптопар приймачів, які визначають вихідну кодову комбінацію.

Введемо поняття алгебраїчної моделі (реляційної моделі [10]) УАК M_A. Моделлю $M_A = \langle A; \pi \rangle$ називають систему [10], що складається з множини A та визначеній на даній множині сукупності предикатів π. Множина A складається з лексикографічно впорядкованих номерів оптопар зчитувача УАК. Елементами множини π є впорядковані сукупності логічних функцій, що відповідають результату зчитування конфігурації пластини променями оптопар. Кожна впорядкована сукупність логічних функцій відповідає результату реєстрації зчитувачем взаємодії променів з конфігурацією окремого інформаційного шару пластини УАК та її кута повороту (вихідними даними якого є кодові комбінації УАК).

Очевидно, що моделлю УАК буде об'єднання моделей конфігурацій пластин:

$$M_{UAK} = U^{N}_{i=1} M_{Ai},$$

де N – кількість кодуючих конфігурацій, M_{Ai} – відповідні їм моделі.

Для конструкції пластини, яка не передбачає зміну довжини хвилі, відбиття, розщеплення променів на сусідні оптопари логічні функції представляють собою впорядкований набір булевих операцій «І», в інших випадках логічні функції будуть складатись з операцій «І» та «АБО».

Отже, аналіз системи УАК-зчитувач зводиться до моделювання відкликів впорядкованої сукупності булевих функцій.

Комбінаторна модель УАК і рідера. Кожна пластина УАК у загальному випадку представляє собою багатогранник (складену прямокутну призму). Зчитування пластини УАК включає реєстрацію основи багатокутника (переднього краю форми багатогранника); кількості й 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. Дві групи фіксують основу (передній і тильний край) багато-

гранника й одна група просторове розташування отворів. Для того, щоб описати процес отримання секретного коду при послідовній зміні відгуків від оптопар під час просування багатогранника вздовж шахти введемо поняття інформаційного зрізу (ІЗ). ІЗ – це впорядкована інформація, яку отримують при зчитуванні форми пластини УАК або розташування та кількості отворів на його гранях. Кількість інформації якою описується стан реєстрації дорівнює числу оптопар. Рис. 5 показує відповідність між зчитаною інформацією та пластиною УАК. Видно, що мінімальна кількість інформаційних шарів для пластини дорівнює трьом, хоча може бути доповнена до будь-якої кількості, яка є експлуатаційно раціональною.

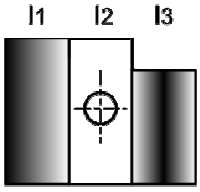


РИС. 5. Схематичний ескіз полюса пластини УАК (вид згори). I_1, I_2, I_3 – інформаційні зрізи

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 симетричних полюсів щодо центра. 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 в фронтальній площині; Z – загальна кількість пластин всіх видів; M – експлуатаційна кількість пластин ключа.

Загальна кількість варіантів виконання пластини визначається числом варіантів розбиття основи складеної призми (опуклого 10-ти або 12-ти кутника) на геометричні фігури (опуклі або вогнуті багатокутники), які можна вписати у зчитувач (табл. 1). Зрозуміло, що така задача вимагає окремої формалізації і декомпозиції, тому наведемо оцінку знизу кількості вписаних трикутників у багатокутник та наведемо далі розв'язок однієї з підзадач. Кількість розбиттів опуклого (n+2)-кутника на трикутники не перетинаючими діагоналями складає [11]:

$$K_n = 1/(n+1) \times C^n_{2n},$$

де n – кількість вершин, K_n – числа Каталана. Для 10-ти і 12-ти кутників маємо: $K_{10} = 16796 \approx 2^{14}$, $K_{12} = 208012 \approx 2^{18}$.

ТАБЛИЦЯ 1. Кількість комбінацій для форм УАК пластин (показник ступеня 2)

Кількість пластин	Кількість граней зчитувача	
	X	XII
8	560	672
14	980	1176

Розв'язування комбінаторних задач з використанням чисел Каталана. Задано натуральне число n і опуклий багатокутник з n+2 вершинами. Скільки існує способів розбити цей багатокутник хордами, що не перетинаються, якщо сам багатокутник вважати одним з варіантів розбиття?

Позначимо кількість способів M_n та підрахуємо їх для невеликих n, просто перебираючи всі можливі розбиття (рис. 6 та 7).

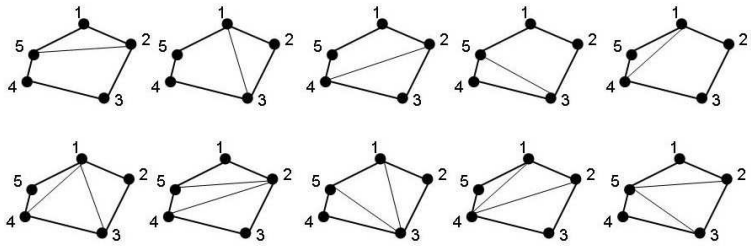


РИС. 6. Варіанти розбиття опуклого 5-кутника на опуклі багатокутники

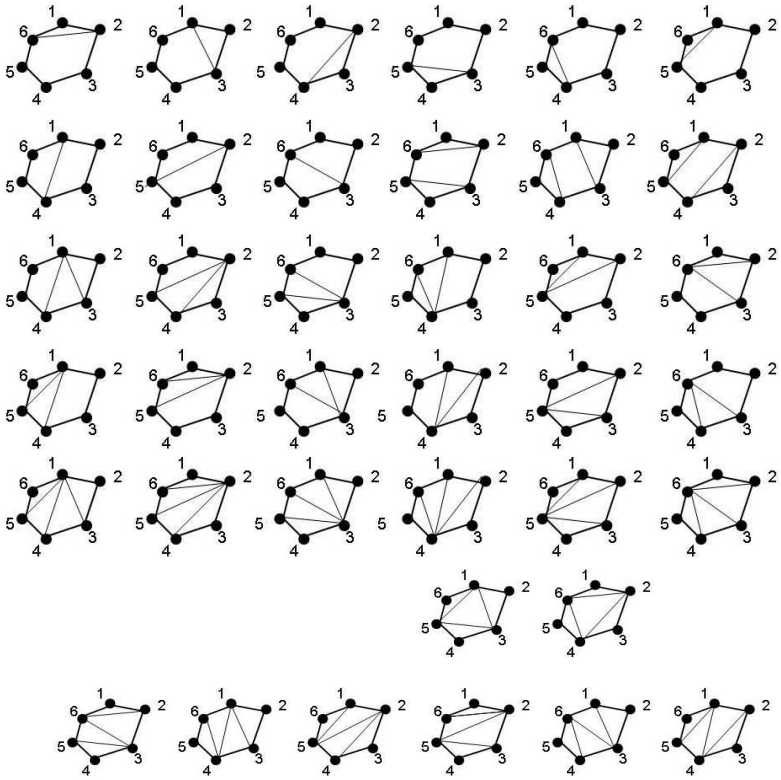


РИС. 7. Варіанти розбиття опуклого 6-кутника на опуклі багатокутники

Розглянемо деякий $(n+2)$-кутник (рис. 8). Нехай k є найменшим номером вершини, з якою з'єднано вершину 1. Дослідження розіб'ємо на три випадки, в залежності від k: а) $k = 1$; б) $1 < k < n$; $k = n$. Ілюстрації будемо малювати для 5-кутника, тому що для трикутника ($n=1$) та чотирикутника ($n = 2$) немає такого k, щоб виконувалась нерівність $1 < k < n$.

а) $\underline{k = 1}$.

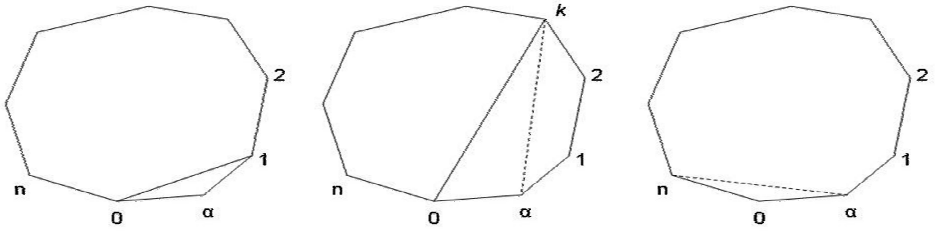
У цьому випадку зліва від хорди розташований (n+1)-кутник, який має M_{n-1} розбиттів, а справа трикутник, який дає $M_1 = 1$ розбиття. Всього для цього випадку виходить $M_{n-1}M_1$ розбиттів.

б) $\underline{1 < k < n}$.

У цьому випадку зліва від хорди розташований ($n - k + 2$)-кутник, який має M_{n-k} розбиттів, а справа треба розглянути два підвипадки. В першому підвипадку є хорда $k\alpha$, а в другому її немає. Якщо хорда $k\alpha$ є, то справа від неї розташований (k+1)-кутник, який має M_{k-1} розбиттів. Якщо хорди $k\alpha$ немає, (k + 2)-кутник $0\alpha12\ldots k0$ має стільки ж розбиттів, що й попередній, тому що в ньому відсутні хорди з вершини 0. Отже, для кожного k маємо $2M_{n-k}M_{k-1}$ розбиттів, а для всіх $1 < k < n$ маємо їх суму: $2\sum_{k=2}^{n-1} M_{n-k}M_{k-1}$.

в) $\underline{k = n}$. Цей випадок стає схожим на попередній, тобто дає два однакових за кількістю підвипадки: коли хорду $k\alpha$ проведено і коли ні. Тобто в цьому випадку маємо $2M_{n-1}M_1 = 2M_{n-1}$ розбиттів.

Додаючи кількість розбиттів у всіх випадках, отримуємо $M_n = 3M_{n-1} + 2\sum_{k=2}^{n-1} M_{n-k}M_{k-1}$.



а – $k = 1$ б – $1 < k < n$ в – $k = n$

РИС. 8. Варіанти розбиття (n+2)-кутника на опуклі багатокутники

З точки зору комбінаторики [11] задачу пошуку максимуму комбінацій на сітці променів можна подати як розміщення (розстановки), перестановки або сполучення груп з k-предметів з n. Вибір комбінаторної моделі визначається процесом зчитування та конструкції пластин ключа. Максимально можлива кількість комбінацій визначається n-розстановками з n різних предметів і для 12-ти оптопар складає: $n^n = 12^{12} \approx 2^{43}$. На сьогодні реалізовано спосіб реєстрації отворів і форм основи пластини без урахування порядку їх зчитування, що описується сумою сполучень. Напрямком подальшого розвитку є створення нової конфігурації ключа та зчитувача, що дозволить враховувати порядок взаємодії променів з конфігурацією ключа. Така модель роботи системи ключ-зчитувач описуватиметься перестановками, і оскільки $A_n^k = n!C_n^k$, то кількість комбінацій зросте в n! раз. Для 12-ти оптопар кількість комбінацій збільшиться приблизно у 10^{20} разів, тобто приблизно до 2^{41} для однієї пластини.

Розрахунок кількості комбінацій для отворів у пластинах УАК. Виходячи з принципу роботи рідера та 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 у 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 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 одної пластини у рідер кількість комбінацій відповідає сумі сполучень від всіх конфігурацій отворів для пластини. Скориставшись відомим у комбінаториці співвідношенням отримуємо:

$$C_N^0 + C_N^1 + C_N^2 + \ldots + C_N^{N-1} + C_N^N = 2^N.$$

Методика розрахунку кількості комбінацій для ключа та рідера. З метою розрахунку кількості комбінацій кодуючу конструкцію багатогранника УАК можна розділити на форму пластини і форму з отворами (кодові канали). Вибір такого розділу обумовлений стадіями процесу реєстрації зміни конфігурації світлового поля всередині зчитувача за мірою проходження пластин УАК вздовж шахти. Дійсно, спочатку стан світлового поля змінюється тільки формою пластин (багатогранників) (етап 1 – інформаційний зріз I_1), а потім, за мірою руху ключа в глиб шахти, через отвори у пластині проходять промені (етап 2 –

інформаційний зріз I_2) і, на завершення процесу, реєструється інформаційний зріз I_3, що відповідає тилу форми. На сьогодні конфігурація пластин ключа така, що $I_1 = I_3$. Тому внаслідок реєстрації процесу проходження пластини вздовж зчитувача УАК маємо два стани для його пластини: затемнення променів формою і реєстрація променів, що проходять наскрізь отвори у пластині. Отже, внаслідок реєстрації процесу проходження пластини вздовж рідера маємо два стани для елемента УАК: затемнення променів формою багатогранника та реєстрація променів, що проходять через отвори в пластині. Таким чином, при реєстрації коду з пластини УАК отримуємо одну кодову комбінацію від форми пластини багатогранника й одну кодову комбінацію від пластини з отворами. Для зчитувача – форма ключа дає кількість (симетричних) поворотів, а перфорована пластина дає сполучення комбінацій. Оскільки, це два різних класи комбінацій і кожна комбінація входить лише в один клас, то загальна кількість комбінацій для пластини підкоряється (підпорядковується) правилу суми комбінацій: «якщо деякий об'єкт *A* можна вибрати *m* способами, а другий об'єкт *B* можна вибрати *m* способами, то вибір або *A*, або *B* можна здійснити *m*+*n* способами».

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 (табл. 2).

ТАБЛИЦЯ 2. Кількість комбінацій для пластин УАК різної конфігурації (за формою)

Кількість						
Симетричних полюсів	4	3	–	1	–	2
Комбінацій	3	4	12	12	12	6

Отже, для системи **зчитувач-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. 3, де наведено наближену до ступеня 2 кількість комбінацій і довжин коду для УАК і зчитувача при оптопарах (N) для одного (для двох введень) і для 8 і 14 пластин (M).

ТАБЛИЦЯ 3. Кількість комбінацій та довжина коду для УАК і зчитувача

Кількість пластин УАК	Максимум рідера		Максимум ключа		Раціональний мінімум рідера і ключа	
8	2^{96}	1153	2^{79}	951	2^{29}	545
	2^{192}	2307	2^{158}	1930	2^{57}	1089
14	2^{168}	2218	2^{138}	1665	2^{50}	953
	2^{336}	4037	2^{276}	3302	2^{100}	1906

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

Висновки. Запропонований вітчизняний механічний ключ-автентифікатор за своїми характеристиками досить унікальний, ефективний і водночас універсальний пристрій. 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.

Запропонована комбінаторна модель дозволяє будувати різні системи персоналізації і захисту інформації з обмеженим доступом технічних систем у залежності від поставлених задач та вартості експлуатації.

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

2. 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.

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

Напрямком подальшого розвитку є створення нової конструкції ключа і зчитувача, що дозволяють враховувати порядок взаємодії променів з конфігурацією ключа. Така модель роботи системи ключ-зчитувач дозволить збільшити кількість комбінацій приблизно в 10^{20} разів.

В.Ю. Королёв, В.В. Полиновский, А.Н. Ходзинский

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ УКРАИНСКОГО КЛЮЧА-АУТЕНТИФИКАТОРА

Представлен отечественный ключ для аутентификации пользователей, – описание, анализ и предложения по использованию средства аутентикации пользователей информационных систем на базе УАК. Разработана математическая реляционная модель системы аутентификации пользователей информационных систем на базе УАК. Построена комбинаторная модель ключа и считывателя. Показано, что система УАК-считыватель позволяет получить длину кода, соответствующую криптографическим стандартам.

V.Yu. Korolyov, V.V. Polinovskiy, O.N. Khodzinskyi

THE MATHEMATICAL MODEL OF THE UKRANIAN-KEY AUTHENTICATOR

The national key for authentication is presented. A description, analysis and proposals for the use of the authentication of users of information systems based on the Ukrainian-key Authenticator (UAC) are given. The mathematical logical model of the users authentication system for information systems based on Ukrainian-key authenticator (UAC) is discussed. Constructions of the combinatorial model key and reader are discussed. It was shown, that the system UAK-reader gives the code length corresponding to cryptographic standards.

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 / В.В. Поліновський, О.М. Ходзінський,Т.Г. Нипорка // Заявл. 06.08.2009; опубл. 25.02.2010, Бюл. № 4.
2. *Корольов В.Ю., Поліновський В.В.* Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним захистом інформації // Математичні машини і системи. – 2009. – № 4. – С. 96 – 105.
3. *Корольов В.Ю.* Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень // Там само. – 2012. – № 2. – С. 60 – 69.
4. *Королёв В.Ю.* Алгоритмизация дистанционного распознавания ВІК-кода // Электронное моделирование. – 2008. – № 2. – С. 19 – 28.
5. *Бардаченко В.Ф., Корольов В.Ю., Полиновский В.В. и др.* Персонализация мобильных телекоммуникационных и вычислительных средств методом оптической регистрации ВІК-кода // Управляющие системы и машины. – 2008. – № 2. – С. 46 – 53.
6. *Бардаченко В.Ф., Корольов В.Ю.* Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа // Там же. – 2007. – № 1. – С. 53 – 61.
7. *Корольов В.Ю., Поліновський В.В., Герасименко В.А.* Персоналізація мобільних телекомунікаційних засобів методом дистанційного розпізнавання ВІК-коду // Вісник Вінницького політехнічного інституту. – 2007. – № 5 (74).– С. 137 – 142.
8. *Корольов В.Ю.* Аналіз способів вводу ВІК-коду для контролю доступу до ПК локальної мережі // Вісник Хмельницького національного університету. – 2007. – № 6. – С. 212 – 220.
9. *Корольов В.Ю., Поліновський В.В., Малікова О.В.* Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора // Там само. – 2008. – № 3. – С. 175 – 181.
10. *Глушков В.М., Цейтлин Г.Е., Ющенко Е.Л.* Алгебра. Языки. Программирование. – Киев: Наук. думка, 1978. – 320 с.
11. *Андерсон Дж.* Дискретная математика и комбинаторика. – Киев: Издательский дом «Вильямс», 2004. – С. 958.
12. *Кривий С.Л.* Дискретна математика: Вибрані питання. Навч. посіб. для студ. вищ. навч. закл. – К.: Вид. дім. «Києво-Могилянська академія», 2007. – 572 с.

Одержано 11.03.2013

Про авторів:

Корольов В'ячеслав Юрійович,
кандидат технічних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України,
E-mail: korolyov@i.ua

Поліновський В'ячеслав Васильович,
кандидат технічних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України,
E-mail: V.Polinovskyi@tau-systems.org.ua

Ходзінський Олександр Миколайович,
кандидат фізико-математичних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України.
E-mail: okhodz@gmail.com