



УКРАЇНА

(19) UA (11) 91031 (13) C2
(51) МПК (2009)
G06K 17/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(54) СПОСОБИ ТА СИСТЕМИ ДЛЯ МАРКУВАННЯ, ВІДСТЕЖУВАННЯ ТА АВТЕНТИФІКУВАННЯ ВИРОБІВ

1

2

(21) а200704331

(22) 29.09.2005

(24) 25.06.2010

(86) РСТ/В2005/003103, 29.09.2005

(31) 04104954.5

(32) 08.10.2004

(33) EP

(46) 25.06.2010, Бюл.№ 12, 2010 р.

(72) САЖЕ АЛЕН, СН, ШАТЕЛЕН ФІЛІПП, СН,
ФРАДЕ ЕРВАН, СН, ВАЙСС ЖАК, СН, ШЕМЛА
МАРК, СН

(73) ФІЛІП МОРРИС ПРОДАКТС С.А., СН

(56) DE 10100248 A1; 11.07.2002

US 6442276 B1; 27.08.2002

(57) 1. Спосіб маркування виготовлених виробів, який включає: надання множини секретних кодів у контрольний центр та на виробничу лінію виготовлення виробів, генерування ідентифікаційного коду для кожного виробленого виробу, підписування у цифровому вигляді кожного ідентифікаційного коду за допомогою секрету, який отримують з множини секретних кодів та який є відомим у контрольному центрі, і маркування кожного виготовленого виробу згаданим підписаним ідентифікаційним кодом.

2. Спосіб за п. 1, який включає застосування прихованого маркера або лазерного пристрою при виконанні операції маркування.

3. Спосіб за п. 1 або п. 2, який відрізняється тим, що згадана множина секретних кодів являє собою заздалегідь обчислені випадкові коди.

4. Спосіб за будь-яким із пп. 1-3, який відрізняється тим, що надання множини секретних кодів включає фізичне передавання енергонезалежного носія даних, на якому записані секретні коди.

5. Спосіб за будь-яким із пп. 1-4, який відрізняється тим, що згаданий секрет, отриманий зі згаданої множини секретних кодів, отримують на кожній з множини виробничих ліній.

6. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що частина згаданого секрету передається генератором коду у контрольний центр за допомогою захищеного мережевого зв'язку.

7. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що множина секретних кодів являє собою масив випадкових кодів, та який

включає: генерування індексу, пов'язаного з виготовленням одного або більше виробів, передавання цього індексу у контрольний центр, отримання секрету генератором коду з масиву випадкових кодів та з індексу, а також підписування у цифровому вигляді кожного ідентифікаційного коду для кожного виготовленого виробу з кодом шуму, отриманим шляхом шифрування копії ідентифікаційного коду із секретом.

8. Спосіб за п. 7, який відрізняється тим, що секрет додатково отримують з ідентифікаційного коду.

9. Спосіб за будь-яким із пп. 1-8, який відрізняється тим, що включає передавання додаткової інформації стосовно виготовлених виробів у контрольний центр.

10. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що згаданий контрольний центр керується довіреною третьою стороною, незалежною від виробника виготовлених виробів.

11. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що згадане маркування виконують на упаковці згаданого виготовленого виробу.

12. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що ідентифікаційний код включає в себе щонайменше один з таких елементів: ідентифікатор місця виготовлення, ідентифікатор виробничої лінії, ідентифікатор генератора коду, ідентифікатор виробу, і інформацію про час.

13. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що включає шифрування ідентифікаційного коду.

14. Спосіб за будь-яким із попередніх пунктів, який відрізняється тим, що згаданий виріб являє собою пачку, блок або коробку сигарет.

15. Виготовлений виріб із маркуванням, виконаним із застосуванням способу за будь-яким із попередніх пунктів.

16. Спосіб автентифікування виробу з маркуванням, виконаним із застосуванням способу за будь-яким із пп. 1-14, який включає: передавання підписаного ідентифікаційного коду у контрольний центр, та автентифікування підписаного ідентифікаційного коду у контрольному центрі.

17. Спосіб за п. 16, який відрізняється тим, що включає: маркування на кожному виготовленому

(13) C2

(11) 91031

(19) UA

виробі частини інформації, що міститься у ідентифікаційному коді цього виробу, і перевірку відповідності інформації з обробленою інформацією, переданою повторно контрольним центром.

18. Спосіб за п. 16, який **відрізняється** тим, що включає повторне передавання контрольним центром додаткової інформації, пов'язаної з переданим ідентифікаційним кодом.

19. Спосіб за будь-яким із пп. 16-18, який **відрізняється** тим, що включає виявлення клонованих кодів у контрольному центрі.

20. Контрольний центр для автентифікування виробу із застосуванням способу за п. 16, п. 17 або п. 18.

21. Система для маркування виготовлених виробів, яка включає в себе: генератор для генерування масивів секретних кодів, виробничу лінію для виготовлення виробів, що підлягають маркуванню, яка включає в себе: генератор коду для генерування ідентифікаційного коду для кожного виготовленого виробу, пристрій для цифрового підписування ідентифікаційних кодів із секретом, отриманим із секретних кодів, передавач даних для передавання секрету у контрольний центр, і пристрій для маркування кожного виготовленого виробу підписаним ідентифікаційним кодом.

22. Система за п. 21, яка **відрізняється** тим, що згаданий пристрій для маркування включає в себе принтер або лазерний пристрій.

23. Система за п. 21 або п. 22, яка **відрізняється** тим, що виробничу лінію призначена для виготовлення тютюнових виробів.

24. Система за п. 21, п. 22 або п. 23, яка **відрізняється** тим, що генератор включає в себе пристрій записування даних для записування масиву секретних кодів на енергонезалежному носії даних.

25. Система за будь-яким із пп. 21-24, яка **відрізняється** тим, що контрольний центр включає в себе інтерфейс для приймання текстових або цифрових запитів із мережі та для передавання відповідей через мережу.

26. Система за будь-яким із пп. 21-25, яка **відрізняється** тим, що генератор для генерування масиву секретних кодів являє собою генератор "солі".

27. Система за будь-яким із пп. 21-26, яка **відрізняється** тим, що виробничу лінію 101 включає в себе датчик для виявлення нанесених підписаних ідентифікаційних кодів.

28. Спосіб автентифікування виготовленого виробу, який включає: генерування коду та підписування згаданого коду цифровим підписом у генераторі коду, маркування виробу підписаним кодом, передавання підписаного коду у контрольний центр через мережу загального користування для автентифікування, автентифікування цифрового підпису контрольним центром, добування значення коду у контрольному центрі, і передавання значення користувачеві через мережу загального користування.

29. Спосіб за п. 28, який **відрізняється** тим, що коди, згенеровані генератором коду, не зберігаються.

30. Спосіб за п. 28 або п. 29, який **відрізняється** тим, що код підписаний із секретом, який спільно

використовується генератором коду та контрольним центром.

31. Спосіб за п. 30, який **відрізняється** тим, що секрет виділяють із масиву секретних кодів, які спільно використовуються генератором коду та контрольним центром, а також модифікують протягом роботи генератора коду.

32. Спосіб за п. 30 або п. 31, який **відрізняється** тим, що згаданий секрет є різним для кожного виготовленого виробу.

33. Спосіб контролювання обсягу виготовлених виробів, маркованих із застосуванням способу за будь-яким із пп. 1-14, який включає: збирання інформації про обсяги виробництва у контрольному центрі, і надання інформації про обсяги виробництва користувачеві.

34. Спосіб за п. 33, який **відрізняється** тим, що інформацію про обсяги виробництва отримують з ідентифікаційних кодів, переданих у контрольний центр.

35. Спосіб відстежування виробу з маркуванням, виконаним із застосуванням способу за будь-яким із пп. 1-14, який включає: передавання підписаного ідентифікаційного коду у контрольний центр, автентифікування підписаного ідентифікаційного коду у контрольному центрі, та повторне передавання інформації відстежування, пов'язаної з ідентифікаційним кодом, користувачеві.

36. Спосіб за п. 34, який **відрізняється** тим, що інформацію відстежування отримують із переданих у контрольний центр ідентифікаційних кодів виготовлених виробів.

37. Спосіб за будь-яким із пп. 32-35, який **відрізняється** тим, що включає ідентифікування користувача.

38. Спосіб за будь-яким із пп. 33-37, який **відрізняється** тим, що включає операцію заборони надання інформації користувачам, які не належать до попередньо визначеної групи привілейованих користувачів.

39. Спосіб автентифікування виготовлених виробів, який включає маркування виробів шляхом: надання множини секретних кодів у контрольний центр та на виробничу лінію виготовлення виробів, генерування ідентифікаційного коду для кожного виготовленого виробу, підписування у цифровому вигляді кожного ідентифікаційного коду за допомогою секрету, який отримують із множини секретних кодів та який є відомим у контрольному центрі, та маркування кожного виготовленого виробу згаданим підписаним ідентифікаційним кодом, а також автентифікування виготовленого виробу на запит шляхом перевірки секрету у контрольному центрі.

40. Система автентифікування виготовлених виробів, яка включає в себе: систему для маркування виготовлених виробів, яка включає в себе: генератор для генерування масивів секретних кодів, виробничу лінію для виготовлення виробів, що підлягають маркуванню, яка включає в себе: генератор коду для генерування ідентифікаційного коду для кожного виготовленого виробу, пристрій для цифрового підписування ідентифікаційних кодів із секретом, отриманим із секретних кодів, передавач даних для передавання секрету у контрольний центр, та маркувальний пристрій для ма-

ркування кожного виготовленого виробу згаданим підписаним ідентифікаційним кодом, причому система автентифікування додатково включає в себе

контрольний центр для автентифікування виготовленого виробу на запит шляхом перевірки секрету.

Винахід стосується маркування, відстежування та автентифікування товарів, зокрема, але не виключно, упакованих товарів, наприклад, пачок, блоків або коробок сигарет та інших тютюнових виробів. Винахід також стосується контролю за процесом виробництва.

Передумови створення винаходу

Контрабандний товар та підробки спричиняють значні втрати доходів як для виробників товарів, що продаються, так і для державних органів. Крім того, незаконний продаж підроблених товарів низької якості є небажаним як для покупця, так і для виробника.

Законно виготовлені товари також можуть бути незаконно імпортовані або продані, наприклад, для уникнення сплати податків або виконання інших національних норм. Таким чином, серйозною проблемою у багатьох зонах торгівлі є виявлення та перекривання каналів несанкціонованого паралельного імпорту.

Проблеми контрабанди та підробок є особливі гострими для товарів, що підлягають спеціальному оподаткуванню, таких як тютюнові вироби. Вони також існують і для багатьох інших видів виробів, що продаються, і мають значну вартість торгової марки, зокрема, для тих виробів, що продаються на міжнародному ринку, таких як парфумерія, алкогольні напої, годинники та предмети розкошу взагалі.

Серйозною проблемою для виробників таких виробів є розробка способів надійного маркування справжніх виробів таким чином, щоб забезпечити однозначну ідентифікацію підроблених виробів та виявлення незаконного імпорту.

Загальною практикою є ідентифікування товарів, що продаються, за кодом виробника або серійним номером, видавленим або надрукованим на упаковці, наприклад, пачці або блоці сигарет. Такий код за певних умов уможливив ідентифікування місця виготовлення а також відстежування торговельного ланцюжка для конкретного виробу. Такі відомості є корисними для ідентифікування контрабандних виробів.

Обмеженням такої практики є те, що розшифрування та перевірка цих кодів виробника можуть виявитися трудомісткими та незручними. Наприклад, автентифікування може вимагати, щоб кожний код виробника, нанесений на виготовлений виріб, був записаний у базу даних та/або вимагати передавання великого обсягу конфіденційних даних із місця виготовлення до центральної бази даних. Ці вимоги можуть погіршувати надійність та безпеку.

Іншим обмеженням цієї практики є те, що коди виробників легко можуть бути імітовані або клоновані. Для того, щоб частково усунути це обмеження, відомий спосіб, що полягає у додаванні прихо-

ваного маркера до фарби, що застосовується для друкування коду виробника на упаковці. Підроблені вироби, на які нанесені клони дійсних кодів, за такої умови виявляються за відсутністю цього прихованого маркера. Ступінь безпеки, що забезпечується цим способом, повністю залежить від здатності контролювати джерела та наявність цього маркера.

Метою цього винаходу є усунення недоліків відомих способів, описаних вище.

Відповідно до винаходу створений спосіб маркування виготовлених виробів, який включає: надання множини секретних кодів у контрольний центр та на виробничу лінію виготовлення виробів; генерування ідентифікаційного коду для кожного виготовленого виробу; підписування у цифровому вигляді кожного ідентифікаційного коду за допомогою секрету, який отримують із множини секретних кодів та який є відомим у контрольному центрі; і маркування кожного виготовленого виробу згаданим підписаним ідентифікаційним кодом.

Винахід також передбачає спосіб автентифікування виробу з маркуванням, виконаним із застосуванням способу, описаного вище, що включає передавання згаданого підписаного ідентифікаційного коду у контрольний центр; і автентифікування цього ідентифікаційного коду у контрольному центрі.

Винахід також передбачає систему маркування виготовлених виробів, яка включає в себе: генератор для генерування масивів секретних кодів; а також виробничу лінію для виготовлення виробів, що підлягають маркуванню, яка включає в себе: генератор коду для генерування ідентифікаційного коду для кожного виготовленого виробу; пристрій для цифрового підписування ідентифікаційних кодів із секретом, отриманим із секретних кодів; передавач даних для передавання секрету у контрольний центр; і пристрій для маркування кожного виготовленого виробу підписаним ідентифікаційним кодом.

Винахід також передбачає спосіб автентифікування виготовленого виробу, яка включає в себе: генерування коду та підписування згаданого коду цифровим підписом у генераторі коду; маркування виробу підписаним кодом; передавання підписаного коду у контрольний центр через мережу загального користування; автентифікування цифрового підпису контрольним центром; добування значення коду у контрольному центрі; і передавання одержаного значення користувачеві через мережу загального користування.

Інший аспект цього винаходу полягає у способі контролювання обсягу виготовлених виробів, маркованих із застосуванням способу, описаного вище, що включає: збирання інформації про обсяги виробництва у контрольному центрі; а також на-

дання інформації про обсяги виробництва користувачеві.

Винахід також передбачає спосіб відстежування виробу з маркуванням, виконаним із застосуванням способу, описаного вище, що включає: передавання підписаного ідентифікаційного коду у контрольний центр; автентифікування цього ідентифікаційного коду у контрольному центрі; а також передавання інформації відстежування, пов'язаної з ідентифікаційним кодом, користувачеві.

Варіанти здійснення різних аспектів винаходу мають перевагу, яка полягає у тому, що маркування та автентифікування може бути доступною та перевіреною віддалено через звичайну мережу, таку як звичайний або мобільний телефон. Такі маркування та автентифікування мають додаткову перевагу, яка полягає у тому, що вони не можуть бути порушені виробниками підроблених виробів. Крім того, справжність виготовленого виробу при продажу може бути легко перевірена, наприклад, протягом кількох секунд на місці продажу.

Варіанти здійснення аспектів винаходу мають додаткову перевагу, яка полягає у тому, що можуть бути виявлені клоновані коди та несанкціоновані копії кодів, а також у тому, що можуть контролюватися обсяги виробництва, наприклад, визначеного виробника, у визначеному місці виготовлення або на виробничій лінії.

Варіанти здійснення аспектів винаходу мають додаткову перевагу, яка полягає у тому, що вони можуть бути застосовані для заміни системи акцизних марок, що застосовується у багатьох країнах для збирання податків, наприклад, на тютюнові вироби.

Далі варіанти здійснення винаходу описані лише як приклад із посиланнями на прикладені фігури, на яких:

Фіг.1 являє собою схематичне зображення системи для маркування та автентифікування відповідно до винаходу;

На Фіг.2 схематично показаний формат маркувального коду відповідно до винаходу;

Фіг.3 являє собою блок-схему, яка показує структуру генерування коду відповідно до винаходу;

Фіг.4 являє собою блок-схему, яка показує структуру автентифікування коду відповідно до винаходу.

Як показано на Фіг.1, вироби, що підлягають маркуванню, виготовляють на одній або більше виробничих лініях 101, 102. Кожна виробнича лінія являє собою комплекс виробничого обладнання для одного або більше виготовлюваних виробів. Наприклад, виробнича лінія може являти собою лінію для виготовлення та пакування сигарет, де виготовлюваними виробами є, наприклад, пачки, блоки та коробки сигарет щонайменше однієї марки. Виробництво може бути організоване партіями. Кожна партія передбачає виготовлення визначеної кількості ідентичних виготовлюваних виробів, наприклад, пачок, блоків та коробок сигарет конкретної марки та виду.

Якщо наявні дві або більше виробничих ліній, то ці лінії можуть бути фізично розташовані у одному місці 10 виготовлення або на різних вироб-

ничих ділянках 10, які територіально знаходяться у різних місцях.

Кожна виробнича лінія має у своєму складі генератор 106 коду, призначений для генерування та шифрування ідентифікаційного коду для кожного виробу, виготовленого на виробничій лінії 101. Виробнича лінія 101 також має у своєму складі маркувальний пристрій 107. Може бути застосований будь-який придатний маркувальний засіб, такий як струменевий принтер безперервної дії, струменевий принтер імпульсної дії, лазерний принтер, або будь-який інший принтер чи маркувальний пристрій, що уможливорює нанесення змінної інформації та виконує тиснення або друкування ідентифікаційного коду на кожному виготовленому виробі. Залежно від виду упаковки ці ідентифікаційні коди можуть бути нанесені на кожний виріб, на зовнішню упаковку, на етикетки або будь-яким іншим відомим способом. У одному з варіантів здійснення ідентифікаційний код друкують на липких ярликах або етикетках, які за варіантом, якому віддається перевага, наносяться на виготовлені вироби незнімним чином.

У одному з варіантів здійснення ідентифікаційний код наносять лазерним променем на шар чутливого до лазерного випромінювання матеріалу, нанесеного на виріб або упаковку виробу. Цей спосіб уможливорює нанесення коду через прозорий шар обгортки.

Інші можливі носії ідентифікаційного коду включають голографічний друк, наприклад, із застосуванням формату HoloSpot®.

Варіанти здійснення цього винаходу можуть також включати радіо, електронне або магнітне записування ідентифікаційного коду, наприклад, із застосуванням RFID-транспондера, електромагнітних маркерів для зчитування EMID® або будь-яких інших засобів маркування.

За варіантом, якому віддається перевага, система має засоби для рахування та звітування про кількість згенерованих та надрукованих кодів у кожній виготовленій партії виробів або за визначений період виготовлення, що далі описано докладно. Виробничі лінії 101 включають в себе систему 106 генерування кодів, яка генерує унікальний шифрований ідентифікаційний код SUP1 для кожного виготовленого виробу. За варіантом, якому віддається перевага, система 106 генерування кодів є повністю автономним комп'ютером або мікроконтролером, призначеним для конкретної виробничої лінії 101. За варіантом, якому віддається перевага, система 106 генерування кодів може здійснювати обмін інформацією з контрольним центром 30 через захищений інтернет-зв'язок 34, місцевий центральний сервер 15 або будь-які інші придатні засоби обміну інформацією.

Контрольний центр 30 приймає та накопичує дані з виробництва, а також обробляє запити від користувачів 80, 70.

У одному з варіантів здійснення цього винаходу декілька рівнів упаковки, таких як пачки, блоки та коробки, що містять декілька пачок, виготовлених на одній виробничій лінії 101, можуть проходити маркування із застосуванням спільних апаратних ресурсів.

У одному з варіантів здійснення система 106 генерування кодів може включати в себе різні або спільні програмні модулі, завантажені у комп'ютер, що є спільним для декількох виробничих ліній та обслуговує декілька виробничих ліній одночасно. Система 106 генерування кодів може бути розташована віддалено, наприклад, у контрольному центрі, і може передавати згенеровані коди на виробничі лінії за необхідністю через відповідні мережеві засоби. Система генерування кодів виконує багато функцій, які описані нижче, включаючи генерування ідентифікаційних (ID) кодів для виробів та нанесення цих ідентифікаційних кодів.

За варіантом здійснення, показаним на Фіг.2, унікальний ідентифікаційний код SUPI отримують шляхом обробки даних у Виробничому Інформаційному Коді PIC. Код PIC об'єднує різні дані, пов'язані з виготовленням виробу, такі як код MC, що ідентифікує місце 10 виготовлення, код PL, що ідентифікує конкретну виробничу лінію 101 у місці 10 виготовлення, а також коди YR, DY, HR, що при виготовленні конкретного виробу ідентифікують рік, дату та годину відповідно. У одному з альтернативних варіантів здійснення код PIC може включати ідентифікатор генератора коду замість кодів місця виготовлення та виробничої лінії MC, PL.

Щоб отримати код PIC, окремі елементи даних можуть бути об'єднані шляхом накладення десяткових або двійкових цифр, шляхом алгебраїчного складання, шляхом застосування визначеної величини зсуву кожного елемента даних та додавання усіх зсунутих величин разом, або ж шляхом застосування будь-яких інших обчислювальних засобів. За варіантом, якому віддається перевага, функція композиції є оборотною для уможливлення декомпозиції коду PIC у вихідні елементи MC, PL, YR, DY, HR. У випадку необоротної функції композиції у код PIC може бути введений додатковий елемент для забезпечення унікальності.

Протягом кожної години роботи виробничі лінії виготовляють велику кількість виробів 43. Кожний виріб 43 ідентифікується у межах години роботи за допомогою індивідуального номера T1, наприклад, послідовного номера, що відповідає хронологічній послідовності виробництва. Можливі також інші способи генерування або надання індивідуальних номерів.

Виробничий інформаційний код PIC та індивідуальний номер T1 об'єднують для отримання ідентифікатора виробу UPI. У подальшому описі кожний код UPI є унікальним для виробу, наприклад, для однієї пачки сигарет, блока або коробки сигарет. Однак винахід не обмежений таким випадком. Він включає варіанти з неунікальними номерами UPI, які розрізняють один від одного їхніми різними цифровими підписами.

Структура коду UPI та значення різних полів, що утворюють код UPI, є лише прикладами, а не обмеженнями. Будь-який код, придатний як код-ідентифікатор виробу, який має будь-яку довільну структуру та значення, може бути застосований у межах обсягу цього винаходу.

Код складової псевдовипадкового шуму об'єднують з кодом UPI для автентифікування генератора 106 коду, який утворює цей код. Складова

шуму діє як цифровий підпис для коду, нанесеного на кожний вироблений виріб, виготовлений на конкретній виробничій лінії 101 та утворений генератором 106 коду, який може бути перевірений контрольним центром 30. Для забезпечення можливості перевірки контрольним центром цей код псевдовипадкового шуму може бути отриманий шляхом шифрування копії коду UPI із секретом, що спільно використовується генератором коду та контрольним центром. "Секрет" означає будь-які дані, що застосовують для генерування або автентифікування цифрового підпису. Можливі також інші способи додавання цифрового підпису до коду UPI, наприклад, із застосуванням криптографії з асиметричними шифрами, які включені у обсяг цього винаходу. Секрет отримують із секретних кодів, які можуть вважатися статичними секретними кодами.

У одному з варіантів здійснення, показаному на Фіг.1, централізований генераторний центр 20 "солі" генерує широкий набір секретних кодів, далі названих "матрицею "солі", яка містить велику кількість заздалегідь обчислених випадкових або псевдовипадкових даних. Кожна матриця "солі" є за варіантом, якому віддається перевага, унікальною та передається у вигляді копії на потрібну виробничу лінію 101 та у контрольний центр 30. Кожна виробничі лінія 101 приймає унікальну матрицю "солі". Матриці "солі", передані у контрольний центр, зберігаються у базі даних 31, яка виконана з можливістю доступу до контрольного центра 30 та яка за варіантом, якому віддається перевага, знаходиться у контрольному центрі 30 з ідентифікуванням виробничих ліній 101, 102, до яких вони належать.

На виробничих лініях 101, 102 ці матриці "солі" застосовують для генерування секретних ключів, призначених для кодування кодів UPI та генерування електронного підпису, як описано далі.

Для забезпечення автентичності, конфіденційності та цілісності матриці "солі", цю матрицю за варіантом, якому віддається перевага, не передають мережевим зв'язком, а записують на енергонезалежних носіях 50 даних, таких як компакт-диски CD-ROM (відомі фахівцям як "Compact Disc Read-Only Memory"), диски DVD-ROM (відомі фахівцям як "Digital Versatile Disc Read-Only Memory"), знімні жорсткі диски, магнітооптичні пристрої або будь-який ' придатний енергонезалежний запам'ятовувальний пристрій. Ці носії даних фізично передаються у контрольний центр 30 та на виробничі лінії 101, 102.

За варіантом, якому віддається перевага, для додаткового підвищення безпеки матриці "солі" шифруються та підписуються у цифровому вигляді генератором 20 "солі" із застосуванням придатного способу шифрування та автентифікації, такого як стандарт шифрування даних DES (відомий фахівцям як "Digital Encryption Standard"), алгоритм Рівеста, Шаміра і Адлемана з відкритим ключем RSA (відомий фахівцям як "Rivest, Shamir, and Adelman algorithm") та їм подібних. Матриці "солі" не надсилаються у контрольний центр як частина контрольного процесу для виробів, як описано далі.

За варіантом, якому віддається перевага, файл "солі" включає в себе такі елементи:

(i) індивідуальний ідентифікатор файла "солі";
 (ii) матрицю "солі", зашифровану із застосуванням стійкого шифру, такого як потрійний-DES, або поліпшений стандарт шифрування AES (відомий фахівцям як "Advanced Encryption Standard"), відповідно до ключа, згенерованого у генераторі 20 "солі". Матриця "солі" може бути, наприклад, довгим рядком випадкових або псевдовипадкових цифр або символів;

(iii) зашифрований ключ, потрібний для декодування матриці "солі", зашифрований за допомогою шифру з відкритим ключем, наприклад, RSA, із застосуванням відкритого ключа контрольного центра 30. Цей компонент запитується у файла "солі", надісланого у контрольний центр 30, та може бути пропущеним у файлі, призначеному для виробничої лінії 101;

(iv) цифровий підпис генератора "солі", отриманий, наприклад, шляхом кодування скороченої профільної версії повного повідомлення за допомогою секретного ключа генератора "солі", відкрита частина загального користування якого є відомою у контрольному центрі.

У цьому варіанті здійснення генератору коду кожної виробничої лінії 101 повинен бути зареєстрованим у контрольному центрі 30. Ця реєстрація відбувається тільки коли застосовується нова матриця "солі" або з визначеними інтервалами. Ця система не вимагає постійного обміну інформацією між генераторами коду та контрольним центром.

Процедура реєстрування включає в себе такі операції:

(i) генератор 106 коду виробничої лінії 101 зв'язаний з контрольним центром 30 за допомогою захищеного інтернет-зв'язку або за допомогою локального центрального сервера, підключеного до Інтернету, і ініціює реєстрування шляхом ідентифікування себе;

(ii) CD-ROM 50, на якому записаний файл "солі", завантажується у генератор коду, цілісність якого перевіряється за його електронним підписом, і його унікальний ідентифікатор передається у контрольний центр 30;

(iii) контрольний центр добуває свою власну копію файла "солі", яка зберігається локально або віддалено, за допомогою унікального ідентифікатора;

(iv) якщо файл "солі" вже застосовувався, то контрольний центр припиняє реєстрування та запитує інший файл "солі" або ініціює відповідні дії, наприклад, видає попередження користувачеві або записує його у журнал безпеки;

(v) якщо цей файл "солі" ще не був застосований, а ідентифікування генератора коду пройшло задовільно, то контрольний центр розшифровує секретний ключ файла "солі" своїм закритим ключем та передає його на генератор коду за допомогою захищеного інтернет-зв'язку 34. У тому ж випадку, коли цей файл "солі" не є унікальним, ця операція має місце незалежно від того, вже застосовувався файл "солі" чи ні;

(vi) генератор коду розшифровує матрицю "солі".

Процедура реєстрування побудована таким чином, що матрицю "солі" ніколи не передають через Інтернет. Тільки одноразовий дешифрувальний ключ передається з контрольного центра 30 у генератор 106 коду. Матриця "солі" виконана доступною для генератора коду тільки після проходження реєстрування у контрольному центрі. Це запобігає несанкціонованому застосуванню генератора коду, тому що не може бути згенерований жодний дійсний код.

За варіантом, якому віддається перевага, дешифрована матриця "солі" видаляється, коли генератор коду вимикається, щоб запобігти отриманню злоумисником доступу до матриці "солі" без належного реєстрування. Можуть бути передбачені також додаткові засоби для блокування генератора коду та запобігання несанкціонованому застосуванню генератора коду та виробничої лінії. Далі описано функціонування генератора 106 коду з посиланнями на Фіг.3.

На кожній виробничій лінії 101, 102 на початку кожної виробничої партії, генератор 106 коду генерує випадковий індекс "солі" "альфа", який він передає у контрольний центр 30 разом із різною інформацією, пов'язаною з виготовлюваним виробом, такою як, наприклад, марка, ринок призначення, упаковка. Новий індекс "солі" "альфа" генерується з кожною зміною виробничої партії. За варіантом, якому віддається перевага, контрольний центр підтверджує успішне отримання індексу "альфа" генератором коду. Цей індекс "альфа" можна вважати динамічним секретним кодом.

У одному з варіантів здійснення код UPI першого виготовлюваного виробу у партії передається з індексом "альфа" у контрольний центр 30. Індекс "солі" "альфа" зберігається у базі даних 31, зв'язаний з різною інформацією про виготовлюваний виріб. Це дає можливість контрольному центру 30 після отримання запиту на перевірку конкретного коду SUPI добути конкретний "альфа" та знати матрицю "солі", що застосовується генератором 106 коду для підписування цього коду SUPI, а також перевірити підпис.

Цей індекс "солі" "альфа" не потрібно передавати у реальному часі у контрольний центр 30 на початку кожної виробничої партії. Після того, як вибрана величина "альфа", генератор коду може негайно запускати генерування дійсних кодів, а величина "альфа" може бути передана після затримки у декілька годин або і більше залежно від наявності мережевого зв'язку.

Допоміжні засоби, такі як телефон або факс, можуть бути застосовані для передавання "альфа" у контрольний центр у випадку, якщо мережевий зв'язок відсутній. Випадковий індекс "солі" "альфа", матриця "солі" та код UPI застосовуються генератором коду для генерування коду шуму (операція 301), який є стійким проти криптографічних атак. Це унеможливає реконструювання первинних значень "альфа", матриці "солі" та коду UPI. Існують різноманітні відомі способи для генерування коду шуму, які включають, але не обмежені табличною підстановкою, індексуванням, хе-

шумуванням та їх видозмінами. Код шуму, згенерований таким чином, однозначно обчислюється з коду UPI, в той час як зворотна операція є неможливою через обчислювання.

Код шуму застосовується як цифровий підпис, що уможливорює перевірку коду UPI. За варіантом, якому віддається перевага, код "альфа" та матриця "солі" комбінуються у інший спосіб для кожного виготовленого виробу, щоб надати цифровим підписам стійкості проти спроб розшифрування.

Матриця "солі" та код "альфа" є відомими тільки генератору коду та контрольному центру. Разом вони утворюють секрет, що уможливорює генератору коду генерування підписаних кодів, які контрольний центр може згодом перевіряти.

Номер UPI та обчислений код шуму комбінуються при виконанні операції 302 та, за варіантом, якому віддається перевага, готовий код заплутується при виконанні операції 303, знищуючи кореляцію між послідовними кодами. Ця операція заплутування є оборотною, уможливаючи контрольному центру добувати значення первинного коду UPI та шуму. Можливе застосування декількох відомих способів заплутування. Конкретний вибраний алгоритм заплутування за варіантом, якому віддається перевага, не оголошують.

Результатом цього заплутування є унікальний код SUPI, який друкують на виготовлених виробах за допомогою принтера 107. Кожний з виробів 43 маркують за допомогою унікального підписаного у цифровому вигляді коду SUPI, що уможливорює ідентифікування виробничої партії, до якої він належить.

За варіантом, якому віддається перевага, дані, пов'язані з виробничою партією, наприклад, тип виробу, марка, ринок призначення, упаковка, зберігаються у базі даних 31 з індексом "альфа" на початку партії. Ці дані доступні контрольному центру. Код SUPI може бути надрукованим на виготовленому виробі із застосуванням різноманітних способів друку та маркування, наприклад, безперервний струменевий друк, краплинно-імпульсний друк, лазерний тощо. Код SUPI може бути надрукований у форматі, придатному для читання людиною, або у машинозчитуваних форматах, таких як штрихкоди типів 1-D або 2-D, або символи, придатні для оптичного розпізнавання (відомого фахівцям як OCR - "Optical Character Recognition").

За варіантом, якому віддається перевага, код SUPI друкують або записують за допомогою друкувальних або записувальних засобів, які включають в себе такі пристрої, як лічильник кодів або, призначені для підрахунку точної кількості промаркованих виробів або протягом виготовлення виробничої партії, або протягом визначеного проміжку часу. Точна кількість промаркованих виробів може зберігатися у базі даних 31, яка виконана з можливістю доступу з контрольного центру та яку застосовують для контролювання обсягів виробництва.

За одним із варіантів, якому віддається перевага, код SUPI друкують фарбою, що містить прихований маркер, який уможливорює швидку перевірку дійсності без запитів до контрольного центру.

Виробнича лінія 101 може мати датчик для виявлення наявності коду SUPI (або із застосуванням системи технічного зору, та/або шляхом виявлення прихованого маркера за необхідністю). Цей датчик може бути підключеним до контролера виробничої лінії, таким чином уможливаючи відбракування виробів, маркованих не належним чином. Контролер може бути настроєний таким чином, щоб не дозволяти роботу виробничої лінії, якщо блок датчиків від'єднаний, відмовив або відбракована визначена кількість виробів. Статистика відбракувань може реєструватися Генератором коду та передаватися на Контрольний пристрій для відстежування зареєстрованими користувачами. Виробничий інформаційний код (код PIC) може повторюватися на виготовленому виробі у прямому форматі без шифрування або заплутування, уможливаючи користувачеві перевіряти відповідь, надану контрольним центром 30 та корисну для керування та відстежування ланцюжка постачання.

Після виходу з виробничого центра 10 виготовлені вироби 43 розповсюджують та реалізують відомими способами. На кожній стадії процесу розповсюдження та реалізації автентичність виробу може бути перевірена шляхом надсилання запиту, що містить код SUPI упаковки, у контрольний центр. Така перевірка може вимагатися, наприклад, звичайними користувачами, такими як роздрібні торговці, покупці або митники, а також привілейованими користувачами, наприклад, співробітниками виробника або організаціями, які мають привілейовані угоди з виробником. Коди SUPI можуть також застосовуватися для відстежування виготовлених виробів по ланцюжку розповсюдження та реалізації.

На Фіг.4 показаний процес обробки запиту на перевірку коду SUPI у контрольному центрі. Отриманий код SUPI спочатку розплутують при виконанні операції 402 шляхом застосування інверсії функції заплутування, описаної вище. При виконанні операції 402 первинний код UPI та компонент шуму відокремлюються. Контрольний центр виконує перший рівень автентифікування при виконанні операції 404 у місці виготовлення MC та на виробничій лінії PL. Якщо виявлено, що лінія PL відповідає існуючій виробничій лінії місця виготовлення MC, автентифікування переходить на наступний рівень, а інакше при виконанні операції 420 генерується відповідь, що цей код SUPI є недійсним, а виріб є підробленим. На другому рівні автентифікування контрольний центр 30 застосовує секретну матрицю "солі", отриману генератором 20 "солі", та код "альфа", переданий на початку виробничої партії. При виконанні операції 410 контрольний центр добуває інформацію, пов'язану з цією виробничою партією, що відповідає отриманому з бази даних 31 коду UPI. Якщо добування здійснено успішно, добути матрицю "солі" та код "альфа" застосовують при виконанні операції 411 для реконструювання коду шуму з отриманого коду UPI та для перевірки дійсності підпису. Якщо отриманий шум та реконструйований шум не збігаються, або якщо жодних даних, що відповідають кодові PIC, нема у базі даних, то код SUPI іденти-

фікується як недійсний, і контрольний центр при виконанні операції 420 відповідає, що цей виріб підроблений.

На третьому рівні автентифікування при виконанні операції 412 контрольний центр перевіряє, чи подані запити на один і той самий код SUPI більше визначеної кількості разів. У цьому випадку виникає підозра, що цей код SUPI може бути клоном дійсного коду, ідентично надрукованим на великій кількості підробок. Контрольний центр тоді при виконанні операції 430 видає відповідь, яка вказує, що поданий код є дійсним, однак цей виріб може бути підробленим.

Виявлення клонованих кодів може бути вдосконалено шляхом застосування іншої інформації, наприклад, походження запиту, який можна визначити, якщо цей запит зроблений з телефону, або визначити час, що пройшов між запитами.

Тут "клонування" означає множинне копіювання дійсного виробничого коду, наприклад, для маркування підроблених виробів. Якщо ж код визнано дійсним (операція 440), то контрольний центр добуває значення цього коду та передає його користувачеві, за варіантом, якому віддається перевага, природною мовою, наприклад: "Ваш код відповідає пачці марки XYZ, ринок призначення роздрібного продажу - Швейцарія", або у вигляді іншого придатного формулювання.

Інформація, повернена контрольним центром, може уможливлувати відстежування виробничої інформації щодо кожного виробу, наприклад, інформації про виробничий пристрій, виробничу лінію, дату та час виготовлення. Така інформація може бути надана у кодованій формі або природною мовою.

Факультативно контрольний центр може формувати значення кодів кількома мовами, та вибрати найбільш відповідну мову для відповіді відповідно до походження або мови запиту. За варіантом, якому віддається перевага, інтерфейс колективного доступу до контрольного центра включає в себе портал 60 коротких повідомлень SMS (Short Message Service) або неструктурованих додаткових даних USSD (Unstructured Supplementary Services Data) мережі радіотелефонного зв'язку з колективним доступом, наприклад, телефонної мережі, де підтримуються текстові або цифрові повідомлення, такий як мережі стандартів GSM, TDMA, CDMA, PDC або UMTS, через які користувачі 80 можуть надсилати запити у контрольний центр 30 у вигляді текстових повідомлень або SMS з їхніх власних стільникових телефонів 82 та приймати відповідь із контрольного центра тим самим шляхом або іншим каналом, наприклад, мовним зверненням. У цей спосіб користувач 80 може перевірити виріб 43 безпосередньо у місці продажу 77.

Обмін інформацією може альтернативно або додатково здійснюватися через мережу інтернет 32 за допомогою веб-сервера, розташованого у контрольному центрі 30, за допомогою сервера електронної пошти або сервера протоколу бездротового доступу WAP (відомий фахівцям як "Wireless Application Protocol").

Альтернативно або додатково цей обмін інформацією може здійснюватися з телефонним мовним сервером, виконаним із можливістю інтерпретації мовних команд або сигналів двотональної багаточастотної системи DTMF (відомої фахівцям як "Dual-Tone Multi-Frequency"), генерованих телефонною клавіатурою.

Варіанти здійснення цього винаходу уможливають звичайному невизначеному користувачеві автентифікувати виготовлений виріб через мережу загального користування, таку як Інтернет 32, телефонну мережу або мобільну телефонну мережу. Користувачеві не потрібно ідентифікувати себе або мати доступ до жодних секретних кодів або закритої інформації. Однак кожний виріб може бути ідентифікований у криптографічно безпечний спосіб.

За варіантом, якому віддається перевага, привілейований користувач 70, наприклад, співробітник виробника, може мати привілейований доступ до контрольного центра 30 та отримувати додаткову привілейовану інформацію, недоступну для звичайного користувача, наприклад, інформацію про обсяги виробництва або статистичну інформацію після отримання доступу до контрольного центра. У цьому випадку привілейований користувач може запитувати інформацію щодо конкретного коду SUPI без маркування його як клонований для подальших запитів від рядових покупців 80.

Цей привілейований користувач може здійснювати обмін інформацією з контрольним центром 30 через мережу загального користування або інтранет-зв'язок 33.

За іншим варіантом, якому віддається перевага, контрольний центр може надавати звичайним або привілейованим користувачам додаткову інформацію, до якої вони мають доступ та яка не міститься у коді UPI, наприклад, строк придатності, інформацію щодо гарантії, адресу локальної підтримки, або ж попередні операції реалізування, шляхи імпортування і так далі.

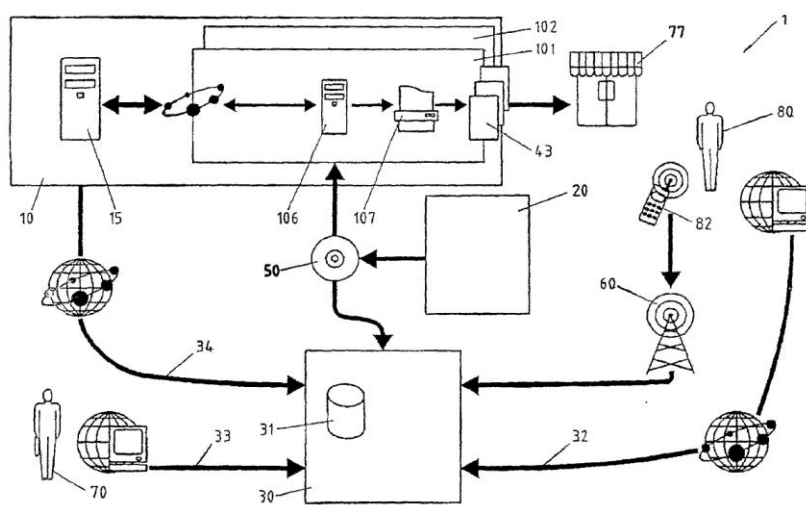
Додатково контрольний центр може збирати та зберігати інформацію про обсяги виробництва, наприклад, кількість виробів, виготовлених у кожній виробничій партії на кожній виробничій лінії, а також статистичні виробничі дані стосовно марки та ринку призначення. Така інформація про обсяги виробництва може бути застосованою для керівництва виробництвом, або з офіційною метою та може бути доступною для вибраних користувачів.

Можуть бути передбачені операції ідентифікування для ідентифікування відомих привілейованих користувачів, наприклад, за паролями, генерованими серверами пароллями (відомими фахівцям як "cookies"), мовними або біометричними даними, або за допомогою будь-яких придатних засобів ідентифікування. Контрольний пристрій може включати в себе або мати доступ до бази даних прав користувачів для зберігання параметрів різних користувачів та визначення того, до якої інформації кожний користувач має доступ.

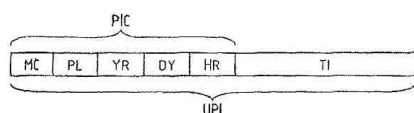
Зрозуміло, що варіанти здійснення цього винаходу не вимагають ні постійного з'єднання між виробничими лініями та контрольним центром, ані

індивідуального зберігання усіх кодів SUPI у базі даних. Фактично не зберігається жодного ідентифікаційного коду. Цифровий підпис забезпечує те, що кожний виріб може бути перевірений з мінімальним передаванням конфіденційних даних, що забезпечує високий рівень надійності та безпеки. Крім того, обсяги виробництва можуть бути точно обліковані. Оскільки жодних ідентифікаційних кодів не зберігається у контрольному центрі, то база даних, потрібна у контрольному центрі, є відносно невеликою у порівнянні з такою, яка була б потрібна у випадку зберігання цих кодів.

У деяких ситуаціях, зокрема, якщо виготовлені товари підлягають спеціальним нормам оподаткування, офіційні державні органи можуть подавати запити у контрольний центр, щоб отримати відповідні виробничі дані, наприклад, обсяги виробництва. У таких випадках контрольний центр 30 може обслуговуватися довіреною третьою стороною, незалежною від виробника виготовлених виробів 43. Описані варіанти здійснення можуть бути застосовані для заміни системи акцизних марок, що застосовується у багатьох країнах для збирання податків, наприклад, на тютюнові вироби.



ФІГ. 1



ФІГ. 2

ФІГ. 3



