



УКРАЇНА

(19) UA (11) 89745 (13) C2

(51) МПК (2009)

E05B 19/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ АВТЕНТИФІКАЦІЇ І ВВЕДЕННЯ КОДОВОЇ ІНФОРМАЦІЇ ТА АВТЕНТИФІКАТОР ЗІ ЗЧИТУВАЧЕМ КОДОВОЇ ІНФОРМАЦІЇ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

1

2

(21) а200908295

(22) 06.08.2009

(24) 25.02.2010

(46) 25.02.2010, Бюл.№ 4, 2010 р.

(72) ПОЛІНОВСЬКИЙ ВЯЧЕСЛАВ ВАСИЛЬОВИЧ,
НИПОРКА ТАРАС МИКОЛАЙОВИЧ, ХОДЗІНСЬКИЙ
ОЛЕКСАНДР МИКОЛАЙОВИЧ, УСАТЕНКО
ОЛЕКСАНДР ВАСИЛЬОВИЧ

(73) ПОЛІНОВСЬКИЙ ВЯЧЕСЛАВ ВАСИЛЬОВИЧ

(56) UA 54597 C2, 17.03.2003

WO 96/08793 A2, 21.03.1996

RU 2057876 C16, 10.04.1996

UA 85 U, 31.10.1997

US 4899038, 06.02.1990

(57) 1. Спосіб автентифікації і введення кодової інформації, що включає набір коду на автентифікаторі шляхом вибіркового обертання секретних елементів з кодовими символами на відповідний кут, який відрізняється тим, що додатково здійснюють періодичну зміну коду шляхом зміни форми автентифікатора.

2. Спосіб за п. 1, який відрізняється тим, що зміну форми автентифікатора здійснюють поворотом секретного елемента на певний кут і фіксацією його у цьому положенні або заміною щонайменше одного секретного елемента на інший.

3. Спосіб за п. 1, який відрізняється тим, що додатково здійснюють зміну коду шляхом відкривання (закривання) або часткового відкривання (закривання) каналів для проходження сигналу, що попередньо виконані в секретних елементах.

4. Автентифікатор, що містить секретні елементи з кодовими символами, які встановлені на осі з можливістю повороту, елементи взаємної фіксації, розміщені на торцях секретних елементів, який відрізняється тим, що секретні елементи виконані у вигляді багатогранників, а елементи фіксації виконані у вигляді конусних виступів та відповідних їм отворів, при цьому кількість отворів дорівнює кількості фіксованих положень секретного елемента.

5. Автентифікатор за п. 4, який відрізняється тим, що елементи фіксації виконані у вигляді конусних виступів та відповідних їм отворів, що рівномірно по колу розміщені на торцях секретних елементів.

6. Автентифікатор за п. 4, який відрізняється тим, що секретні елементи виконані у вигляді багатогранників, які мають від трьох і більше граней.

7. Автентифікатор за п. 4, який відрізняється тим, що секретні елементи виконані однополюсними.

8. Автентифікатор за п. 4, який відрізняється тим, що секретні елементи виконані двополюсними.

9. Автентифікатор за п. 4, який відрізняється тим, що поперечним перерізом багатогранника є трикутник зі зрізаними вершинами.

10. Автентифікатор за пп. 8, 9, який відрізняється тим, що полюси секретних елементів розміщені під різними кутами.

11. Автентифікатор за п. 4, який відрізняється тим, що поперечним перерізом багатогранника є квадрат зі зрізаними вершинами.

12. Автентифікатор за п. 4, який відрізняється тим, що поперечним перерізом багатогранника є десятикутник або багатокутник з більшою ніж десять кількістю сторін.

13. Автентифікатор за п. 4, який відрізняється тим, що він виконаний складеним.

14. Автентифікатор за п. 4, який відрізняється тим, що секретні елементи встановлені симетрично або асиметрично відносно осі.

15. Автентифікатор за п. 4, який відрізняється тим, що кодовими символами секретних елементів є цифри та/або букви, та/або зірочки, та/або решітки.

16. Автентифікатор за п. 4, який відрізняється тим, що секретні елементи містять канали для проходження оптичного або електромагнітного сигналу та перекриваючі елементи, наприклад гвинти, для встановлення їх в вищезгадані канали.

17. Автентифікатор за п. 16, який відрізняється тим, що канали мають складну форму для забезпечення можливості їх часткового перекривання, наприклад гвинтами.

18. Автентифікатор за п. 16, який відрізняється тим, що канали розміщені під різними кутами.

19. Автентифікатор за п. 4, який відрізняється тим, що в секретному елементі кодові символи розташовані симетрично або асиметрично.

20. Автентифікатор за п. 4, який відрізняється тим, що габарити секретних елементів відповідні розміру шахти зчитувача механічної кодової інформації або є меншими за них.

(13) C2

(11) 89745

(19) UA

21. Зчитувач кодової інформації з автентифікатора, що містить корпус з шахтою для проходження автентифікатора, а також компоненти випромінювання та прийому сигналу, який **відрізняється** тим, що в корпусі виконані канали для проходження оптичного або електромагнітного сигналу, а шахта має форму багатогранника.

22. Зчитувач за п. 21, який **відрізняється** тим, що кількість граней шахти багатогранника дорівнює 10-12.

23. Зчитувач за п. 21, який **відрізняється** тим, розмір шахти зчитувача співпадає з габаритами секретних елементів автентифікатора або дещо перевищує їх.

24. Зчитувач за п. 21, який **відрізняється** тим, що в корпусі, навколо шахти, виконані виступи для його монтажу.

25. Зчитувач за п. 21, який **відрізняється** тим, що компоненти випромінювання та прийому сигналу змонтовані безпосередньо на корпусі у паралельному порядку.

26. Зчитувач за п. 21, який **відрізняється** тим, що компоненти випромінювання та прийому змонтовані на встановлених на корпусі платах у паралельно-последовному порядку.

27. Зчитувач за п. 21, який **відрізняється** тим, що корпус виконаний складеним.

Група винаходів належить до сфери механічних носіїв кодової інформації, що використовуються зі зчитувачами кодової інформації, а точніше до способів ідентифікації та автентифікації, а також пристроїв, за допомогою яких визначається право доступу до будь-яких об'єктів і систем.

До таких способів та пристроїв висуваються наступні вимоги:

- надійний захист об'єктів від несанкціонованого доступу;
- надійна та проста конструкція;
- надійний та простий спосіб використання, зрозумілий пересічному користувачеві різного віку та різного рівня інтелектуального розвитку.

Відомий спосіб ідентифікації права доступу до об'єктів та ідентифікатор для його здійснення, що передбачають використання постійного коду (патент ВНР №181176, МПК E05B 7/10, опубл. 31.12.84р.). Надійність такого способу та ідентифікатора не безумовні, особливо у випадку втрати, крадіжки чи копіювання ідентифікатора.

Відомий спосіб ідентифікації права доступу до об'єктів і введення кодової інформації, ідентифікатор та зчитувач, що реалізують цей спосіб, які описані в патенті Російської Федерації на винахід №2097519, МПК6 E05B 19/18, опубл. 27.11.97р. бюл. №33). Відомий спосіб включає набір коду на ідентифікаторі шляхом вибіркового обертання його елементів з кодовими мітками.

Ідентифікатор, що реалізує цей спосіб, містить встановлені на стрижні з можливістю повороту однієї відносно другої пластини (секретні елементи), що мають на своїх сторонах частини коду. Кодові символи 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 підпружнений уздовж осі стрижня. Елементами фіксації є клиноподібні виступи і відповідні до них шліци.

При проходженні ідентифікатора через шахту починається робота зчитувача (контрольного пристрою). При цьому можливі різні варіанти зчитування інформації: оптичний, електромагнітний. Зчитувач кодової інформації з ідентифікатора міс-

тить корпус, в якому виконана шахта для проходження ідентифікатора, і є канали для проходження оптичного або електромагнітного сигналу.

Найближчим аналогом способу, що заявляється, є спосіб ідентифікації права доступу до об'єктів та введення інформації, описаний в патенті UA 54597 C2, МПК7 G06K19/06, опублікованому 17.03.2003, Бюл.3,2003р. Цей спосіб включає в себе оперативний набір коду на ідентифікаторі шляхом вибіркового обертання його елементів з кодовими мітками. Відповідно до способу в ньому додатково здійснюють періодичну зміну коду на ідентифікаторі шляхом однакового відкривання (закривання) частини кодових міток.

Найближчим аналогом автентифікатора (механічного носія кодової інформації) є ідентифікатор (МНКІ), описаний в міжнародній публікації WO 96/08793, 21.03.96, МКП 6: G07C.

Відомий ідентифікатор містить встановлені на стрижні з можливістю повороту однієї відносно другої пластини (секретні елементи), що мають на своїх сторонах частини коду. Кодові символи 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 підпружнений уздовж осі стрижня. Елементами фіксації є клиноподібні виступи і відповідні до них шліци.

У відомому рішенні (WO 96/08793), на Фіг.1-3 представлені зовнішні види ідентифікатора у різних формах його виконання, крім того, можливі фіксовані положення відповідають 0, 90, 180, 270 градусам, що не призводить до зміни форми механічного носія кодової інформації (ідентифікатора).

Відомі винаходи мають такі 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 (підглядіти) третіми особами будь-якими оптичними пристроями зйому інформації

(фото, відео) під час користування ідентифікатором;

- використання багатозначних кодів (порядку 10-14 знаків), які не просто запам'ятати пересічному користувачеві.

Найближчим аналогом зчитувача кодової інформації з автентифікатора є зчитувач, який описаний в патенті RU 2 057 876 Cl, МПК 6: E05B 47/00, опублікованому 10.04.1996. В цьому патенті описаний електронний замок, який містить корпус з шахтою для ключа, компоненти випромінювання, та прийому сигналу, а також схему ИЛИ, схему порівняння, елемент затримки, лічильник, комутатор, перемикачі, селектор, інвертор, дві схеми збігу, виконавчий пристрій, сигналізацію.

Відповідно до відомого патенту RU №2057876 процедура внесення «вірного» ключа та подальшого порівняння його, проводиться завдяки перемикачам, що є не зручним, а інколи не прийнятним (з точки зору можливого несанкціонованого доступу до перемикачів), бо користувач повинен буде оперувати достатньо великою кількістю перемикачів (для 4-х положень кожного секретного елемента - повинно бути 4 положення перемикача, і все це треба помножити на кількість секретних елементів). Таким чином, для отримання бажаних мільярдів комбінацій необхідно буде перемкнути 15 перемикачів в одне з 4 положень, тобто, при цьому виникає висока вірогідність помилки користувача, і, як наслідок, «вірний» ключ буде вважатися «не вірним». А це з точки зору контролю доступу є неприпустимим.

Група винаходів, що заявляється, дозволяє вирішити технічну задачу, яка полягає у створенні більш досконалого способу автентифікації і введення кодової інформації та створити автентифікатор 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-ти - 12-ти значної буквено-цифрової системи запам'ятовування коду та зменшення довжини коду до 4-8 знаків.

Визначена задача та технічний результат досягаються завдяки тому, що, здійснюючи набір коду на механічному носії кодової інформації (МНКИ), у нашому випадку на автентифікаторі, шляхом вибіркового обертання секретних елементів з кодовими символами на визначений кут навколо осі, згідно з винаходом, періодично змінюють форму автентифікатора, що являється додатковою зовнішньою ознакою коду.

Зміну форми автентифікатора здійснюють поворотом секретного елемента на певний кут і фіксацією його в цьому положенні або заміною щонайменше одного секретного елемента на інший. МНКИ може мати так звану нейтральну форму, в якій всі секретні елементи займають таке положення один відносно одного та відносно основи, в якому всі зовнішні площини елементів та основи

співпадають між собою. В такій нейтральній формі зручніше зберігати автентифікатор, оскільки він не має різких виступів чи впадін вздовж осі. Така зручність примушує користувача щоразу після введення кодової інформації із МНКИ зі зміненою формою перестроювати його в нейтральну форму, що в свою чергу виключає можливість заволодіння кодом іншою особою у випадку втрати, крадіжки чи копіювання МНКИ. Нейтральна форма автентифікатора теж може бути використана як одна із кодівих комбінацій.

Зміну форми автентифікатора можна досягти заміною щонайменше одного секретного елемента певного типу на інший. При цьому користувач може навіть зібрати свій МНКИ, нанизавши які завгодно секретні елементи в будь-якому порядку, що дозволяє створювати різні типи автентифікаторів несхожі один на одного, та збільшує кількість можливих кодівих комбінацій у тисячі разів.

Згідно зі способом додатково здійснюють зміну коду шляхом відкривання (закривання) або часткового закривання (відкривання) каналів для проходження сигналу, що попередньо зроблені в секретних елементах.

Для здійснення способу, що заявляється, призначений автентифікатор, який містить секретні елементи з кодовими символами що встановлені на осі з можливістю повороту, та елементи взаємної фіксації, що розміщені на торцях секретних елементів. Згідно з винаходом, секретні елементи виконані у вигляді багатогранників, а елементи фіксації - виконані з можливістю забезпечення фіксації секретного елемента після його повороту на певний кут.

Елементи фіксації можуть бути виконані у вигляді конусних виступів та відповідних їм отворів, що рівномірно по колу розміщені на торцях секретних елементів, при цьому кількість отворів дорівнює кількості фіксованих положень секретного елемента.

Згідно з винаходом секретні елементи можуть мати вигляд багатогранників, що мають кількість граней від трьох і більше.

Згідно з винаходом, поперечним перерізом багатогранника може бути трикутник або квадрат зі зрізаними вершинами, а також десятикутник або багатокутник з кількістю сторін більшою ніж десять.

Згідно з винаходом, автентифікатор виконаний складеним, що дозволяє нанизувати секретні елементи на вісь у довільному порядку, створюючи пристрій за власним бажанням.

Як зазначалося вище, форма секретних елементів, з яких складається механічний носій кодової інформації, може бути довільною, але з явно вираженими та достатньо наглядними для користувача, полюсами у вигляді площин, гострих, заокруглених чи зрізаних вершин, виступів і т.п. Такі полюси повинні допомагати користувачеві без зайвих міркувань визначити зміну форми МНКИ та кодової комбінації при провертанні секретних елементів один відносно одного. Кількість полюсів секретного елемента та їх взаємне розташування може бути довільним за умови безперешкодного проходження МНКИ в нейтральній та будь-якій змі-

нений формі крізь шахту зчитувача, забезпечуючи мінімальне відхилення механічного носія кодової інформації відносно зчитувача у трьох основних площинах.

Секретний елемент може встановлюватися по один бік осі і виконуватися у вигляді однополюсного елемента. Під полюсом слід розуміти найбільш віддалені від осі частини секретного елемента. Як видно на Фіг.1А, поперечним перерізом однополюсного елемента є чотирикутник, який своєю основою з'єднаний з однією із сторін восьмикутника. Замість чотирикутника можуть бути інші фігури: трикутники, п'яти- та шестикутники та інші багатокутники з більшою кількістю сторін.

Секретний елемент, згідно з винаходом, може бути двополюсним. Як видно на Фіг.2А, поперечним перерізом двополюсного елемента є два чотирикутники, що розміщені діаметрально протилежно один одному і своїми основами з'єднані з відповідними сторонами восьмикутника. Як і в попередньому випадку, замість чотирикутника можуть бути інші фігури, вказані вище.

Поперечним перерізом багатогранника може бути трикутник із зрізаними вершинами (на Фіг.3 (А,Б) він представлений як триполюсний елемент).

Полюси секретних елементів можуть розміщуватися під різними кутами (це показано на прикладі двополюсних та триполюсних елементів - Фіг.7 - Фіг.11).

Згідно з винаходом поперечним перерізом багатогранника може бути квадрат (чотирикутник) із зрізаними вершинами (на Фіг.4 (А,Б) він представлений як чотириполюсний елемент).

Секретні елементи можуть встановлюватися симетрично або асиметрично відносно осі.

Кодові символи автентифікатора розміщені на гранях багатогранника, цими символами можуть бути різноманітні позначення, наприклад, букви, числа, зірочки, решітки, точки, трикутники та інші позначення. Кодові символи можуть розташовуватися симетрично або асиметрично.

Згідно з винаходом, секретні елементи автентифікатора містять канали для проходження оптичного або електромагнітного сигналу і перекриваючі елементи, наприклад гвинти, що можуть перекривати ці канали. Канали також є кодовими символами автентифікатора.

Канали можуть мати складну форму: виконуватися з різьбою або бути ступінчастими для забезпечення їх часткового перекривання гвинтами, або можуть використовуватися для цього більш короткі гвинти.

Канали можуть розташовуватися симетрично або асиметрично.

Габарити секретних елементів відповідні розміру шахти зчитувача кодової інформації або дещо менші за них.

Для здійснення способу автентифікації і введення кодової інформації призначений також зчитувач кодової інформації з автентифікатора. Він містить корпус, в якому виконана шахта для проходження автентифікатора, і є канали для проходження оптичного або електромагнітного сигналу. Зчитувач містить компоненти випромінювання та прийому сигналу, що попарно розташовані на кор-

пусі, а шахта зчитувача має форму багатогранника.

Оптимальна кількість граней багатогранника становить 10-12.

В корпусі, навколо шахти, виконані виступи для монтажу зчитувача в різні корпуси.

Компоненти випромінювання та прийому сигналу можуть монтуватися безпосередньо на корпусі зчитувача у паралельному порядку або на встановлених на корпусі платах у паралельно-послідовному порядку.

Розмір шахти зчитувача співпадає з габаритами секретних елементів або дещо перевищує їх.

Корпус зчитувача може виконуватися складеним.

Сутність корисної моделі пояснюється кресленнями, на яких зображено:

на Фіг.1(А,Б) - автентифікатор з однополюсними секретними елементами встановленими по один бік осі, в аксонометричній проекції та вигляді спереду (нейтральна та змінена форми);

на Фіг.2(А,Б) - автентифікатор з двополюсними секретними елементами, в аксонометричній проекції та вигляді спереду (нейтральна та змінена форми);

на Фіг.3(А,Б) - автентифікатор з триполюсними секретними елементами, в аксонометричній проекції та вигляді спереду (нейтральна та змінена форми);

на Фіг.4(А,Б) - автентифікатор з чотириполюсними секретними елементами, в аксонометричній проекції та вигляді спереду (нейтральна та змінена форми);

на Фіг.5(А,Б) - секретний елемент автентифікатора з каналами для проходження сигналів, в якому виконані канали для встановлення перекриваючих елементів, наприклад, гвинтів (на Фіг.5Б - часткове перекриття каналу гвинтом);

на Фіг.6 - зображений автентифікатор, зібраний із секретних елементів різної форми;

на Фіг.7 - триполюсний секретний елемент із розташуванням полюсів під кутами 90° та 120° та відкритими усіма каналами;

на Фіг.8 - триполюсний секретний елемент із розташуванням полюсів під кутами 90° та 90° та закритими усіма каналами;

на Фіг.9 - двополюсний секретний елемент із розташуванням полюсів під кутом 90° та відкритими усіма каналами;

на Фіг.10 представлений триполюсний секретний елемент із розташуванням полюсів під кутами 90° та 90° та відкритими усіма каналами;

на Фіг.11 - двополюсний секретний елемент з каналами, що розміщені під кутами 30°;

на Фіг.12 представлений зчитувач кодової інформації з автентифікатора з 10-ма паралельно розташованими компонентами випромінювання та прийому сигналу, що утворюють пару сканування, в частково рознесеному виді та вигляді спереду;

на Фіг.13 - зчитувач з 12-ма паралельно-послідовно розташованими компонентами випромінювання та прийому сигналу (парами сканування) в частково рознесеному виді, вигляді зверху та збоку;

на Фіг.14 - триполюсний секретний елемент з перекриваючими елементами (гвинтами), один з яких частково перекриває промінь (напіввідкритий полюс перекриваючим елементом (гвинтом)).

на Фіг.15 - однополюсний секретний елемент з каналом, розташованим перпендикулярно до осі полюса, що частково пропускає промінь, бо канал розташований на межі променя (напіввідкритий полюс на 90°);

на Фіг.16 зображений однополюсний секретний елемент з каналом, розташованим перпендикулярно до осі полюса, що безперешкодно пропускає промінь, (відкритий полюс на 90°);

на Фіг.17 - однополюсний секретний елемент без каналу (закритий полюс);

на Фіг.18 - однополюсний секретний елемент без каналу, що частково перекриває промінь, своїм тілом (закритий полюс, напівперекриті промені тілом секретного елемента (полюса));

на Фіг.19 - однополюсний секретний елемент з каналом, розташованим під кутом 60° до осі полюса, що частково пропускає промінь (напіввідкритий полюс на 60°);

на Фіг.20 - однополюсний секретний елемент з каналом, розташованим під кутом 60° до осі полюса, що безперешкодно пропускає промінь (відкритий полюс на 60°);

Всі секретні елементи автентифікатора, зображені на фігурах, можуть провертатись навколо осі на 10-12 (в залежності від кількості фіксаторів) фіксованих положень відносно один одного та відносно основи. Отже кожен секретний елемент забезпечує на своїй позиції 10-12 кодових варіантів.

Така конструкція МНКІ з секретних елементів одного виду дозволяє при невеликій кількості секретних елементів набирати на ньому велику кількість варіантів коду, а саме - x^n , де n - кількість секретних елементів встановлених на МНКІ, а x - кількість фіксованих положень секретного елемента.

Додатково секретні елементи, з яких можуть комплектуватись МНКІ, можуть мати різну геометричну форму і крім того мати один і більше каналів, які можуть по різному розташовуватись на секретному елементі (під різним кутом один до одного) - тобто секретні елементи можуть бути різних видів, отже мати різні кодові варіанти в кожному з фіксованих положень.

Це дає можливість значно збільшити кількість варіантів кодів МНКІ, а саме - $(\sum X_i)^n$, де X_i - кількість фіксованих положень окремого секретного елемента, i - кількість видів секретних елементів, n - кількість секретних елементів встановлених на МНКІ.

Перевага у збільшенні кодових комбінацій тут очевидна. Крім того, є ще одна неявна перевага, - набраний власноруч з різних видів секретних елементів автентифікатор є так би мовити довгостроковим ключем з $(\sum X_i)^n$ кількістю можливих комбінацій, на якому для оперативного набору коду залишається x^n варіантів коду, але для злоумисника, який не знає з чого складається довгостроковий ключ, при підборі коду все одно необхідно буде перебирати $(\sum X_i)^n$ комбінацій!

Слід зазначити, що наявність різних видів секретних елементів, якими можуть комплектуватись МНКІ мають деякі незручності:

у розпорядженні користувача для оперативного набору коду все ж таки залишається x^n варіантів коду на одному автентифікаторі;

для того, щоб користувач зміг використовувати усі $(\sum X_i)^n$ варіанти кодів, йому необхідно мати всі види секретних елементів та щоразу при значному перепрограмуванні МНКІ потрібно його розбирати та комплектувати іншими видами та порядком секретних елементів, що не дуже зручно.

Цю проблему можна вирішити зображеною на Фіг.5(А,Б) конструкцією секретного елемента, до якої входить секретний елемент 3 із каналами 4, та встановлювальний гвинт 10.

Спосіб автентифікації і введення кодової інформації здійснюють за допомогою автентифікатора та читувача механічної кодової інформації з автентифікатора, конструкції яких представлені на Фіг.1-20.

Автентифікатор, зображений на кресленнях, містить вісь 1, на яку насаджені основа 2 та секретні елементи 3 з можливістю незалежного повороту навколо осі 1 на відповідний кут відносно основи 2 та один відносно одного. Секретні елементи мають канали 4 для проходження оптичного або електромагнітного сигналу. Торці секретних елементів 3 та основи 2, що прилягають один до одного, мають елементи взаємної фіксації 5. Як видно із приведених креслень, секретні елементи утворюють багатогранник. На Фіг.1-4 представлені різноманітні варіанти виконання багатогранників. На видимій поверхні секретних елементів, що утворюють грані багатогранника, нанесені буквенно-цифрові позначки 6, що допомагають користувачеві безпомилково встановлювати необхідний код. Крім позначок у вигляді букв та цифр можуть бути решітки, зірочки, точки, трикутники та інші позначки. На торцях секретних елементів та основи додатково нанесені мітки (стрілки) 7, що також допомагають користувачеві визначитись із положенням секретного елемента відносно основи чи інших секретних елементів.

На кінці осі 1 встановлені пружина 8 та гайка 9, які дають можливість:

- піджимати увесь набір секретних елементів 3 до основи 2;

- в разі необхідності перешкоджати самовільному або несанкціонованому повертання секретних елементів;

- розбирати автентифікатор при необхідності переналагодження чи ремонту.

Позицією 10 показаний перекриваючий елемент (гвинт), призначений для встановлення в канали 4, а позицією 11 - полюси (найбільш віддалені від осі 1 частини секретного елемента 3).

Елементи фіксації 5 представляють собою конусні виступи та відповідні їм отвори, що рівномірно по колу розміщені на торцях секретних елементів 3 (Фіг.1-2). Кількість отворів дорівнює кількості фіксованих положень секретного елемента після його повороту на певний кут.

Всі секретні елементи 3 автентифікатора, зображені на фігурах, можуть провертатись навколо

осі відносно один одного та відносно основи. Така конструкція МНКІ дозволяє при невеликій кількості секретних елементів набирати на ньому велику кількість варіантів коду в залежності від кількості секретних елементів та кількості фіксованих положень секретного елемента. Секретні елементи можуть встановлюватись симетрично або асиметрично, канали на секретних елементах також можуть розташовуватись симетрично або асиметрично, що призводить до збільшення ємності кодової інформації автентифікатора. Додатково секретні елементи, з яких комплектуються МНКІ, можуть мати один і більше каналів 4 для проходження сигналу, які по-різному розташовані в секретному елементі 3 (під різним кутом один до одного), тобто секретні елементи можуть бути різних видів, отже мати різні кодові варіанти в кожному з фіксованих положень.

Це дає можливість значно збільшити кількість варіантів кодів автентифікатора.

На Фіг.5(А,Б) представлена конструкція, до якої входить секретний елемент 3 з каналами 4, та встановлювальний гвинт 10, за допомогою якого користувач, вкручуючи або викручуючи, (в залежності від конструкції секретного елемента) перекриває або відкриває канал 4 секретного елемента. Також секретний елемент може бути оснащений встановлювальними гвинтами 10, кількість яких може дорівнювати кількості каналів, що дає додаткову можливість користувачеві перекривати або відкривати усі канали секретного елемента, що робить його так би мовити невидимим при перекритих усіх каналах, та прозорим при відкритих усіх каналах для зчитувача. Це стає можливим завдяки спеціально розробленій конструкції зчитувача, який може зафіксувати такий момент. Це дає унікальну можливість вводити код меншої довжини з визначених секретних елементів, або код, розбитий на декілька менших частин, чого не можна зробити за допомогою інших сучасних систем ідентифікації та автентифікації. Канали можуть виконуватись під різними кутами див. Фіг.10 - Фіг.11).

На Фіг.12 зображений зчитувач механічної кодової інформації з автентифікатора. Він складається із двох однакових за конструкцією симетричних частин 12 та 13, які утворюють корпус зчитувача. Кожна з частин має канали 14 для проходження оптичних або електромагнітних сигналів, елементи взаємної фіксації 15 у вигляді конусів та відповідних їм отворів, 10-ти гранні шахти 16 для проходження автентифікатора, та круглі виступи 17 навколо шахт 16, призначені для монтажу зчитувача. На корпусні частини 12 та 13 за допомогою централізації в каналах 14 монтується через один по колу компоненти 18 та 19, що відповідно випромінюють та приймають сигнали. Розташовуючись один навпроти одного у паралельному порядку, компоненти 18 та 19 утворюють пари сканування, за допомогою яких відбувається зчитування механічної кодової інформації із автентифікатора та перетворення її в електронну. На Фіг.12 показаний зчитувач з 10-ма паралельно розташованими парами сканування та 10-ти гранною формою шахти 16.

На Фіг.13 зображений зчитувач з 12-ма паралельно-послідовним розташуванням пар сканування. Він складається із двох однакових зовнішніх 20 та двох однакових внутрішніх 21 корпусних частин, кожна з яких має канали 14 аналогічні зображеним на Фіг.12 для проходження сигналів, елементи взаємної фіксації 15 аналогічні зображеним на Фіг.12 у вигляді конусів та відповідних їм отворів, елементи фіксації плат 22 у вигляді конусів, та 12-ти гранні шахти 23 для проходження автентифікатора. Зовнішні корпусні частини 20 мають круглі виступи 17 навколо шахт 23 аналогічні зображеним на Фіг. 12, призначені для монтажу зчитувача. На корпусні частини 20 та 21 за допомогою елементів фіксації 22 кріпляться плати 24 із вмонтованими компонентами 18 та 19, що відповідно випромінюють та приймають сигнали. Розташовуючись один навпроти одного у паралельно-послідовному порядку, плати із компонентами 18 та 19 утворюють пари сканування, за допомогою яких відбувається зчитування кодової інформації з автентифікатора та перетворення її в електронну.

Спосіб автентифікації і введення кодової інформації здійснюють за допомогою автентифікатора, що зображений на одній із представлених фігур. Елементи фіксації 5 дозволяють після повороту секретного елемента 3 зафіксувати його в певному положенні, це дає можливість періодично змінювати форму автентифікатора (див. Фіг.1(А,Б) - Фіг.4(А,Б)). Зміну форми автентифікатора можна здійснювати заміною його секретних елементів іншими, що мають, наприклад, іншу форму, або якісь інші відмінності. На Фіг.6 зображений автентифікатор, складений із різних секретних елементів 3. Як видно на Фіг., для зміни форми автентифікатора достатньо замінити щонайменше один секретний елемент на елемент іншої форми.

Додатково, конструкція автентифікатора (див. Фіг.5) дозволяє здійснити зміну коду шляхом відкривання (закривання) або часткового закривання (відкривання) каналів 4 за допомогою гвинтів 10. Для забезпечення часткового закривання (відкривання) каналів вони можуть мати складну форму, а саме, виконуватись ступінчастими, мати різьбу, можливо також використання коротких гвинтів.

Автентифікатор працює наступним чином. Перед використанням на ньому набирають необхідний код, наприклад обертанням певних секретних елементів 3 відносно осі 1. Після цього його вводять в шахту зчитування (16 або 23), що розташована в зчитувачі кодової інформації з автентифікатора (Фіг.12-13). Відбувається послідовне або паралельно-послідовне зчитування кодової інформації з автентифікатора та перетворення її в електронну форму, зчитування відбувається за допомогою компонентів 18 та 19, що відповідно випромінюють та приймають сигнали та утворюють пари сканування. При цьому можливі різні варіанти зчитування інформації: оптичний, електромагнітний та інші. Для цього канали виконуються з матеріалів, що дозволяють виконати ці варіанти зчитування.

Для більш наглядної демонстрації сигнали та конкретний секретний елемент, що проходить

процедуру зчитування показано на (Фіг.16-20), сигнали умовно позначені римськими цифрами.

Секретний елемент автентифікатора проходить крізь площину, в якій випромінюються сигнали, завдяки своїй конструкції, може повністю або ж частково перетинати (частково або повністю закриваючи) або не перетинати (частково або повністю відкриваючи) деякі сигнали у будь-якому порядку. Все, що відбувається із сигналами під час послідовного проходження повз них секретних елементів автентифікатора, фіксує контролер (на Фіг. не показаний).

При цьому слід згадати, що автентифікатор може повністю відповідати габаритам шахти 16 або 23, або бути трохи меншим за неї, (це досягається або розмірами шахти зчитувача або розмірами автентифікатора). У цих випадках один і той же секретний елемент може утворювати зовсім різні вихідні кодові комбінації. Це добре показано на попарних ілюстраціях з однаковими за формою секретними елементами, з різними за розмірами шахтами зчитувача (або самого автентифікатора): Фіг.16 - Фіг.15, Фіг.17 - Фіг.18, Фіг.20 - Фіг.19.

Крім того на Фіг.17 - Фіг.18 показано як відбувається сканування секретного елемента без каналів для проходження сигналу, а на Фіг.14 показано як відбувається зчитування секретного елемента, який містить в собі елементи, що перекривають канали для проходження сигналу.

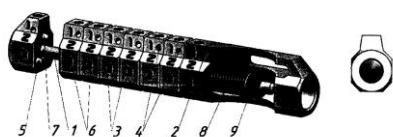
Сукупність частково або повністю закритих, відкритих сигналів при проходженні крізь них секре-

тного елемента автентифікатора утворює певну кодову комбінацію елемента у відповідному положенні на автентифікаторі. Сукупність кодових комбінацій секретних елементів автентифікатора у певних положеннях утворюють вихідну кодову послідовність автентифікатора, яку можна змінювати наприклад завдяки повороту секретних елементів навколо осі автентифікатора.

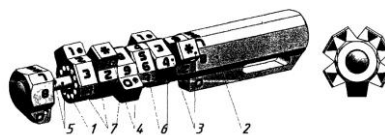
У випадку встановлення невірності коду доступ до об'єкта залишається перекритим (не відбувається) і може спрацювати сигналізація.

Запропонована група винаходів має значну перевагу над існуючими аналогами, вказаними вище, в плані використання значно більшої кількості кодових комбінацій, при суттєвому зменшенні кількості секретних елементів в автентифікаторі (так для того, щоб ввести 24 бітний ключ, потрібно було б використати ключ-ідентифікатор з 24 сегментів, а з використанням запропонованого автентифікатора лише двох!), в плані зручності користування пересічним користувачем та гнучкості використання.

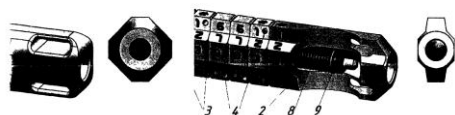
Запропоновані можливі варіанти конструкції МНКІ, що призначені для здійснення способу автентифікації права доступу до об'єктів і введення кодової інформації, які використовуються разом із зчитувачем кодової інформації, являють собою універсальну систему та можуть використовуватись на будь-якому об'єкті, доступ до якого потребує введення кодової інформації.



Фіз. 1А

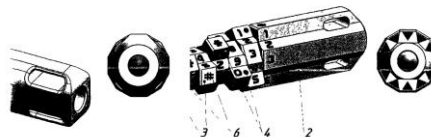


Фіз. 1Б



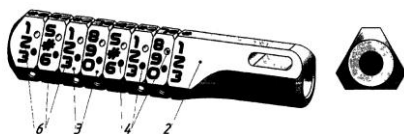
А

Фіз. 2А

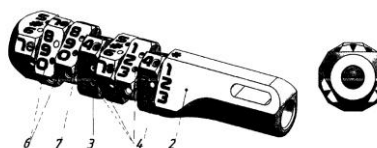


Б

Фіз. 2Б



Фіз. 3А

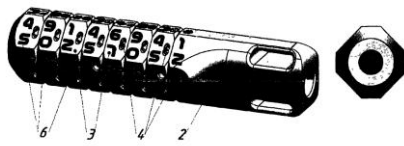


Фіз. 3Б

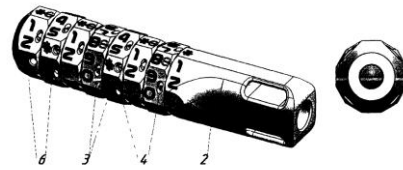
15

89745

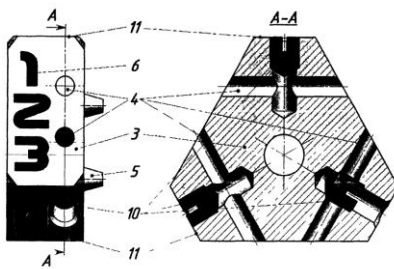
16



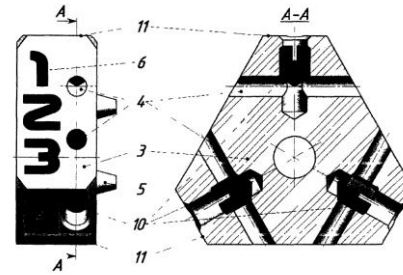
Фиг. 4А



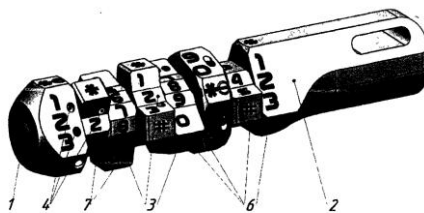
Фиг. 4Б



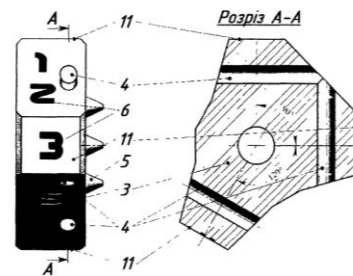
Фиг. 5А



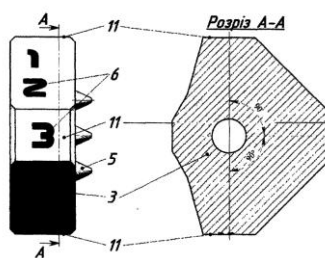
Фиг. 5Б



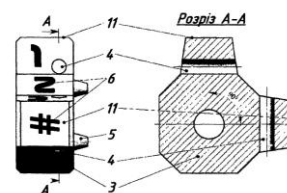
Фиг. 6



Фиг. 7



Фиг. 8

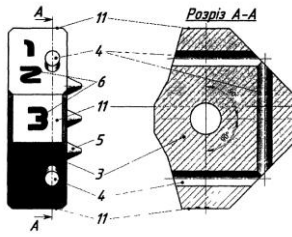


Фиг. 9

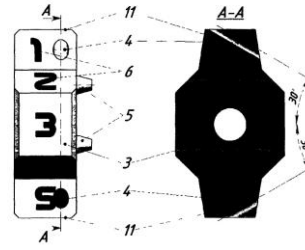
17

89745

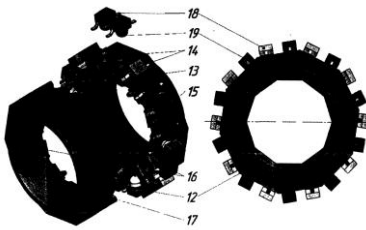
18



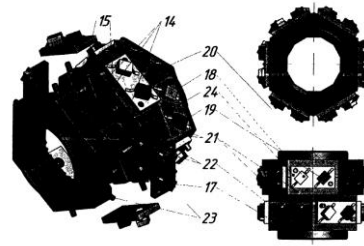
Фіз. 10



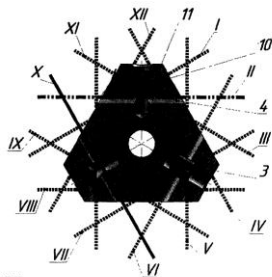
Фіз. 11



Фіз. 12

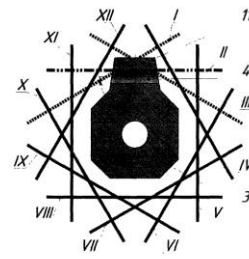


Фіз. 13



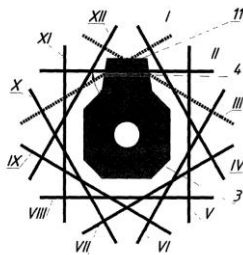
Умовні позначення:
 відкритий промінь —————
 закритий промінь —————
 частково закритий (відкритий) промінь — — — — —
 I, II, III, IV — номери променів

Фіз. 14



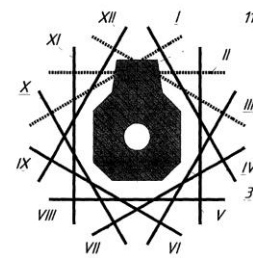
Умовні позначення:
 відкритий промінь —————
 закритий промінь —————
 частково закритий (відкритий) промінь — — — — —
 I, II, III, IV — номери променів

Фіз. 15



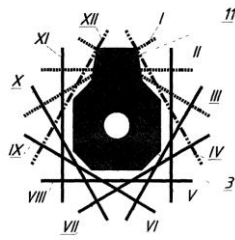
Умовні позначення:
 відкритий промінь —————
 закритий промінь —————
 частково закритий (відкритий) промінь — — — — —
 I, II, III, IV — номери променів

Фіз. 16



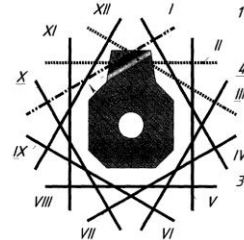
Умовні позначення:
 відкритий промінь —————
 закритий промінь —————
 частково закритий (відкритий) промінь — — — — —
 I, II, III, IV — номери променів

Фіз. 17



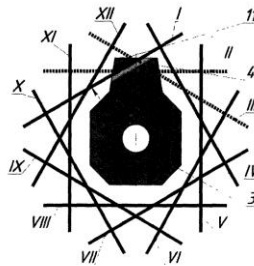
Умовні позначення:
 відкритий промінь —————
 закритий промінь - - - - -
 частково закритий (відкритий) промінь - · - · -
 (I,II,III,IV) - нумерація променів

Fig. 18



Умовні позначення:
 відкритий промінь —————
 закритий промінь - - - - -
 частково закритий (відкритий) промінь - · - · -
 (I,II,III,IV) - нумерація променів

Fig. 19



Умовні позначення:
 відкритий промінь —————
 закритий промінь - - - - -
 частково закритий (відкритий) промінь - · - · -
 (I,II,III,IV) - нумерація променів

Fig. 20