



УКРАЇНА

(19) **UA** (11) **90371** (13) **C2**
(51) МПК (2009)
G07F 7/10
G07F 7/00
G07D 7/20 (2006.01)

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ТА ПРИСТРІЙ ДЛЯ ІДЕНТИФІКАЦІЇ ОСОБИ АБО ПІДТВЕРДЖЕННЯ ПРАВ З ЗАСТОСУВАННЯМ ОДНОРАЗОВИХ КОДІВ ТРАНЗАКЦІЙ

1

(21) a200808525
(22) 30.11.2006
(24) 26.04.2010
(86) PCT/GB2006/050422, 30.11.2006
(31) 0524414.0
(32) 01.12.2005
(33) GB
(31) 0601910.3
(32) 31.01.2006
(33) GB
(31) 60/774,225
(32) 17.02.2006
(33) US
(31) 0613835.8
(32) 13.07.2006
(33) GB
(31) 0614902.5
(32) 27.07.2006
(33) GB
(46) 26.04.2010, Бюл.№ 8, 2010 р.
(72) КРЕЙМЕР ДЖОНАТАН, GB, ХОУЕС СТИВЕН, GB
(73) ГРІДЛОКТС ЛІМІТЕД, GB
(56) US 6246769 B1; 12.06.2001
FR 2459514 A; 09.01.1981
EP 1239426 A; 11.09.2002
WO 95/20820 A; 03.08.1995
(57)

1. Спосіб ідентифікації особи, який включає етап реєстрації для особи особистої конфігурації певної кількості позицій у сітці у зв'язку з особистими ідентифікаційними даними, з наступним застосуванням конфігурації у процесі перевірки, причому наступний процес перевірки включає етапи:

(а) представлення особі контрольної сітки позицій, зайнятих псевдовипадковим набором символів, з вимогою вказати відповідний набір символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається;

(b) отримання відповідного набору у перевірному пристрої та генерації на основі контрольної сітки та конфігурації, що зберігається, перевірною набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається;

2

(с) порівняння відповідного набору символів з перевірним набором символів;
та

(d) підтвердження ідентифікації особи, якщо відповідний набір є таким самим, що й перевірний набір.

2. Спосіб за п. 1, який **відрізняється** тим, що етап реєстрації включає спочатку представлення особі сітки з пропозицією вибрати особисту конфігурацію позицій.

3. Спосіб за п. 1 або 2, який **відрізняється** тим, що включає повідомлення відповідного набору на комп'ютер, який дає дозвіл, на транзакцію, у місці, віддаленому від особи, причому етапи з (b) по (d) здійснюються у вищезгаданому комп'ютері, який дає дозвіл.

4. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає генерацію контрольної сітки у терміналі користувача та передачу на комп'ютер, який дає дозвіл, відповідного набору символів та контрольної сітки або даних, що дозволяє комп'ютерові, який дає дозвіл, розпізнати або відновити контрольну сітку.

5. Спосіб за п. 4, який **відрізняється** тим, що включає використання алгоритму в терміналі користувача для генерації псевдовипадкової послідовності символів згідно з датою та/або часом дня та ідентифікаційних даних для того, щоб термінал та/або особа могли скласти контрольну сітку, та передачу на комп'ютер, який дає дозвіл, принаймні відповідного набору та ідентифікаційних даних, причому комп'ютер, який дає дозвіл, використовує такий самий алгоритм та вищезгадані ідентифікаційні дані і дату та/або час дня для генерації такої самої псевдовипадкової послідовності символів, таким чином, відновлюючи контрольну сітку.

6. Спосіб за п. 5, який **відрізняється** тим, що включає застосування другого алгоритму для генерації, на основі відповідного набору та додаткового ідентифікатора, пароля, який складається з послідовності символів, які приховують відповідний набір, причому етап (b) включає використання відновленої контрольної сітки для генерації перевірною набору, застосування другого алгоритму з використанням фактора або факторів для генера-

(13) **C2**

(11) **90371**

(19) **UA**

ції пароля з перевірного набору, і етап (с) включає порівняння отриманого пароля з генерованим паролем.

7. Спосіб за п. 6, який **відрізняється** тим, що додатковим ідентифікатором є принаймні один з факторів, до яких належать:

- (i) час та/або дата транзакції;
- (ii) ідентифікатор особи або рахунку;
- (iii) ідентифікатор терміналу;
- (iv) ключ шифрування публічних/приватних даних;
- (v) сума платежу, у разі платіжної транзакції; та
- (vi) повний номер рахунку отримувача або його частина.

8. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає алгоритмічний вибір у терміналі користувача однієї з багатьох контрольних сіток, які були попередньо надані вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, та передачу на комп'ютер, який дає дозвіл на транзакцію, відповідного набору та даних, які ідентифікують перед комп'ютером, який дає дозвіл, алгоритмічно вибрану сітку.

9. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає алгоритмічний вибір у терміналі користувача початкової контрольної точки у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору та початкової контрольної точки.

10. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає алгоритмічний вибір у терміналі користувача заданої кількості символів з великої таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, представлення контрольної сітки з вищезгаданих вибраних символів, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору, причому на етапі (d) комп'ютер, який дає дозвіл, використовує такий самий алгоритм для вибору з попередньо наданої великої таблиці однакових символів для відновлення контрольної сітки.

11. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає отримання у терміналі користувача початкової контрольної точки, яка передається на нього комп'ютером, який дає дозвіл, початкова контрольна точка вказує позицію у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл, і зберігається у терміналі, представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору.

12. Спосіб за п. 3, який **відрізняється** тим, що етап (а) включає знаходження у базі даних сіток,

незалежних від комп'ютера, який дає дозвіл, алгоритмічно вибраної однієї з багатьох сіток, які зберігаються у вищезгаданій базі даних, причому вищезгадана сітка має унікальний ідентифікатор, та передачу на комп'ютер, який дає дозвіл, відповідного набору та вищезгаданого ідентифікатора сітки, і етап (b) включає надсилання комп'ютером, який дає дозвіл, ідентифікатора на незалежну базу даних для знаходження контрольної сітки.

13. Спосіб за будь-яким з пп. з 4 по 12, який **відрізняється** тим, що термінал користувача є автоматичною касовою машиною (АТМ).

14. Спосіб за будь-яким з пп. з 4 по 12, який **відрізняється** тим, що термінал користувача є комп'ютером, який може бути з'єднаний з комп'ютером, який дає дозвіл, через мережне з'єднання.

15. Спосіб за будь-яким з пп. з 4 по 12, який **відрізняється** тим, що термінал користувача є переносним електронним пристроєм, який з'єднується з комп'ютером, який дає дозвіл, через безпроводний зв'язок.

16. Спосіб за будь-яким з пп. з 4 по 12, який **відрізняється** тим, що передача на комп'ютер, який дає дозвіл, включає усне повідомлення.

17. Спосіб за будь-яким з попередніх пп., який **відрізняється** тим, що особа також повідомляє на комп'ютер, який дає дозвіл, інформацію від пристрою ідентифікації або запам'ятовування транзакції.

18. Спосіб за п. 17, який **відрізняється** тим, що запам'ятовуючий пристрій міститься у/на кредитній або дебетовій картці.

19. Спосіб за п. 17, який **відрізняється** тим, що запам'ятовуючий пристрій є включеним до переносного електронного пристрою, який переноситься особою.

20. Спосіб за будь-яким з попередніх пп., який **відрізняється** тим, що особиста конфігурація включає послідовність, у якій використовують позиції.

21. Спосіб за п. 1, 2 або 3, який **відрізняється** тим, що контрольна сітка представляється як попередньо надрукований лист з певною кількістю символів у відповідних позиціях сітки.

22. Спосіб за п. 1, 2 або 3, який **відрізняється** тим, що на етапі (а) контрольна сітка надається особі чіпом пам'яті у кредитній або дебетовій картці.

23. Спосіб за п. 22, який **відрізняється** тим, що на етапі (а) сітка зчитується з вищезгаданого чіпа пам'яті пристроєм для зчитування карток.

24. Спосіб за п. 23, який **відрізняється** тим, що вищезгаданий пристрій для зчитування карток забезпечується у переносному електронному пристрої, яким володіє особа.

25. Спосіб за п. 1 або 2, який **відрізняється** тим, що пристрій для перевірки є електронним пристроєм, який переноситься особою.

26. Спосіб за п. 25, який **відрізняється** тим, що електронний пристрій є включеним у картку для здійснення транзакцій або ідентифікаційну картку.

27. Спосіб за п. 1 або 2, який **відрізняється** тим, що пристрій для перевірки є комп'ютером для контролю доступу.

28. Спосіб транзакції, який включає первісний етап реєстрації зберігання в організації, яка здійснює транзакцію, особистої конфігурації певної кількості

позицій у сітці у зв'язку з особистими ідентифікаційними даними та особистого ідентифікаційного номера (PIN), з наступним включенням у кожну наступну транзакцію етапу автентифікації, який підтверджує користувачеві справжність організації, яка здійснює транзакцію, причому етап автентифікації включає повідомлення користувачем організації, яка здійснює транзакцію, його прізвища або іншого основного ідентифікатора, і організація, яка здійснює транзакцію, у відповідь забезпечує показ користувачеві сітки з псевдовипадкових цифр, у якій PIN користувача займає комірки особистої конфігурації користувача.

29. Спосіб автентифікації повідомлень, які надсилаються організацією окремим отримувачам, який включає первісний етап реєстрації зберігання в організації особистої конфігурації певної кількості позицій у сітці для потенційного отримувача у зв'язку з особистими ідентифікаційними даними та особистого ідентифікаційного номера (PIN), з наступним наданням у повідомленні, надісланому організацією отримувачеві, сітки з псевдовипадкових цифр, у якій PIN отримувача займає комірки особистої конфігурації отримувача.

30. Пристрій для застосування при ідентифікації особи, який включає засоби для отримання та зберігання ідентифікаційних даних особи та пов'язаної з ними конфігурації позицій на сітці, електронні засоби за місцем особи для представлення особі контрольної сітки та пропозиції особі щодо введення у відповідь на неї відповідного набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається, та засоби перевірки для отримання від особи відповідного набору, причому засоби перевірки є пристосованими для генерації на основі контрольної сітки та конфігурації, що зберігається, перевірного набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається, для порівняння відповідного набору символів з перевірним набором символів, і для підтвердження ідентичності особи, якщо відповідний набір є таким самим, що й перевірний набір.

31. Пристрій за п. 30, який **відрізняється** тим, що конфігурація позицій є конфігурацією, первісно вибраною користувачем.

32. Пристрій за п. 30 або 31, який **відрізняється** тим, що засоби перевірки включають комп'ютер, який дає дозвіл на транзакцію.

33. Пристрій за п. 30 або 31, який **відрізняється** тим, що електронними засобами є термінал користувача, віддалений від комп'ютера, який дає дозвіл на транзакцію.

34. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим для генерації контрольної сітки і пристосованим для передачі на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від вищезгаданого терміналу користувача, відповідного набору та контрольної сітки або даних, які дозволяють комп'ютерові, який дає дозвіл на транзакцію, ідентифікувати або відновити контрольну сітку.

35. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на використання алгоритму для генерації псевдовипадко-

вої послідовності символів згідно з датою та/або часом дня та ідентифікаційних даних для того, щоб термінал та/або особа могли скласти контрольну сітку, і пристосованим для передачі на комп'ютер, який дає дозвіл на транзакцію, принаймні ідентифікаційних даних, причому комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на використання вищезгаданих ідентифікаційних даних та дати/часу дня для генерації, з застосуванням такого самого алгоритму, такої самої псевдовипадкової послідовності символів, таким чином, відновлюючи контрольну сітку.

36. Пристрій за п. 35, який **відрізняється** тим, що термінал користувача є запрограмованим на застосування другого алгоритму для генерації на основі відповідного набору та додаткового ідентифікатора пароля, який складається з послідовності символів, які приховують відповідний набір, і комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на використання відновленої контрольної сітки для генерації перевірного набору символів, на застосування другого алгоритму з використанням фактора або факторів для генерації пароля з перевірного набору та наступне порівняння отриманого пароля з генерованим паролем для надання або відхилення підтвердження.

37. Пристрій за п. 36, який **відрізняється** тим, що додатковим ідентифікатором є принаймні один з факторів, до яких належать:

- (i) час та/або дата транзакції;
- (ii) ідентифікатор особи або рахунку;
- (iii) ідентифікатор терміналу;
- (iv) ключ шифрування публічних/приватних даних;
- (v) сума платежу, у разі платіжної транзакції; та
- (vi) повний номер рахунку отримувача або його частина.

38. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на алгоритмічний вибір однієї з багатьох контрольних сіток, які були попередньо надані вищезгаданому терміналові користувача і зберігаються в ньому, і пристосованим для передачі на комп'ютер, який дає дозвіл, відповідного набору та даних, які ідентифікують вибрану сітку.

39. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на алгоритмічний вибір початкової контрольної точки у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача і зберігається в ньому, на представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, з наступною передачею на комп'ютер, який дає дозвіл, відповідного набору та початкової контрольної точки.

40. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на алгоритмічний вибір заданої кількості символів з великої таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, на представлення контрольної сітки з вищезгаданих вибраних символів, з наступною передачею на комп'ютер, який дає дозвіл, відповідного набору, причому комп'ютер, який дає дозвіл, є запрограмованим на використання такого самого

алгоритму для вибору з попередньо наданої великої таблиці однакових символів для відновлення контрольної сітки.

41. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на отримання початкової контрольної точки, яка передається на нього комп'ютером, який здійснює перевірку, початкова контрольна точка вказує позицію у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача і зберігається в ньому, на представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, з наступною передачею на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від терміналу користувача, відповідного набору.

42. Пристрій за п. 33, який **відрізняється** тим, що термінал користувача є запрограмованим на знаходження у базі даних сіток, незалежних від комп'ютера, який дає дозвіл на транзакцію, та від особи, алгоритмічно вибраної однієї з багатьох сіток, які зберігаються у вищезгаданій базі даних, причому вищезгадана сітка має унікальний ідентифікатор, і на передачу на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від терміналу користувача, відповідного набору та вищезгаданого ідентифікатора сітки, і комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на передачу ідентифікатора на незалежну базу даних для знаходження контрольної сітки.

43. Пристрій за будь-яким з пп. з 33 по 42, який **відрізняється** тим, що термінал користувача є автоматичною касовою машиною (АТМ).

44. Пристрій за будь-яким з пп. з 33 по 42, який **відрізняється** тим, що термінал користувача є комп'ютером, який може бути з'єднаний з комп'ютером, який дає дозвіл на транзакцію, через мережне з'єднання.

45. Пристрій за будь-яким з пп. з 33 по 42, який **відрізняється** тим, що термінал користувача є переносним електронним пристроєм, який може бути з'єднаний з комп'ютером, який дає дозвіл, через безпроводний зв'язок.

46. Пристрій за будь-яким з пп. з 30 по 45, який **відрізняється** тим, що електронні засоби є пристосованими для повідомлення на комп'ютер, який

дає дозвіл на транзакцію, інформації від пристрою ідентифікації або запам'ятовування транзакції.

47. Пристрій за п. 46, який **відрізняється** тим, що запам'ятовуючий пристрій міститься у/на кредитній або дебетовій картці.

48. Пристрій за п. 47, який **відрізняється** тим, що запам'ятовуючий пристрій є включеним до переносного електронного пристрою, який може переноситись особою.

49. Пристрій за п. 47, який **відрізняється** тим, що електронні засоби включають у комбінації чіп пам'яті у картці та пристрій для зчитування карток.

50. Пристрій за п. 49, який **відрізняється** тим, що пристрій для зчитування карток є включеним у мобільний або стільниковий телефон.

51. Пристрій за пп. 30 або 31, який **відрізняється** тим, що засоби перевірки є електронним пристроєм, який може переноситись особою.

52. Пристрій за п. 51, який **відрізняється** тим, що електронний пристрій є включеним у картку для здійснення транзакцій або ідентифікаційну картку.

53. Система контролю доступу, яка включає пристрій за п. 30 або 31, у якій засоби перевірки є комп'ютером для контролю доступу, запрограмованим на надання доступу у відповідь на підтвердження справжності.

54. Система контролю доступу за п. 53, яка **відрізняється** тим, що комп'ютер для контролю доступу контролює зняття блокування.

55. Пристрій для здійснення транзакцій, який включає засоби отримання та зберігання в організації, яка здійснює транзакцію, ідентифікаційних даних для користувача та пов'язаної з ними конфігурації позицій на сітці, разом з особистим ідентифікаційним номером (PIN) користувача, електронні засоби за місцем користувача для представлення користувачеві процесу автентифікації, який підтверджує користувачеві справжність організації, яка здійснює транзакцію, причому процес автентифікації включає надсилання користувачеві запиту про надання організації, яка здійснює транзакцію, його прізвища або іншого основного ідентифікатора, і організація, яка здійснює транзакцію, у відповідь забезпечує надання користувачеві за допомогою електронних засобів сітки з псевдовипадкових цифр, у якій PIN користувача займає комірки особистої конфігурації користувача.

Даний винахід стосується способу та пристрою для ідентифікації особи або підтвердження прав особи, наприклад, на доступ у приміщення або на отримання певних послуг.

Підробка кредитних карток є головною проблемою для реалізаторів та виробників кредитних карток. Багато компаній-виробників кредитних карток розв'язують цю проблему через впровадження технології "Chip and Pin", але це не розв'язує проблему шахрайства "Card not present", яка поширюється зі збільшенням кількості людей, які здійснюють онлайніві покупки за допомогою кредитних карток або купують товари по телефону.

Крім того, з поширенням комп'ютерних вірусів, зокрема, "троянських коней", які фіксують комбінації

клавів (включаючи номери кредитних карток та особисті ідентифікаційні номери ("PIN-коди")), надсилання інформації про кредитні картки та PIN-кодів другій стороні, яка не викликає довіри, само по собі не є безпечним.

Даний винахід забезпечує спосіб, який дозволяє зменшити кількість випадків шахрайства завдяки застосуванню "одноразових" кодів транзакцій, а також забезпеченню загальних засобів ідентифікації особи або підтвердження прав особи.

Потенційними галузями застосування є купівля за допомогою кредитних карток, системи контролю входу до приміщень та транспортних засобів (увімкнення запалювання транспортних засобів), пе-

ревірка клієнтів банку, паспортний контроль, заміни паспортів або інші ситуації, в яких вимагається право особи на отримання послуги.

У патенті US-B-6 246 769 описується система заміни PIN-кодів на спеціальний код транзакції, який користувач розпізнає з таблиці символів, користуючись особистою випадково вибраною конфігурацією та послідовністю позицій таблиці, які користувач реєструє у центральній базі даних разом з особистими ідентифікаційними даними / даними рахунку. Коли, наприклад, треба здійснити транзакцію, конфігурація користувача відшукується у базі даних, і спеціальний код транзакції створюється, а потім поміщається у таблицю згідно з позиціями конфігурації. Решта позицій заповнюється символами, які не використовуються у спеціальному коді транзакції, для приховування коду, доки користувачеві не буде показано таблицю з вимогою про введення символів, які займають позиції особистої конфігурації користувача. Після цього термінал визначає, що користувач ввів правильний прихований код, перш, ніж вимагати дозволу на транзакцію.

У багатьох ситуаціях цей процес є небажаним з двох принципових причин. По-перше, він вимагає передачі особистої конфігурації користувача, яка зберігається, з центральної бази даних на термінал користувача (наприклад, АТМ), що може бути ненадійним, а по-друге, транзакція вимагає або двох окремих сеансів передачі даних до центральної бази даних, або одного безперервного з'єднання протягом усієї транзакції. У будь-якому разі це є неприйнятним для транзакцій у магазинах та банках, оскільки суттєво збільшує витрати на функціонування системи - такі транзакції мають включати лише одне коротке повідомлення для отримання права на транзакцію - і при цьому можуть бути пов'язані зі збільшенням ризику порушення безпеки транзакції, якщо процес надання дозволу вимагає безперервного з'єднання протягом усієї транзакції.

Крім того, процес, описаний у US-B-6 246 679, не може застосовуватися для автономних платіжних систем, оскільки вимагає доступу до особистої конфігурації користувача.

Даний винахід забезпечує спосіб ідентифікації особи, який включає зберігання особистої конфігурації певної кількості позицій у сітці у зв'язку з особистими ідентифікаційними даними, з наступним застосуванням конфігурації у процесі перевірки, причому наступний процес перевірки включає етапи:

(а) представлення особі контрольної сітки позицій, зайнятих псевдовипадковим набором символів, з вимогою вказати відповідний набір символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається;

(b) отримання відповідного набору у перевірному пристрої та генерації на основі контрольної сітки та конфігурації, що зберігається, перевірному набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається;

(с) порівняння відповідного набору символів з перевірним набором символів; та

(d) підтвердження ідентифікації особи, якщо відповідний набір є таким самим, що й перевірний набір.

В оптимальному варіанті етап реєстрації включає спочатку представлення особі сітки з пропозицією вибрати особисту конфігурацію позицій. Пропозиція може стосуватися вибору заданої кількості позицій для утворення особистої конфігурації або вибору довжини конфігурації з одного або кількох заданих чисел, наприклад, 4, 5 або 6, або навіть вибору такої кількості позицій, яку особа може надійно запам'ятати, з певною мінімальною кількістю.

В одному аспекті винаходу спосіб включає повідомлення відповідного набору на комп'ютер, який дає дозвіл, на транзакцію, у місці, віддаленому від особи, та здійснення етапів з (b) по (d) у вищезгаданому комп'ютері, який дає дозвіл.

Згідно з одним варіантом втілення винаходу, етап (а) включає генерацію контрольної сітки у терміналі користувача та передачу на комп'ютер, який дає дозвіл, відповідного набору символів та контрольної сітки або даних, що дозволяє комп'ютерові, який дає дозвіл, розпізнати або відновити контрольну сітку. В оптимальному варіанті цей варіант втілення включає використання алгоритму в терміналі користувача для генерації псевдовипадкової послідовності символів згідно з датою та/або часом дня та ідентифікаційних даних для того, щоб термінал та/або особа могли скласти контрольну сітку, та передачу на комп'ютер, який дає дозвіл, принаймні відповідного набору символів та ідентифікаційних даних, причому комп'ютер, який дає дозвіл, використовує такий самий алгоритм та вищезгадані ідентифікаційні дані і дату та/або час дня для генерації такої самої псевдовипадкової послідовності символів, таким чином, відновлюючи контрольну сітку.

Цей спосіб дозволяє досягати додаткової безпеки завдяки використанню другого алгоритму для генерації, на основі відповідного набору та додаткового ідентифікатора, наприклад, принаймні одного з факторів, до яких належать:

- (i) час та/або дата транзакції;
- (ii) ідентифікатор особи або рахунку;
- (iii) ідентифікатор терміналу;
- (iv) ключ шифрування публічних / приватних даних;
- (v) суму платежу, у разі платіжної транзакції; та
- (vi) повний номер рахунку отримувача або його частина;

пароля, який складається з послідовності символів, які приховують відповідний набір, причому етап (с) включає використання відновленої контрольної сітки для генерації перевірного набору, застосування другого алгоритму з використанням фактора або факторів для генерації пароля з перевірного набору, і етап (d) включає порівняння отриманого пароля з генерованим паролем.

Згідно з іншим варіантом втілення винаходу, етап (а) включає алгоритмічний вибір у терміналі користувача однієї з багатьох контрольних сіток, які були попередньо надані вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на

транзакцію, і зберігаються у терміналі, та передачу на комп'ютер, який дає дозвіл на транзакцію, відповідного набору та даних, які ідентифікують перед комп'ютером, який дає дозвіл, алгоритмічно вибрану сітку.

В іншому варіанті втілення винаходу етап (а) включає алгоритмічний вибір у терміналі користувача початкової контрольної точки у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору та початкової контрольної точки.

У ще одному варіанті втілення винаходу етап (а) включає алгоритмічний вибір у терміналі користувача заданої кількості символів з великої таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, представлення контрольної сітки з вищезгаданих вибраних символів, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору, причому на етапі (б) комп'ютер, який дає дозвіл, використовує такий самий алгоритм для вибору з попередньо наданої великої таблиці однакових символів для відновлення контрольної сітки.

В іншому альтернативному варіанті втілення винаходу етап (а) включає отримання у терміналі користувача початкової контрольної точки, яка передається на нього комп'ютером, який дає дозвіл, початкова контрольна точка вказує позицію у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл, і зберігається у терміналі, представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, та наступну передачу на комп'ютер, який дає дозвіл, відповідного набору.

У ще одному варіанті втілення винаходу етап (а) включає знаходження у базі даних сіток, незалежних від комп'ютера, який дає дозвіл, алгоритмічно вибраної однієї з багатьох сіток, які зберігаються у вищезгаданій базі даних, причому вищезгадана сітка має унікальний ідентифікатор, та передачу на комп'ютер, який дає дозвіл, відповідного набору та вищезгаданого ідентифікатора сітки, і етап (с) включає надсилання комп'ютером, який дає дозвіл, ідентифікатора на незалежну базу даних для знаходження контрольної сітки.

Доступ до комп'ютера або іншого обладнання може контролюватися способом згідно з винаходом.

Сітка може бути попередньо надрукована з певною кількістю символів у відповідних позиціях сітки.

В одному варіанті втілення винахід включає спосіб ідентифікації особи або перевірки "права на послугу", який може (але не обов'язково повинен) застосовуватись у зв'язку з пристроєм для надійного запису будь-яких кодів або PIN-кодів і т. ін.

Зокрема, даний винахід може застосовуватись у взаємодії з картою "Craumer Grid", яка є предметом паралельно перебуваючої у стадії розгляду патентної заявки № GB0517333.1.

Craumer Grid є пристроєм для надійного зберігання інформації і включає перший елемент, який має першу поверхню, другий елемент, який має другу поверхню, перший та другий елементи можуть переміщуватись відносно один одного у вибрану позицію, перша поверхня має принаймні одне вікно для того, щоб частини другої поверхні можна було побачити крізь принаймні одне вікно, і перша та друга поверхні мають сітчасті позначення, у які користувач може вписувати знаки, таким чином, щоб задані знаки на другій поверхні можна було побачити лише крізь принаймні одне вікно, коли перший та другий елементи перебувають у вибраній позиції. Пристрій може бути у формі плоскої гільзи, яка містить ковзний елемент, позначений порожнім сітчастим малюнком, на якому користувач може вводити один або кілька PIN-кодів або інші захисні цифри, літери або їх комбінації. Після цього користувач може заповнити решту позицій сітки випадковими цифрами, літерами і т. ін. Наприклад, коли користувач хоче використати конкретний PIN-код, він вставляє елемент всередину гільзи доки у вікні не з'явиться потрібний код. Лише користувач знає, якою є ця позиція. Користувач може у прихований спосіб зробити позначки на сітці, які нагадуватимуть йому, якою є "вихідна позиція", що дозволить користувачеві зчитувати правильний код.

Слід розуміти, що застосування авторами терміну "сітка" включає не лише правильні сітки, як описано нижче з посиланням на фігури, але й невідповідне розташування позицій. Наприклад, розташування на "решітці" може бути представлене різними елементами малюнка, і проміжки між однією позицією та будь-якою іншою не обов'язково мають бути рівномірними, ні за відстанню, ні за напрямком.

В альтернативному варіанті у винаході можуть застосовуватись віртуальні сітки, які зберігаються на чіпах кредитних або дебетових (або інших ідентифікаційних) карток, тобто, віртуальна сітка є представленою даними, які можуть бути показані користувачеві у вигляді сітки пристроєм для зчитування карток. Вони можуть зчитуватись за допомогою EPOS або спеціально призначеним пристроєм для зчитування карток або телефоном, таким, як мобільний телефон, який може бути оснащений пристроєм для зчитування карток, або будь-яким придатним електронним пристроєм. Сітки в альтернативному варіанті можуть зберігатись (як віртуальні сітки) у телефоні. EPOS може генерувати власну сітку. Вибрана конфігурація користувача може надійно зберігатись, наприклад, на чіпі картки.

В альтернативному варіанті винаходу можуть використовуватись сітки, які автоматично генеруються автентифікатором, причому перевірка здійснюється шляхом порівняння відповіді користувача з попередньо зареєстрованою конфігурацією, яку було надійно закодовано автентифікатором на чіпі кредитної / дебетової картки користувача або

іншого пристрою для ідентифікації особи або підтвердження прав.

Спосіб згідно з даним винаходом вимагає, щоб сторона (автентифікатор), яка бажає здійснити перевірку (наприклад, компанія, що випускає кредитну / дебетову картку), надіслала запит користувачеві (наприклад, покупцеві) щодо набору цифр (розпізнавального коду) на основі сітки, яку генерує автентифікатор, або за "координатами сітки", визначеними автентифікатором.

Після цього користувач використовує сітку цифр, яка також відома автентифікаторові (наприклад, Craymer Grid, або представлену не екрані онлайнову сітку, яка генерується автентифікатором), і вибирає набір цифр згідно з конфігурацією або "формою", яку знає лише він та автентифікатор, а потім повідомляє ці цифри назад автентифікаторові.

Оскільки автентифікатор також знає цифри сітки та відому користувачеві послідовність та конфігурацію, він також може відшукати таку саму послідовність та конфігурацію цифр, і у разі їх збігу, результат перевірки є позитивним.

Оскільки автентифікатор може запитати послідовність та конфігурацію цифр на основі власної випадкової комбінації або координат сітки, наступні транзакції можуть вимагати від користувача іншої вихідної позиції координат сітки. Це означає, що в наступних транзакціях вимагатиметься інший розпізнавальний код. (Ця ситуація зазвичай виникає тоді, коли користувач використовує автономну, а не онлайнову сітку).

Слід розуміти, що посилання на "набір цифр" і т. ін. також включає символи, відмінні від арабських цифр.

Пристрій для перевірки може бути електронним пристроєм, який носить користувач, наприклад, електронним чіпом, включеним у картку для здійснення транзакцій або ідентифікаційну картку.

Згідно з одним аспектом винаходу, пристрій для перевірки є комп'ютером для контролю доступу, який контролює доступ у приміщення та інші місця, або до обладнання або транспортних засобів.

Винахід також забезпечує пристрій для застосування при ідентифікації особи, який включає засоби для отримання та зберігання ідентифікаційних даних особи та пов'язаної з ними конфігурації позицій на сітці, електронні засоби за місцем особи для представлення особі контрольної сітки та пропозиції особі щодо введення у відповідь на неї відповідного набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається, та засоби перевірки для отримання від особи відповідного набору, причому засоби перевірки є пристосованими для генерації на основі контрольної сітки та конфігурації, що зберігається, перевірного набору символів, які займають позиції у контрольній сітці, які відповідають особистій конфігурації, що зберігається, для порівняння відповідного набору символів з перевірним набором символів, і для підтвердження ідентичності особи, якщо відповідний набір є таким самим, що й перевірний набір.

Засоби перевірки можуть включати комп'ютер, який дає дозвіл на транзакцію.

Електронні засоби в оптимальному варіанті являють собою термінал користувача віддалений від комп'ютера, який дає дозвіл на транзакцію.

В одному варіанті втілення винаходу термінал користувача є запрограмованим для генерації контрольної сітки і пристосованим для передачі на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від вищезгаданого терміналу користувача, відповідного набору та контрольної сітки або даних, які дозволяють комп'ютерові, який дає дозвіл на транзакцію, ідентифікувати або відновити контрольну сітку.

В іншому варіанті втілення термінал користувача є запрограмованим на використання алгоритму для генерації псевдовипадкової послідовності символів згідно з датою та/або часом дня та ідентифікаційних даних для того, щоб термінал та/або особа могли скласти контрольну сітку і пристосованим для передачі на комп'ютер, який дає дозвіл на транзакцію, принаймні ідентифікаційних даних, причому комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на використання вищезгаданих ідентифікаційних даних та дати / часу дня для генерації, з застосуванням такого самого алгоритму, такої самої псевдовипадкової послідовності символів, таким чином, відновлюючи контрольну сітку.

Термінал користувача також може бути запрограмований на використання другого алгоритму для генерації, на основі відповідного набору та додаткового ідентифікатора, наприклад, принаймні одного з факторів, до яких належать:

- (i) час та/або дата транзакції;
- (ii) ідентифікатор особи або рахунку;
- (iii) ідентифікатор терміналу;
- (iv) ключ шифрування публічних / приватних даних;
- (v) суму платежу, у разі платіжної транзакції; та
- (vi) повний номер рахунку отримувача або його частина;

пароля, який складається з послідовності символів, які приховують відповідний набір, і комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на використання відновленої контрольної сітки для генерації перевірного набору символів, на застосування другого алгоритму з використанням фактора або факторів для генерації пароля з перевірного набору та наступне порівняння отриманого пароля з генерованим паролем для надання або відхилення підтвердження.

В іншому варіанті втілення термінал користувача є запрограмованим на алгоритмічний вибір однієї з багатьох контрольних сіток, які були попередньо надані вищезгаданому терміналові користувача і зберігаються в ньому, і пристосованим для передачі на комп'ютер, який дає дозвіл, відповідного набору та даних, які ідентифікують вибрану сітку.

У ще одному варіанті втілення термінал користувача є запрограмованим на алгоритмічний вибір початкової контрольної точки у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача і зберігаються в ньому, на представлення контрольної сітки, отриманої з великої таблиці з використанням контро-

льної точки, з наступною передачею на комп'ютер, який дає дозвіл, ідентифікованих символів та початкової контрольної точки.

В іншому варіанті втілення, в якому термінал користувача є запрограмованим на алгоритмічний вибір заданої кількості символів з великої таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача органом, який дає дозвіл на транзакцію, або комп'ютером, який дає дозвіл на транзакцію, і зберігається у терміналі, на представлення контрольної сітки з вищезгаданих вибраних символів, з наступною передачею на комп'ютер, який дає дозвіл, відповідного набору, причому комп'ютер, який дає дозвіл, є запрограмованим на використання такого самого алгоритму для вибору з попередньо наданої великої таблиці однакових символів для відновлення контрольної сітки.

У ще одному варіанті втілення термінал користувача с запрограмованим на отримання початкової контрольної точки, яка передається на нього комп'ютером, який здійснює перевірку, початкова контрольна точка вказує позицію у великій таблиці символів, яка була попередньо надана вищезгаданому терміналові користувача і зберігаються в ньому, на представлення контрольної сітки, отриманої з великої таблиці з використанням контрольної точки, з наступною передачею на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від терміналу користувача, ідентифікованих символів.

У ще одному варіанті втілення термінал користувача є запрограмованим на знаходження у базі даних сіток, незалежних від комп'ютера, який дає дозвіл на транзакцію, та від особи, алгоритмічно вибраної однієї з багатьох сіток, які зберігаються у вищезгаданій базі даних, причому вищезгадана сітка має унікальний ідентифікатор, і на передачу на комп'ютер, який дає дозвіл на транзакцію, у місці, віддаленому від терміналу користувача, ідентифікованих символів та вищезгаданого ідентифікатора сітки, причому комп'ютер, який дає дозвіл на транзакцію, є запрограмованим на передачу ідентифікатора на незалежну базу даних для знаходження контрольної сітки.

Термінал користувача може бути автоматичною касовою машиною (АТМ). В альтернативному варіанті термінал користувача є комп'ютером, який може бути з'єднаний з комп'ютером, який дає дозвіл, через мережне з'єднання, або переносним електронним пристроєм, який може бути з'єднаний з комп'ютером, який дає дозвіл, через безпроводний зв'язок.

У разі, коли контрольна сітка розраховується алгоритмічно, пристрій користувача може бути повністю відокремлений від ідентифікуючого комп'ютера. У цьому разі перевірні символи можуть повідомлятися, наприклад, вербально, третій стороні - операторові з телефонних продажів, який завершує етап перевірки, або через програму розпізнавання голосу.

До переваг винаходу належать такі:

Людям важко пам'ятати PIN-коди. Але людина пам'ять значно краще запам'ятовує форми та малюнки. Цей спосіб звільняє від необхідності запам'ятовування PIN-кодів. Це забезпечує вищий ступінь

безпеки ніж той, що існує нині, водночас забезпечуючи для користувача спрощений спосіб запам'ятовування його засобів автентифікації.

Через випадковість контрольної сітки правильний розпізнавальний код у наступних транзакціях змінюється. Таким чином, у разі купівлі за допомогою кредитної картки, якщо хтось бачить, як користувач вводить код транзакції, а потім викрадає кредитну / дебетову картку, то не зможе скористатися PIN-кодом / кредитною картою, якщо не знає вибраних користувачем "послідовності" та "конфігурації". Люди часто послаблюють безпеку своїх кредитних / дебетових карток через написання їх PIN-кодів. Абстрактний характер конфігурацій, які пропонуються згідно зі способом цього винаходу, утруднює написання або "опис" конфігурації.

Оскільки коди транзакцій змінюються для кожної окремої транзакції, існує можливість здійснення відносно безпечних онлайнних транзакцій через Інтернет або телефон. Перевірка транзакції також може здійснюватися за допомогою переносного електронного пристрою, зокрема, пристрою зв'язку, такого, як смарт-телефон, тобто, мобільного телефону, оснащеного пристроєм для зчитування карток, або менш складного мобільного телефону, як описується авторами нижче.

Більшість систем автентифікації запитують PIN-код з чотирьох цифр. Однак, оскільки людині легше запам'ятовувати конфігурації, ніж цифри, можна впроваджувати розпізнавальні коди з 5, 6 або більшої кількості знаків без зайвих проблем для користувача.

Спосіб може застосовуватися без будь-якої додаткової апаратної інфраструктури у терміналах для оплати в місцях купівлі, для онлайнних інтернет-покупок або в АТМ. Такі термінали можуть забезпечуватися через смарт-телефони, як описується нижче. Передбачається, що може застосовуватися існуюче обладнання "Chip and Pin", хоча й з мінімальним перепрограмуванням.

Для покупців через кредитні / дебетові картки можуть бути зареєстровані кілька кредитних / дебетових карток для застосування з числовою сіткою.

Процес легко засвоюється і не вимагає високого ступеня навичок з боку користувача.

Для людей з порушеним зором можуть бути легко створені системи зі шрифтом Брайля.

Для онлайнних або інших електронних покупок не вимагається додаткового обладнання з боку користувача. Для інших ситуацій, коли вимагається нанесена на папір сітка, необхідне обладнання користувача є дешевим у виробництві і не являє або майже не являє цінності у разі крадіжки.

Безпека послаблюється лише у разі, якщо третя сторона знає "послідовність" та "конфігурацію". Випадковий або навіть зловмисний спостерігач не зможе її легко визначити.

Важливим є те, що система не здійснює на будь-якому етапі передачу фактичної особистої конфігурації, так само, як не використовує цю конфігурацію для побудови контрольної сітки, а це дозволяє уникнути ризику перехоплення та незаконного використання з боку третьої сторони. Крім

того, система забезпечує безпечно отримання дозволу на транзакцію, наприклад, у торговому автоматі або касовому терміналі через одноразове короточасне з'єднання з комп'ютером, який дає дозвіл, що мінімізує витрати на з'єднання і збільшує безпеку з'єднання. Це є особливо важливим, коли з'єднання з комп'ютером, який дає дозвіл, здійснюється через модем та комутоване з'єднання, яке на даний час є стандартним способом. В результаті кожен телефонний дзвінок може включати вартість, а також потребує часу на встановлення з'єднання, і за телефонні дзвінки також зазвичай стягується плата згідно з тривалістю дзвінка, тому підтримання з'єднання протягом усієї транзакції може суттєво збільшувати витрати, зокрема, у випадках, коли деякі користувачі повільніше за інших виконують транзакції.

Хоча винахід є важливим для ідентифікації особи перед організацією, такою, як банк, він також дозволяє користувачеві встановити справжність банку або іншої організації. Це може бути важливим для боротьби з таким видом шахрайства, як "фішинг", коли людей змушують розкривати конфіденційну інформацію про рахунок через фальшиві інтернет-сайти банку, і ця інформація потім використовується для крадіжок грошей з банківського рахунку особи. Для того, що продемонструвати користувачеві, що інтернет-сайт банку є справжнім, можна використовувати два секретні фрагменти інформації, спільні для банку та користувача, згідно зі способом винаходу, тобто, стандартний PIN-код та секретну конфігурацію користувача. Перш, ніж повідомити будь-які конфіденційні дані (наприклад, вхідний пароль) на інтернет-сайті банку, користувач має пересвідчитися, що сайт є справжнім. Це може забезпечуватися через сайт банку, який показує, наприклад, у відповідь на введення імені користувача, сітку, заповнену випадковими (або принаймні псевдовипадковими) цифрами, за винятком показу PIN-коду користувача у позиціях секретної конфігурації користувача. Користувач може перевірити їх правильність, перш, ніж перейти до введення пароля для доступу на сайт.

До інших можливостей належать надання сітки з прихованим PIN-кодом у друкованій формі, наприклад, з підтвердженням справжності поштового листа, або через електронне повідомлення, наприклад, повідомлення електронною поштою, що дозволяє отримувачеві встановити справжність відправника.

Короткий опис фігур

Винахід описується з посиланням на супровідні фігури, серед яких:

Фігури з 1 по 3 показують сітку та різні способи використання сітки згідно з винаходом;

Фігура 4 показує варіант сітки;

Фігура 5 показує варіанти мозаїки які можуть застосовуватися для сітки;

Фігура 6 є блок-схемою, яка показує спосіб онлайнної перевірки згідно з одним варіантом втілення винаходу;

Фігура 7 є блок-схемою, яка показує спосіб онлайнної перевірки з застосуванням зовнішньої бази даних стандартних контрольних сіток;

Фігура 8 є блок-схемою, яка показує спосіб перевірки, згідно з яким застосовують одну велику сітку, коли користувач спрямовується на конкретну позицію на сітці як початкову контрольну точку;

Фігура 9 є блок-схемою, яка показує спосіб перевірки з застосуванням сітки, локально генерованої за допомогою залежного від часу алгоритму;

Фігура 10 показує пристрій для перевірки транзакції згідно з іншим варіантом втілення винаходу;

Фігура 11 показує варіант пристрою з Фігури 10, з застосуванням зовнішньої бази даних стандартних контрольних сіток, наприклад, як у способі, показаному на Фігурі 7;

Фігура 12 показує варіант пристрою з Фігури 10, з застосуванням стільникового телефону як перевірочного терміналу користувача;

Фігура 13 є блок-схемою, яка показує спосіб перевірки згідно з ще одним варіантом втілення винаходу;

Фігура 14 є схематичним поясненням пристрою та способу для місцевої перевірки особи користувача з застосуванням кредитної картки користувача або іншої картки з даними; і

Фігура 15 показує пристрій, який може застосовуватися для надання користувачеві підтвердження справжності організації, яка здійснює транзакцію.

Детальний опис показаних варіантів втілення

Для полегшення розуміння представленого нижче опису авторами було вжито такі терміни:

"Сітка" - табличний набір символів, таких, як цифри або літери або їх комбінація. Сітка може (але не обов'язково повинна) являти собою "Crauter Grid", що є предметом вищезгаданої паралельно перебуваючої у стадії розгляду патентної заявки.

"Конфігурація" - вибір позицій сітки, які складають "конфігурацію", яка відома лише користувачеві сітки та автентифікаторові (див. нижче). Конфігурація не обов'язково повинна мати звичну форму, таку, як пряма лінія, квадрат або трикутник. Дійсно, перевага віддається конфігурації неправильної форми.

"Послідовність" - порядок, у якому вибрано позиції сітки у "конфігурації".

"Автентифікатор" - особа або організація, яка бажає перевірити чиюсь особу або підтвердження прав.

"Користувач" - особа або організація, яка застосовує систему і потребує підтвердження або засвідчення її особи.

Здійснення способу

Спосіб згідно з винаходом включає представлені нижче складові етапи, які

залежать від того, чи застосовує користувач спосіб електронним способом (наприклад, за допомогою телефону або Інтернет), чи вручну (наприклад, використовуючи паперову сітку, доступну користувачеві).

1. Реєстрація (включає три нижчезазначені заходи):

A. Випуск переносних сіток (не обов'язково для онлайнної автентифікації)

B. Реєстрація переносної сітки (не обов'язково для онлайнної автентифікації)

С. Реєстрація послідовності та конфігурації (яка вимагається як для переносних сіток, так і для онлайнної автентифікації)

2. З застосуванням системи з переносною сіткою. АБО

3. Застосування системи з електронною сіткою (наприклад, для онлайнних покупок або через АТМ).

Різні етапи нижче описуються більш детально.

1. Реєстрація

а Випуск сіток

При застосуванні переносного варіанта цього способу необхідно видати користувачеві попередньо надруковану сітку. Для більш масштабного застосування (наприклад, компанією, що випускає кредитні / дебетові картки) може бути надруковано багато мільйонів різних сіток з метою зниження ймовірності того, що дві людини матимуть однакову сітку. Не обов'язково кожна особа має унікальну сітку; але чим більше варіантів сітки, тим більше підвищується безпека. У сітках мають показуватись ідентифікатори у рядках та колонках, наприклад, літери для колонок і цифри для рядків. Ідентифікаторами в альтернативному або додатковому варіанті можуть бути символи, кольори або їх комбінації.

Сітки мають однаковий розмір та формат, але розташування символів (цифр, літер та ін.) у різних сітках є різним. Однак цей спосіб може функціонувати успішно й надійно, якщо на кожній сітці друкуються однакові символи, оскільки кожен користувач вибирає свою конфігурацію та послідовність для ідентифікації власної особи або підтвердження прав.

Кожна сітка містить ідентифікаційний код, який унікальним чином ідентифікує сітку. Цей ID-код має зберігатись у надійній комп'ютерній базі даних разом з деталями про користувача та електронною копією цифр сітки. Ідентифікаційний номер не повинен давати жодних підказок стосовно цифр на сітці.

b. Реєстрація переносних сіток

Від користувачів вимагається підтвердження факту отримання ними Сітки та реєстрація сітки як такої, що їм належить. Кожен емітент картки (наприклад, банк) має свій оптимальний спосіб випуску сіток та ідентифікації кінцевого користувача, залежно від потрібного рівня безпеки. Прикладами можуть бути особиста реєстрація, онлайнна реєстрація або автоматична телефонна реєстрація.

Агентство, яке випускає картку, може бути довіреним агентством, послугами якого можуть користуватись багато організацій. Наприклад, довіреним агентством може представляти кілька компаній - емітентів кредитних карток.

Реєстрація конфігурації / послідовності

Відразу після того, як особа користувача стає відомою автентифікаторові, користувач має зареєструвати власну особисту "послідовність та конфігурацію". Це може бути "секрет групи осіб", відомий лише користувачеві та автентифікаторові.

Конкретний спосіб онлайнної реєстрації конфігурації показано на Фігурі 1. Користувачеві представляється сітка з квадратиків. Фігура 1 показує сітку 7x7, яка забезпечує високий ступінь безпеки для таких операцій, як купівля за допомогою кре-

дитних карток. Однак сітка також може бути більшою для більшої безпеки або меншою для меншої безпеки, але більш зручного застосування.

Центр сітки (А), Фігура 1, називається "вихідною позицією" або "контрольною точкою сітки", навколо якої користувач має вибрати конфігурацію. Сітка може бути позначена кольором для полегшення орієнтації користувача по сітці, але кольори або затінення і т. ін. не є необхідними.

Користувач зазвичай отримує запит від автентифікатора про створення конфігурації з чотирьох позицій, тобто, рівня безпеки, рівноцінного стандартному PIN. Якщо враховувати, що цей процес здійснюється електронними засобами, користувач має послідовно натискати на потрібні квадратики. Коли він це здійснює, вибрані квадратики можуть показуватись, наприклад, через освітлення, поясу самого символу або, можливо, через єдиний символ, такий, як * у кожній позиції. (Від користувача має вимагатись більше або менше позицій сітки, залежно від потрібного ступеня безпеки).

Наведений авторами приклад показує, що у вибраній послідовності конфігурації позиція (1) знаходиться по діагоналі зліва над контрольною точкою сітки. Друга позиція (2) знаходиться зліва від контрольної точки, третя позиція (3) знаходиться зліва від другої, і четверта позиція (4) знаходиться під другою. Звичайно, у більшості випадків для автентифікації критичним є вказування правильної конфігурації у належній послідовності. Звичайно, це так само передбачає вимогу введення знаків PIN-коду у належній послідовності, інакше неправильну послідовність не буде прийнято, навіть, якщо знаки будуть такими самими. Однак слід зазначити, що у випадках, коли вимагається нижчий рівень безпеки, ідентифікація правильної конфігурації може відбуватись й без врахування послідовності.

При виборі конфігурації користувач має заохочуватись до якомога більш "обхідних" шляхів, тоді, як вибір прямих ліній або інших правильних форм вважається небажаним (а може й заборонятись). Так само при виборі не обов'язково використовувати контрольну точку сітки. Конфігурація може знаходитись у будь-якому місці сітки, і окремі елементи конфігурації не обов'язково мають межувати один з одним або навіть перебувати в одній ділянці сітки. По суті, чим більш невиразною є конфігурація, тим надійнішою вона є. Вибирати один квадратик більше, ніж один раз, прямо не забороняється, хоча з точки зору безпеки автентифікатор навряд чи може дозволити користувачеві вибрати одну цифру, наприклад, чотири рази.

Зрозуміло, що сітка 7x7 передбачає безліч можливих конфігурацій, які може вибрати користувач. Слід зазначити, що існує приблизно 5,7 мільйона конфігурацій для 4-значного коду, а для 5-значного коду ця кількість збільшується приблизно до приблизно 282,5 мільйона. Позиції у сітці, вибрані користувачем, не повинні межувати уздовж сторін або у кутах.

Якщо користувач реєструє стандартну сітку "Craumer Grid", він додатково має ввести вибраним ним "вихідну позицію" та вибраний колір з боку під'єднання (сірий або чорний). Ці дані стають час-

тиною ключа або "секретом групи осіб" між користувачем та автентифікатором.

Якщо система використовується, наприклад, у зв'язку з кредитною / дебетовою картою, автентифікатор на цьому етапі може виявити бажання встановити зв'язок картки з реєстрацією особи. Це є необхідним у випадках, коли користувач намагається здійснити покупку "Card not present". Це може здійснюватися через "swiping" картки або шляхом стандартної автентифікації "chip and pin" для встановлення зв'язку номера картки з користувачем.

Так само, як при онлайнному способі реєстрації конфігурації, також існує можливість реєстрації по телефону або усно через вказування кожної позиції в сітці, скажімо, з 1 по 49 (для сітки 7 x 7). Конкретний спосіб залежить від потрібного рівня безпеки. Наприклад, банк може вимагати від особи застосування засобів електронних банківських послуг для реєстрації послідовності та конфігурації або особистої присутності у відділенні для їх введення.

Альтернативний підхід до реєстрації конфігурації для автентифікатора може полягати у введенні у реєстраційну сітку випадково розташованих неповторюваних знаків. Наприклад, для сітки 5x5 можуть використовуватися літери від А до Y без повторів. Користувач у цьому разі може вказати автентифікаторові вибрану ним конфігурацію шляхом введення літер у вибрані квадратики. Оскільки вони є неповторюваними, автентифікатор може легко визначити конфігурацію / послідовність.

2. Застосування системи з переносною сіткою (наприклад, Craymer Grid)

Для застосування сітки необхідно, щоб сітка була зареєстрована на користувача, і щоб користувач зареєстрував конфігурацію та (як правило) послідовність у реєстраційному агентстві (автентифікатор, компанія, що випускає кредитну / дебетову картку та ін.), як щойно було описано.

Для пояснення процесу як приклад може бути застосована кредитна картка для роздрібних покупок, при яких здійснюються такі етапи:

а) Клієнт вибирає певні товари і йде на касу для сплати за них за допомогою кредитної / дебетової картки як зазвичай.

б) Він віддає свою картку як зазвичай, і вона поміщається у пристрій "Chip and PIN".

с) Замість запитання про PIN-код його просять ввести чотири цифри, які відповідають випадково вибраним координатам сітки (наприклад, G4) на попередньо зареєстрованій сітці. Вихідна позиція або координати на сітці вибираються випадково або алгоритмічно агентством, яке випускає кредитну картку.

д) Типова сітка, показана на Фігурі 4, складається з колонок, позначених літерами від А до Q, та рядків, позначених цифрами від 1 до 12. Звичайно, так само прийнятними є інші комбінації. Кількість рядків та/або колонок може бути різною, залежно від потрібного рівня безпеки. Позиція на сітці, таким чином, може бути визначена унікальною комбінацією цифр / літер. Однак сітка "Craymer Grid" може забезпечувати вищий рівень безпеки.

е) Застосовуючи вищенаведений приклад та приклад конфігурації, показаний під час процесу реєстрації (Фігура 2), користувач має знайти позицію на сітці G4 (у цьому разі цифра 0) і використати її як контрольну точку сітки.

ф) Знайшовши позицію G4 і запам'ятавши свою послідовність та конфігурацію, користувач вводить чотири цифри, пов'язані з попередньо зареєстрованою конфігурацією, (див. фігуру 2). Так, у цьому прикладі цифри є такими: "9846".

г) Після цього він вводить чотири цифри на клавішній панелі "chip and pin".

h) Комп'ютерна система компанії, яка випустила кредитну картку, порівнює ці чотири цифри з сіткою, пов'язаною з його кредитною картою і з попередньо вибраною послідовністю та конфігурацією.

і) Якщо ці цифри збігаються, користувач підтверджується, і транзакція завершується.

Наступного разу, коли користувач здійснює покупку, агентство, яке випустило кредитну картку, випадково або алгоритмічно вибирає нову позицію "координат сітки", і, таким чином, чотирицифровий код, який вимагається для автентифікації транзакції, буде іншим. Наприклад, при наступній транзакції у користувача можуть запитати цифру, яка відповідає "K9", і в такому разі дійсним кодом має бути "9047".

Для транзакції особа не обов'язково має використовувати власну сітку. Може використовуватися будь-яка зареєстрована сітка (наприклад, сітка, зареєстрована на власника крамниці або на друга). У цьому разі альтернативний ID сітки має бути введений у місці продажу перед введенням користувачем його коду транзакції. Ця зміна процесу означає, що користувач все одно може користуватися системою без необхідності носіння власної картки. Це дає особливу перевагу, якщо, наприклад, кредитну картку та картку з сіткою біло вкрадено. У цій ситуації користувач може зателефонувати до автентифікатора і ідентифікувати себе, наприклад, за прізвищем та адресою, а потім агентство вимагає автентифікації через використання сітки третьої сторони.

Хоча це не забезпечує такого ж високого рівня безпеки, за відсутності будь-якої іншої форми ідентифікації це все ж краще, ніж нічого. Таким чином, цей захід може достатньо надійно застосовуватися у транзакціях "низької вартості", коли ризик є невисоким.

Нижче представлено опис ще одного прикладу того, яким чином винахід може бути застосований для купівлі товарів або послуг, наприклад, театральних квитків, по телефону.

Користувач телефонує агентові з замовлення квитків, який запитує номер кредитної картки. Після цього агент з замовлення квитків підтверджує кредитну картку, а потім компанія, яка випустила кредитну картку, пропонує операторові запитати у клієнта код транзакції на основі координат сітки, вказаних компанією, яка випустила кредитну картку.

Після цього агент по телефону запитує у користувача код транзакції, користувач знаходить цифри коду транзакції, використовуючи свою сітку і зчитує їх агентом.

Після цього агент вводить цифри, і агентство, яке випустило кредитну / дебетову картку, приймає або відхиляє транзакцію.

Цей процес є значно безпечнішим за нині існуючі, оскільки він не вимагає повідомлення даних агентів з замовлення квитків. Навіть якщо запам'ятає код транзакції та номер кредитної картки, він не зможе дістати з цього ніякої вигоди, якщо спробує обманним шляхом здійснити ще одну транзакцію, оскільки наступного разу буде запитаний інший код транзакції.

Цей спосіб також стане у пригоді інвалідам, які мають доглядальника, наприклад, пацієнтам після інсульту, яким важко розмовляти по телефону або користуватися клавіатурою "chip and pin", але які можуть користуватися сіткою. Таким чином, користувач-інвалід може повідомити доглядальникові код транзакції, і він може бути надійно повідомлений відповідній компанії по телефону або введений за допомогою клавіатури. Доки користувач-інвалід надійно зберігає сітку та конфігурацію, його транзакції є безпечними.

3. Застосування системи з електронною сіткою (наприклад, для онлайнних покупок через мережу, АТМ або термінал у місці продажу)

Для онлайнної автентифікації (наприклад, онлайнних покупок) існує три можливі варіанти застосування цього винаходу. Вибір способу великою мірою залежить від усвідомлення ризику для безпеки та потрібного рівня зручності.

Цими трьома способами є такі:

3 застосуванням зареєстрованої паперової сітки, як показано вище у прикладі.

3 застосуванням електронної "одноразової" сітки у такій самій формі, як показано вище (Фіг. 4) або з застосуванням електронної сітки "Craymer Grid"

3 застосуванням спрощеної "одноразової" електронної сітки у формі, показаній на Фігурі 3.

У такому випадку, як цей, користувачеві показується сітка у формі показаній на Фігурі 3. Однак цифри, які показуються, є алгоритмічно генерованими системою автентифікації. Система автентифікації таємно "запам'ятовує" цифри сітки до завершення транзакції.

Після цього користувач вибирає свою конфігурацію цифр шляхом натискання на відповідні квадратики, контактів з сенсорним екраном або, в оптимальному варіанті, шляхом введення відповідних цифр на клавіатурі, оскільки хтось, хто заглядає через плече, може побачити конфігурацію, яка вводиться, і так само існує ймовірність незаконного спостереження на відстані за натисканням на квадратики. Введення цифр не вказує конфігурацію, оскільки однакові цифри можуть бути представлені багатьма різними конфігураціями. Єдиний раз, коли хтось може натиснути на квадратики, пов'язані з конфігурацією, є реєстрація конфігурації, і передбачається, що користувач має зробити це безпечно.

Згідно з прикладом з Фігури 2, розпізнавальний код у цьому разі має бути "5178". Відразу після введення автентифікатор перевіряє введені цифри з відомою йому конфігурацією та послідовністю і, у разі їх збігу, користувач підтверджується.

Існують різні переваги використанні електронної сітки в цій формі:

а. Будь-яка особа, яка підглядає за натисканням клавіш на комп'ютері, бачитиме введення цифр, але оскільки код транзакції є "одноразовим", ним неможливо скористатись у будь-яких подальших транзакціях.

б. Навіть якщо особа, яка підглядає, може виявити цифри на екрані (що буває зробити дуже важко, якщо цифри показуються у графічному зображенні), вона все одно не зможе визначити "послідовність та конфігурацію" користувача, що підглядає, що підглядає, бачила натискання клавіш. Оскільки в цьому прикладі цифри "5178" на сітці трапляються багато разів, особі, що підглядає, має поспостерігати за кількома транзакціями для того, щоб отримати достатній "ключ", за допомогою якого вона зможе визначити конфігурацію.

с. Зрозуміло, що чим більш вигадливим є користувач при виборі конфігурації, тим важче буде визначити конфігурацію будь-якій особі, що підглядає.

Застосування системи з мобільними телефонами

Даний винахід може застосовуватися з мобільними телефонами різними способами, залежно від того, чи має мобільний телефон функцію зчитування карток (тобто, чи є він "смартфоном").

Якщо телефон включає пристрій для зчитування карток, він, по суті, стає персональною системою EPOS. По-перше, користувач має вставити свою картку в телефон (як у терміналах EPOS у магазинах). Комп'ютер, який підтверджує справжність, після цього надсилає сітку 7x7 (або, наприклад, 5X5) на екран телефону. Користувач, застосовуючи систему конфігурації та послідовності, ключову для даного винаходу, має визначити цифри, які вимагаються комп'ютером, що підтверджує справжність, у відповідь на його запит, і ввести їх через клавіатуру мобільного телефону, завершуючи автентифікацію транзакції.

Для мобільних телефонів з меншою кількістю функцій мають бути створені прикладні програми, які безпечно завантажуються у телефон (так сам, як, наприклад, рингтон), який зберігає номери віртуальних сіток з цифрами. Так само, як у разі паперової сітки, система автентифікації надсилає користувачеві запит про координати сітки, але замість, наприклад, 'G4' вона має здійснювати запит з номером сітки, наприклад, "234". Користувач набирає 234 у телефоні, і після цього телефон показує стандартну сітку, яка належить до типу, описаного з посиланням на Фігуру 3, на LCD-дисплеї. У цьому разі користувач має використовувати її так само, як в онлайнній системі. Компанія, яка випустила кредитну / дебетову картку, може автоматично надавати користувачеві вигляд набору сіток через GPRS або SMS на періодичній основі, наприклад, щотижня або щомісяця.

В альтернативному варіанті мобільний телефон може генерувати контрольну сітку алгоритмічно, а отже, незалежно від комп'ютера, який підтверджує справжність.

Слід зазначити, що форма системи згідно з винаходом, якій на даний час віддають перевагу, залежить від унікальної комбінації конфігурації та

послідовності, забезпечуючи особисту ідентифікаційну конфігурацію (PIR), яка є унікальною для конкретного користувача.

Крім того, також слід зазначити, що застосування сіток, які містять лише квадрати або прямокутники, як було описано вище, не є єдиним варіантом. Фактично можуть використовуватися будь-які мозаїчні форми. Таким чином, правильний багатокутник має 3 або 4 або 5 або більше однакових сторін та кутів. Правильною мозаїкою є мозаїка, яка складається з конгруентних правильних багатокутників. З усіх практичних точок зору, лише три правильні багатокутники укладаються в евклідову площину, тобто, трикутники, квадрати та шестикутники. На Фігурі 5 показано приклади укладених у мозаїку трикутників, квадратів та шестикутників. З цих прикладів можна легко побачити, що квадрати розташовуються в лінію один з одним, на відміну від трикутників та шестикутників. Крім того, якщо шість трикутників утворюють шестикутник, укладання трикутників та укладання шестикутників є подібним, і вони не можуть бути сформовані шляхом прямого укладання фігур в лінію одна під одною - передбачається зміщення. Маючи правильну форму, вони можуть легко використовуватися як еталонна сітка для вибору користувачем його унікальної конфігурації та послідовності.

Існує схема найменування, за допомогою якої ідентифікуються мозаїки. Таким чином, мозаїка з квадратів називається "4.4.4.4". Для цього вибирають вершину, а потім дивляться на один з багатокутників, який торкається цієї вершини, і визначають кількість його сторін. Оскільки він є квадратом, то має чотири сторони, що дає першу цифру "4". Повторення процедури через просування навколо вершини у будь-якому напрямку та визначення кількості сторін багатокутників до повернення до багатокутника, з якого починався відлік, дає кількість нарахованих багатокутників. У разі квадратів існує чотири багатокутники, і кожен має чотири сторони. Остаточною "назвою", таким чином, є 4.4.4.4, як показано на Фігурі 5.

Мозаїка з правильних конгруентних шестикутників ідентифікується як 6.6.6, а мозаїка з трикутників - як 3.3.3.3.3.3, оскільки кожен трикутник має шість багатокутників, які оточують вершину, і кожен має три сторони. Однак винахід також передбачає застосування напівправильних мозаїк, які складаються з утворення правильних багатокутників з ідентичним розташуванням правильних багатокутників при кожній вершині. Приклади напівправильних мозаїк показано на Фігурі 5, з використанням суміші з квадратів та трикутників (3.3.3.4.4 або 3.3.4.3.4), квадратів, трикутників та шестикутників (3.4.6.4); трикутників та шестикутників (3.6.3.6); квадратів та восьмикутників (4.8.8) та більш незвичних комбінацій квадратів, шестикутників та дванадцятигранників (4.6.12).

Незначна перевага використання таких мозаїк полягає в тому, що конфігурація кожної решітки може бути ідентифікована за допомогою унікальної схеми найменування для мозаїк до запиту власної конфігурації та послідовності користувача. Це у разі потреби забезпечує додатковий рівень безпеки системи.

Аспекти безпеки

1. Система, яка є предметом винаходу, складається з кількох компонентів

a. Сітка цифр, відома користувачеві та автентифікаторові

b. При використанні сітки "Craumer Grid", крім цифр, користувачеві та автентифікаторові мають бути відомі орієнтація та "вихідна позиція".

c. "Послідовність" та "конфігурація", які мають бути відомі ВИКЛЮЧНО користувачеві та автентифікаторові.

2. Якщо сітка викрадається, рівень безпеки не знижується, оскільки для успішної автентифікації вимагається як конфігурація, так і послідовність.

3. У разі покупок, якщо і кредитна / дебетова картка, і сітка є вкраденими, рівень безпеки не знижується, оскільки для успішної автентифікації вимагається як конфігурація, так і послідовність.

4. У разі паперових сіток, таких, як "Craumer Grid", якщо конфігурація є відомою третій стороні, то (залежно від потрібного рівня безпеки) сітка також має бути вкраденою або скопійованою. Автентифікатор має врахувати цей ризик, перш, ніж дозволити третій стороні використовувати сітку.

5. Залежно від потрібного рівня безпеки, користувачеві може бути відмовлено у реєстрації конфігурації, які можна легко розпізнати, наприклад, прямих ліній. Автентифікатор може запровадити програмні правила, які дозволяють вибирати лише "обхідні" конфігурації.

6. Може вважатися доцільним використання літер (A-Z) замість цифр або разом з ними з метою збільшення "унікальності" коду транзакції. Однак слід враховувати, що чим більш унікальним є номер, тим більше підказок може мати особа, що підглядає, для визначення конфігурації. Для більшшої безпеки автентифікатор може вирішити, що п'яти- або шестизначний цифровий код є більш надійним, ніж, наприклад, чотиризначний літерно-цифровий код.

7. При будь-якій транзакції (наприклад, у магазині) користувач не повинен повідомляти продавцеві транзакції та "початкової контрольної точки" і показувати йому сітку, оскільки в цьому разі існує ймовірність (хоча й не абсолютна) визначення продавцем конфігурації. Чим більше елементів інформації користувач триматиме у таємниці, тим краще.

8. Для електронних транзакцій має бути створена програма, яка не допускає передачу цифр сітки, ключа конфігурації, початкової контрольної точки та особистої інформації про користувача в одному наборі даних, оскільки це надавало б цінні підказки стосовно конфігурації користувача. Натомість має надсилатися мінімальна кількість даних. Наприклад, квадратики сітки можуть відображатися графічно, а не як набір ASCII знаків.

9. Усі електронні передачі в ідеальному варіанті мають шифруватися.

10. Ідентифікаційні дані (наприклад, код транзакції) мають передаватися лише для автентифікації з прихованим ідентифікатором, який позначає продаж.

Не допускається передача будь-яких інших даних, які можуть дати підказку щодо цифр сітки або конфігурації.

Різні конкретні варіанти способу та пристрою згідно з винаходом далі описуються з посиланням на Фігури з 6 по 12.

На Фігурі 6 показано спосіб онлайнової перевірки згідно з винаходом, який включає генерацію контрольної сітки у терміналі користувача, яким може бути АТМ або комп'ютер користувача, як описано нижче з посиланням на Фігуру 10, або переносний електронний пристрій користувача, такий, як система на базі стільникового телефону, яка описується нижче з посиланням на Фігуру 12.

Сітка може бути генерована алгоритмічним способом або з застосуванням генератора псевдовипадкових чисел. Такі системи є загальновідомими і, таким чином, не потребують детального опису. Генерація чисел не може бути цілком випадковою, оскільки це теоретично могло б створити можливість генерації сітки з довгими рядками однакових цифр, і перевірний рядок у такому разі міг би складатися з однієї цифри. Якщо будь-яка цифра трапляється у сітці більш, ніж середню кількість разів, вона з більшою ймовірністю, ніж інші, має бути частиною конфігурації користувача і, таким чином, може допомогти злодієві вгадати правильну послідовність цифр. Хоча ймовірність відгадування є дуже низькою, ризик відгадування має бути мінімізований через забезпечення появи всіх цифр у сітці 5x5 принаймні двічі, але не більше трьох разів. Може бути бажаним використання сітки, в якій усі цифри можуть траплятися з однаковою частотою. Наприклад, сітка 5x6 має 30 комірок, і, таким чином, кожна цифра може траплятися рівно три рази, що зводить до мінімуму ймовірність вгадування сторонньою особою правильного рядка цифр. Вона може називатися збалансованою сіткою.

Таким чином, стає зрозумілим, що вжиті в цьому описі терміни "псевдовипадковий", "алгоритм" та "алгоритмічно" вказують на процеси, в результаті яких створюється видимість випадковості, але результати не є цілком випадковими, і процес може включати правила кодування, наприклад, на основі додаткових даних. Одним з факторів, задіяних в алгоритмі, може бути, наприклад, ключ шифрування публічних / приватних даних.

Генерована контрольна сітка зберігається у пам'яті у терміналі, хоча показується на надісланій користувачеві запит про введення цифр, які займають позиції у сітці, які відповідають вибраній конфігурації (та послідовності) користувача. Відповіді користувача після цього передаються на автентифікатор разом із сіткою, що зберігається, для порівняння з конфігурацією користувача, яка зберігається у базі даних для автентифікації. Якщо перевірний набір цифр відповідає цифрам у переданій контрольній сітці, ідентифікованій з посиланням на конфігурацію користувача, яка зберігається, дається підтвердження, а за інших обставин дається відмова.

Як можна побачити, секретна особиста конфігурація користувача не передається за межі комп'ютера, який підтверджує справжність. Однак, хоча дані, які передаються від терміналу користувача на автентифікатор, мають бути зашифровані, якщо хакер їх перехопить і розшифрує, він матиме

доступ до ключа до особистої конфігурації користувача, ввівши рядок у сітку. Спосіб, який пояснюється на Фігурі 7, забезпечує один шлях уникнення цього можливого недоліку. На початку транзакції термінал користувача контактує з окремою базою даних сіток, яка надсилає на термінал контрольну сітку, алгоритмічно вибрану з великої кількості сіток, які зберігаються у базі даних. Контрольна сітка містить унікальний ідентифікаційний код. Транзакція продовжується по суті у такий самий спосіб, як показано на Фігурі 6, за винятком того, що контрольна сітка не передається на автентифікатор; натомість надсилається ідентифікаційний код сітки, і він застосовується автентифікатором для знаходження сітки серед окремої бази даних сіток для етапу порівняння.

Згідно зі способом, показаним на Фігурі 8, автентифікатор спочатку надсилає користувачеві велику сітку цифр, причому ця сітка є значно більшою, ніж контрольна сітка, яка використовується для транзакції (як правило, сітка 5x5 або 7x7). Надсилання нової великої сітки на термінал може здійснюватися з регулярними інтервалами, можливо, автоматично, і використовувана сітка зберігається автентифікатором у базі даних сіток для контролю. На початку транзакції автентифікатор вказує користувачеві псевдовипадково генеровані координати початкової точки на сітці для терміналу для того, щоб з великої сітки можна було вибрати контрольну сітку. Наприклад, сітка 5x5 може бути вибрана з використанням координат сітки як верхній лівий кут. Термінал користувача має лише передати автентифікаторові цифри, введені користувачем у відповідь на запит про перевірне порівняння, яке має здійснюватись автентифікатором.

Слід розуміти, що хоча кожен з цих способів описується з посиланням лише на передачу цифр, введених користувачем, у разі необхідності - з іншими ідентифікаторами сітки, вони обов'язково супроводжуються певним номером рахунку або іншим особистим ідентифікатором, що підлягає перевірці.

У варіанті способу, показаного на Фігурі 8, термінал користувача сам псевдовипадково вибирає координати початкової точки на сітці на початку транзакції, і вони передаються разом з цифрами запиту користувача автентифікаторові, який після цього може знайти контрольну сітку у сітці, яка зберігається, для терміналу користувача.

В іншому варіанті цього способу термінал користувача застосовує простий алгоритм для генерації з великої сітки, яка складається, скажімо, з 1000 цифр, контрольної сітки, скажімо, з 25 цифр, які не є окремим суміжним фрагментом великої сітки. Цей спосіб має перевагу, яка полягає в тому, що від цього алгоритму не вимагається цілкомітої безпеки. Наприклад, користувачеві раз на місяць автентифікатором може надсилатися віртуальна велика сітка цифр. Оскільки автентифікатор знає і алгоритм, і віртуальну сітку, він може визначати, які цифри слід очікувати. Якщо ж алгоритм стає відомим, хакер не отримує доступу до віртуальної сітки, яка має бути різною для кожної особи і регулярно змінюється. Так, якщо у найгіршому випадку хакер може дізнатися про позицію на віртуальній сітці, яка має використовуватися для генерації

контрольної сітки, він не дізнається про цифри, які займають конкретну віртуальну сітку, і, таким чином, не зможе генерувати контрольну сітку.

В іншому варіанті замість великої сітки термінал користувача отримує від автентифікатора певну кількість контрольних сіток так само, як для великої сітки, причому кожна сітка містить ідентифікатор. Після цього на початку транзакції автентифікатор може вказати на термінал користувача сітку, яка має використовуватися, шляхом передачі відповідного ідентифікатора, або термінал користувача може алгоритмічно вибрати одну з сіток і надіслати її ідентифікатор разом із цифрами, введеними у відповідь на запит.

Фігура 9 показує ще один підхід. Місцевий термінал є пристосованим для запускання на початку транзакції алгоритму, який використовує дату та час дня та ідентифікатор терміналу та/або особи для генерації псевдовипадкового рядка цифр. Загальновідомим є застосування таких алгоритмів для захисту персональних комп'ютерів або персональних інформаційних пристроїв (PDA), користувач має ручну електронний шифрувальний пристрій, який показує номери ключа, які змінюються з регулярними інтервалами. Пристрій, який має бути захищений, застосовує такий самий алгоритм, використовуючи такі самі вихідні дані, для внутрішньої генерації таких самих цифр синхронно з шифрувальним пристроєм. Користувач вводить номер ключа для розблокування комп'ютера або PDA. У даному варіанті цей тип алгоритму має бути розширеним для генерації, скажімо, 25-цифрового ключа замість 5- або 6-цифрового, який традиційно застосовується, і для заповнення контрольної сітки цими цифрами. Алгоритм може використовувати ключові дані, такі, як ідентифікатор терміналу, особистий ідентифікатор та номер рахунку, номер мобільного телефону, якщо термінал є мобільним телефоном, або їх комбінації. Автентифікатор застосовує такий самий алгоритм для генерації такого самого 25-цифрового рядка на основі таких самих ключових даних та позначки часу транзакції. Таким чином, перевірка може здійснюватися без необхідності у передачі будь-якої інформації про сітку. Як альтернативу застосуванню позначки часу алгоритм може розрахувати сітку на основі попереднього часу, а також поточного часу і використовувати два показники (або насправді кілька, залежно від широти часу, яка допускається системою) для того, щоб визначити, чи створює будь-який з них відповідність конфігурації для перевірки справжності.

Слід розуміти, що можуть застосовуватися гібридні способи між цим способом та іншими описаними способами. Наприклад, алгоритм генерації чисел може застосовуватися для генерації коду, який ідентифікує сітку, яка має бути вибрана з окремої бази даних або з-поміж багатьох сіток, які попередньо було збережено у терміналі, після цього автентифікатор запускає алгоритм з такими самими початковими числами для генерації коду та визначення, таким чином, правильної сітки для порівняння.

Фігура 10 показує типовий пристрій, який застосовується в онлайнній транзакції. Термінал користувача, яким може бути, наприклад, АТМ або

навіть персональний комп'ютер, має центральний процесор 100, з'єднаний з дисплеєм 101, цифрову клавіатуру 102 та пристрій для зчитування карток 103. Під'єднання до мережі 104, наприклад, через Інтернет, представлений як 105, веде до процесора автентифікації транзакції 106, під'єднаного до бази даних 107, у якій зберігаються деталі про користувача та пов'язана з ним особиста ідентифікаційна конфігурація (PIR). Для початку транзакції користувач вставляє персональну картку 108, наприклад,дебетову або кредитну картку, у зчитувальний пристрій 103. Номер рахунку користувача зчитується з картки, і потім термінал генерує контрольну сітку 109, наприклад, з 25 квадратиків, яка містить псевдовипадково генеровані цифри від 0 до 9, і показує її на дисплеї 101, пропонуючи користувачеві ввести на клавіатурі 102 цифри, які займають PIR користувача у сітці. Після цього термінал встановлює з'єднання з процесором автентифікації транзакції 106 для передачі у шифрованій формі номера рахунку користувача, суми транзакції, цифр, введених користувачем, та контрольної сітки. По отриманню цих даних процесор автентифікації 106 використовує номер рахунку для знаходження у базі даних 107 PIR користувача та даних кредиту / рахунку. Після цього здійснюється перевірка, як описано вище з посиланням на Фігуру 6, і якщо справжність підтверджується, і транзакція в цілому є прийнятною, процесор автентифікації 106 надсилає назад на термінал код дозволу для того, щоб термінал міг завершити транзакцію.

Фігура 11 показує пристрій, який виконує варіант цієї процедури, як описано з посиланням на Фігуру 7. При цьому додається окремий процесор контрольної сітки ПО, який має базу даних 111 контрольних сіток, кожна з яких має пов'язаний з нею унікальний ідентифікатор. Процесор сітки ПО може бути віддаленим як від терміналу користувача, так і від процесора автентифікації 106, і з'єднання між ними може відбуватися через мережний канал 112, наприклад, через Інтернет 105.

Фігура 12 показує інший варіант втілення, у якому мобільний або стільниковий телефон користувача 120 служить як термінал користувача. У цьому разі телефон 120 також зберігаються деталі про особу та рахунок користувача, замість їх зберігання на окремій картці транзакції. Процес може бути таким, як описано з посиланням на будь-яку з Фігур з 6 по 9, з передачами на процесор автентифікації та від нього, які здійснюються у безпроводний спосіб, наприклад, з застосуванням будь-якої з радіомереж або способів передачі даних, таких, як GPRS.

Фігура 13 є блок-схемою ще одного способу, який є вдосконаленням способу, що пояснюється на Фігурі 9. Після генерації сітки за допомогою алгоритму та введення користувачем відповідного рядка застосовується інший алгоритм для генерації на основі відповідного рядка та одного або кількох ідентифікаторів, згаданих у зв'язку зі способом, описаним з посиланням на Фігуру 9, "пароля", наприклад, у формі десятизначного числа (або, можливо, рядка з літер та цифр), який маскує відповідь, але у спосіб, який може бути розпізнаний органом засвідчення, який має доступ до цих іден-

тифікаторів. Після цього пароль передається до органу засвідчення разом з принаймні одним з ідентифікаторів.

Орган засвідчення тимчасово зберігає пароль, застосовуючи такий самий алгоритм та ідентифікатор(и) для розрахунку такого самого 25-цифрового рядка для відтворення контрольної сітки. Секретна конфігурація користувача відшукується у базі даних конфігурацій і застосовується для вибору з контрольної сітки очікуваної правильної відповіді. На кінцевому етапі ця очікувана відповідь (скажімо, рядок з 4 цифр) вводиться в алгоритм пароля з використанням необхідних ідентифікаторів, принаймні один з яких було передано з паролем від користувача, для розрахунку пароля. Потім він може бути порівняний з переданим паролем. Якщо вони є однаковими, справжність підтверджується, а за інших обставин транзакція відхиляється.

Варіант цього процесу може застосовуватися для захисту передачі повідомлень електронною поштою. Відправник запускає на своєму терміналі електронної пошти процес перевірки, який може базуватися, наприклад, на ідентифікаторах, які зберігаються в його терміналі (наприклад, персональному комп'ютері або переносному пристрої зв'язку). Він генерує контрольну сітку, застосовуючи алгоритм генерації чисел, як описано з посиланням на Фігури 9 та 13. Після цього відповідь перетворюється на пароль, як описано з посиланням на Фігуру 13, причому пароль також кодує дату та час передачі. Пароль вставляється у повідомлення електронною поштою і передається адресатові. Після цього адресат запускає відповідний процес перевірки, в якому використовується доданий ключ для підтвердження справжності відправника, згідно з попередньо збереженою інформацією. Дата та час передачі, як вказано у повідомленні електронною поштою, використовуються за допомогою процесу перевірки для відтворення пароля, який виконується у спосіб, описаний з посиланням на Фігуру 13, і якщо паролі не збігаються, то це є свідченням того, що електронне повідомлення було підроблено або не було надіслане відповідним відправником.

Фігура 14 показує спосіб та пристрій для автономної місцевої перевірки з застосуванням терміналу та платіжної картки. Він є подібним до того, який застосовують у даний час у супермаркетах та ресторанах під назвою "Chip & PIN", коли PIN-код перевіряється на місці пристроєм для зчитування карток з кредитною або дебетовою картою; у цьому разі немає потреби у безпосередньому з'єднанні з віддаленим комп'ютером, який дає дозвіл. У способі та пристрої згідно з цим аспектом винаходу користувач вставляє платіжну картку у термінал, у разі типової контактної картки, таким чином, щоб встановити електричне з'єднання з електронним чіпом, включеним у картку. Однак

слід зазначити, що подібний спосіб може здійснюватися й з безконтактною картою, яка забезпечує індуктивний або безпроводний зв'язок. Термінал у цьому разі перевіряє цілісність картки, перевіряючи певні основні характеристики картки. Після успішного завершення цього етапу машина видає запит, представляючи користувачеві контрольну сітку з цифр і пропонує користувачеві ввести код відповіді, який складається з цифр у сітці, які займають позиції в особистій конфігурації та послідовності користувача. Термінал надсилає відповідь на чіп картки, разом з контрольними цифрами, для перевірки.

Картка використовує контрольну сітку, відповідні номери та конфігурацію користувача, яка зберігається (зберігається лише у чіпі картки і не повідомляється за межами чіпа) для того, щоб визначити, чи відповідає відповідь правильній конфігурації у контрольній сітці, а потім повертає дійсне або недійсне повідомлення на термінал. Якщо повідомлення, отримане у терміналі, вказує на дійсну відповідь, платіж приймається. Слід зазначити, що у разі онлайнового терміналу, наприклад, АТМ, отримання дійсного повідомлення запускає передачу на комп'ютер, який дає дозвіл, деталей рахунку та суми транзакції з запитом про дозвіл.

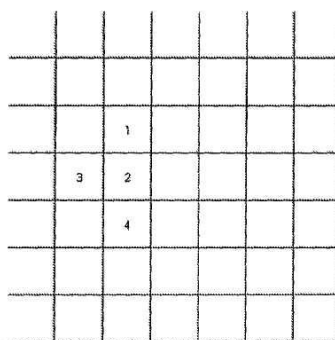
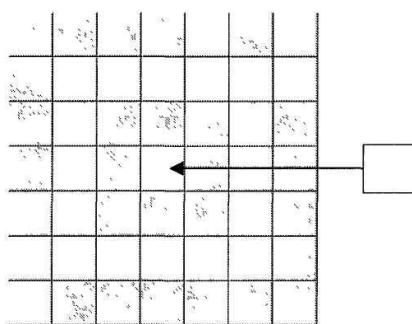
Фігура 15 показує пристрій, який по суті є таким самим, що й на Фігурі 10, але виконаний без пристрою для зчитування карток для онлайнових транзакцій, і показує ще один аспект винаходу, в якому користувач може отримувати підтвердження справжності організації, яка здійснює онлайнову транзакцію, наприклад, банку, таким чином, уникаючи ризику стати жертвою "фішингу". Для того, щоб пересвідчитись у тому, що ця організація є справжньою організацією, в якій користувач первісно зареєстрував свої особисті дані, частина процесу реєстрації включає вибір користувачем особистої конфігурації та послідовності позицій у сітці та реєстрацію цієї особистої конфігурації в організації. Також має бути зареєстрований особистий ідентифікаційний номер (PIN) користувача. Під час транзакції користувач спочатку ідентифікує себе, наприклад, за прізвищем, застосовуючи клавіатуру 150. Процесор автентифікації 106 знаходить особисту конфігурацію користувача та PIN у базі даних 107 і забезпечує генерацію сітки з псевдовипадкових чисел, в яку включається PIN користувача у позиціях особистої конфігурації користувача. На Фігурі 15, PIN користувача 5946, вказаний в особистій конфігурації користувача, є виділеним, але на практиці, звичайно, він жодним чином не відрізняється від навколишніх псевдовипадкових цифр. Після цього користувач може підтвердити, що PIN дійсно показується у правильних позиціях на сітці, перш, ніж продовжувати транзакцію.

33

90371

34

ФІГ. 1



ФІГ. 2

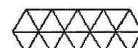
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	3	5	7	9	4	7	3	2	0	2	7	4	9	7	8	8	4
2	5	3	5	7	9	5	6	4	8	0	1	2	4	2	7	9	4
3	0	4	7	9	4	9	4	9	3	0	3	8	2	8	2	1	9
4	8	2	6	7	4	8	0	4	7	4	8	0	9	8	4	6	3
5	0	3	2	6	2	6	6	7	5	8	0	4	6	4	3	2	5
6	5	5	6	7	8	4	2	6	2	6	8	0	4	6	2	1	8
7	1	1	4	6	4	8	7	9	8	5	4	2	1	4	2	0	7
8	2	4	8	2	4	5	6	1	7	9	1	5	2	1	5	6	4
9	4	6	8	4	1	0	2	0	4	0	4	5	2	4	1	5	1
10	8	7	4	8	5	6	3	7	1	7	9	0	5	0	4	7	5
11	7	3	4	7	5	1	0	1	4	5	1	8	4	5	1	5	1
12	0	5	0	7	5	1	5	7	1	8	7	1	5	0	4	4	0

ФІГ. 4

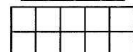
ФІГ. 3

1	8	4	9	6	5	4
9	9	4	6	2	7	3
1	7	5	8	2	7	2
3	7	1	0	1	0	9
5	4	8	9	3	7	2
6	3	2	3	7	9	9
7	1	8	6	7	8	9

мозаїка з трикутників



мозаїка з квадратів



мозаїка з шестикутників



4.4.4.4



6.6.6



3.3.3.3.3.3



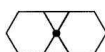
3.3.3.4.4



3.3.4.3.4



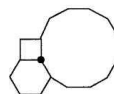
3.4.6.4



3.6.3.6

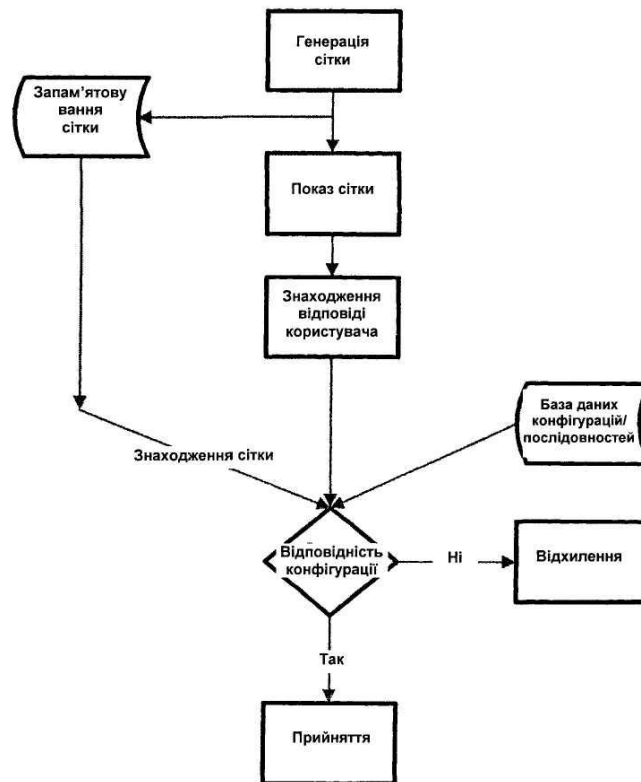


4.8.8

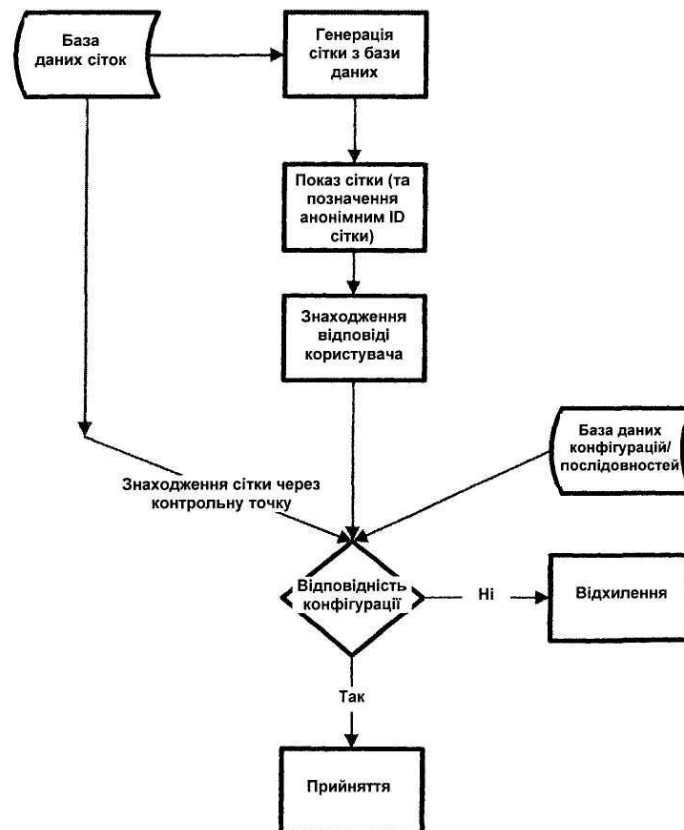


4.6.12

ФІГ. 5

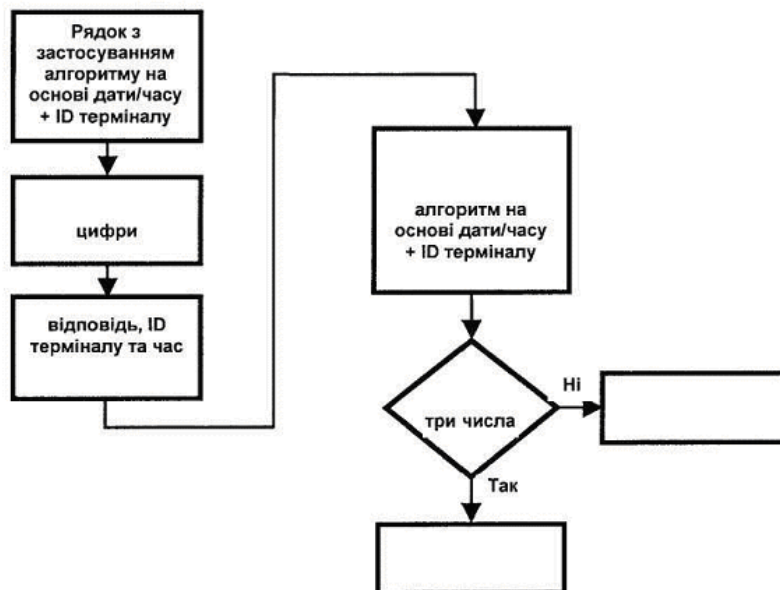
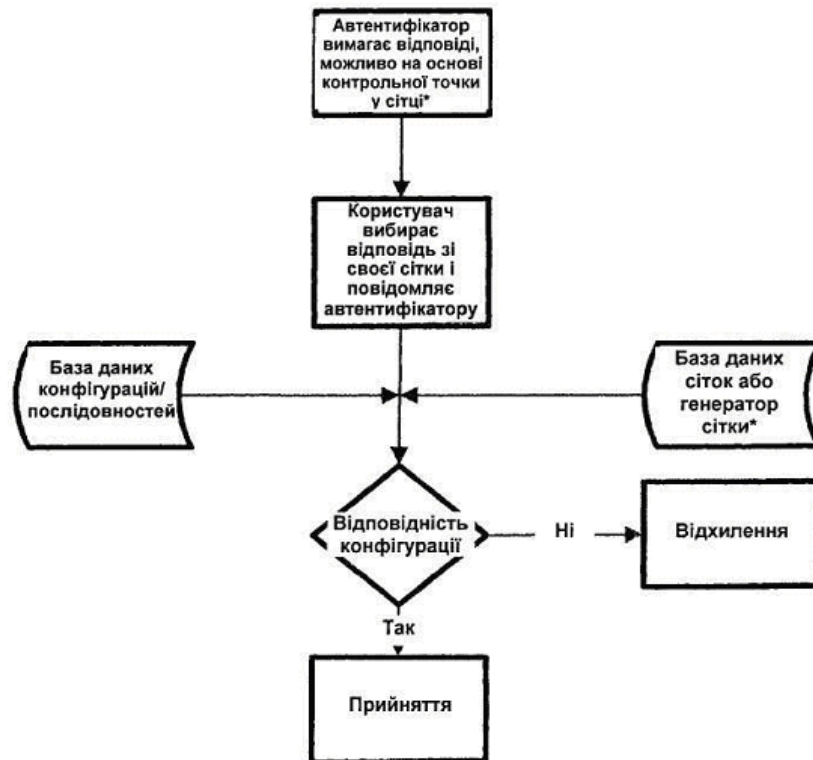


ФІГ. 6



ФІГ. 7

ФІГ. 8



ФІГ. 9

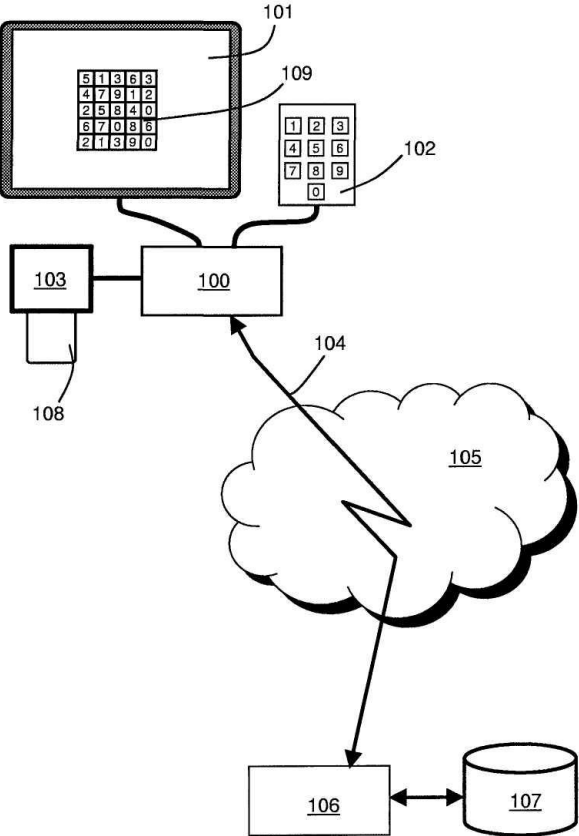


FIG. 10

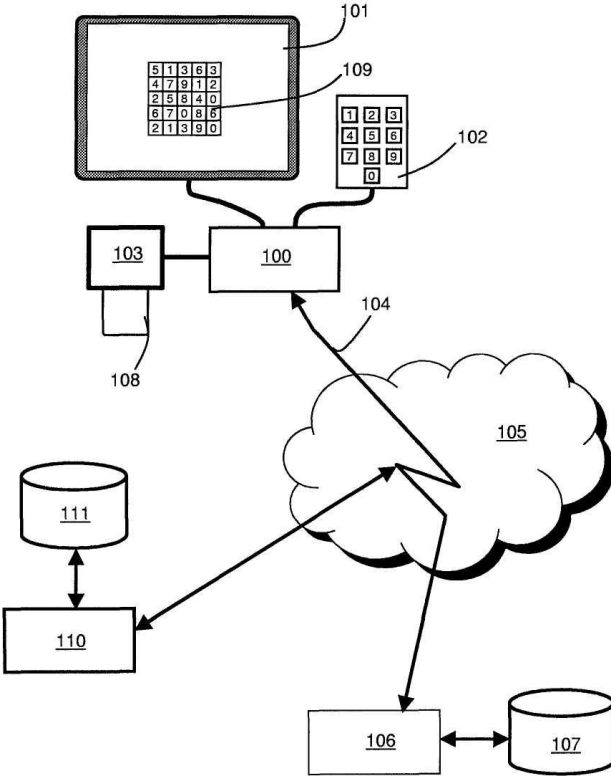
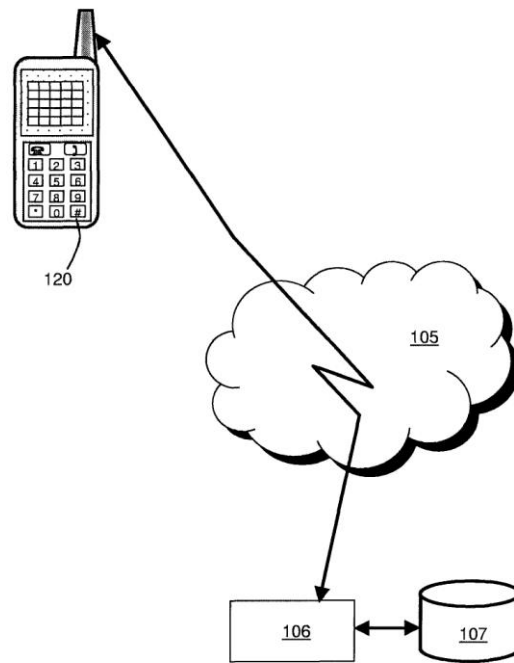
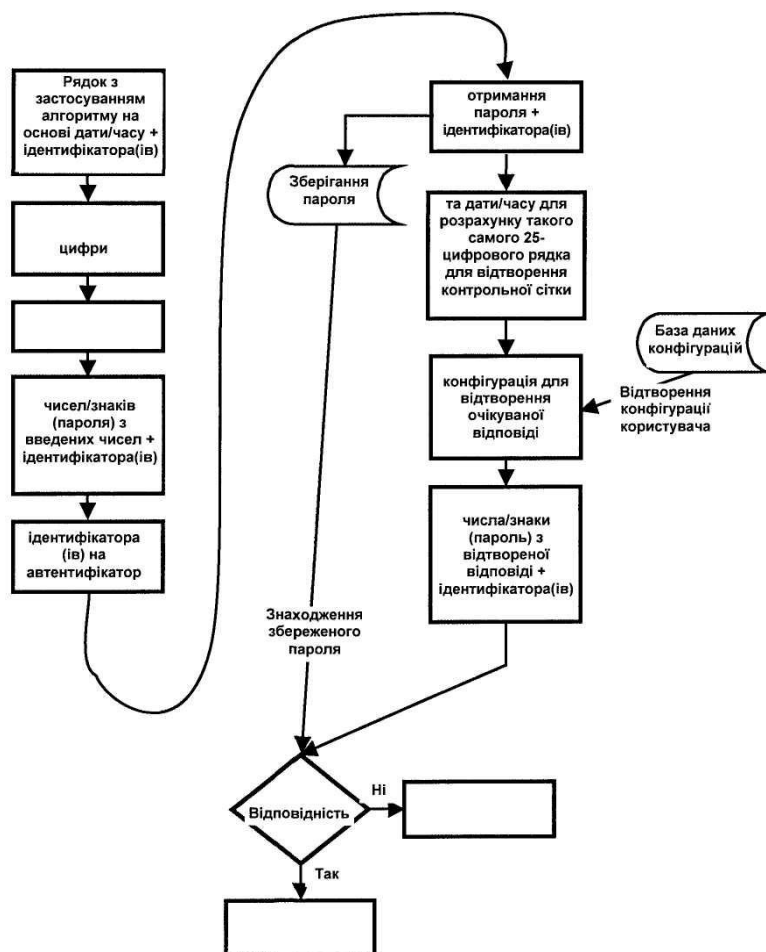


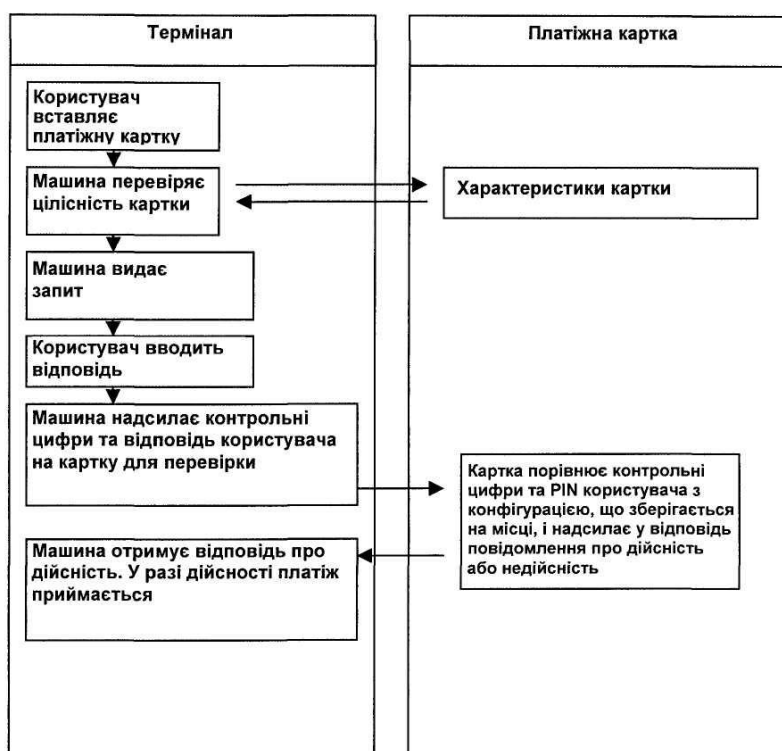
FIG. 11



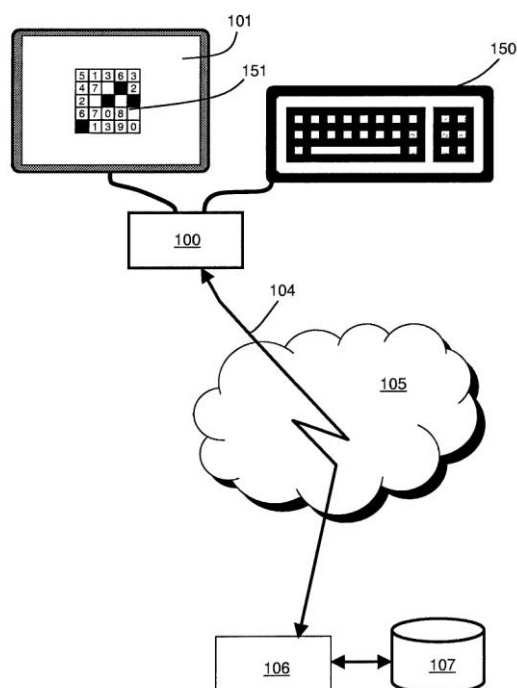
ФІГ. 12



ФІГ. 13



ФІГ. 14



ФІГ. 15