



УКРАЇНА

(19) UA

(11) 58402

(13) A

(51) 7 G06K9/00

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІОПИС  
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ  
НА ВИНАХІДвидається під  
відповідальність  
власника  
патенту

## (54) СПОСІБ ВИЗНАЧЕННЯ АВТЕНТИЧНОСТІ ВИРОБУ

1

2

(21) 2003032182

(22) 12 03 2003

(24) 15 07 2003

(46) 15 07 2003, Бюл. №7, 2003 р

(72) Залізняк Денис Петрович, Рудой Олександр Петрович

(73) Залізняк Денис Петрович, Рудой Олександр Петрович

(57) 1 Спосіб визначення автентичності виробу, що включає нанесення на товар індивідуального коду, повідомлення його покупцем після придбання покупки в службу інформації, визначення відповідного коду та ідентифікацію виробу, який відрізняється тим, що додатково на виріб наносять щонайменше один захисний код, що формується за допомогою алгоритмів криптографічних перетворень з індивідуального коду виробу, а ви-

значення відповідного коду в службі інформації здійснюють за тим же алгоритмом криптографічних перетворень і при збігу його з захисним кодом, проставленим на виробі, ідентифікують останній як автентичний

2 Спосіб за п 1, який відрізняється тим, що як індивідуальний код виробу використовують простий числовий або текстовий вираз, або вираз, до якого були застосовані криптографічні перетворення

3 Спосіб за п 1 або п 2, який відрізняється тим, що індивідуальний код та/або захисний код виконані як візуально недоступні до придбання виробу

4 Спосіб за будь-яким з пп 1-3, який відрізняється тим, що на виріб наносять кілька захисних кодів

Винахід відноситься до способів визначення автентичності контрольованих об'єктів і може бути застосований для широкого спектра товарів, у першу чергу для деяких видів медикаментів і алкогольної продукції

Відомий спосіб визначення автентичності контрольованого об'єкта, що полягає в нанесенні на нього мпок, що містять інформацію про об'єкт, з наступним зчитуванням цієї інформації і порівнянням отриманої в результаті зчитування інформації з базою даних інформації про справжні об'єкти. При цьому інформацію про об'єкт формують у цифровому вигляді, включаючи інформацію про тип об'єкта, виробника, дату виробництва, унікальний номер об'єкта, супровідних документів до об'єкта, підписують її електронним цифровим підписом маркірувальника, перетворюють отриману інформацію з цифрової форми в штрих-код і наносять його на об'єкт чи етикетку, закріплену на об'єкті, а при зчитуванні інформації перетворюють штрих-код у цифрову форму, виділяють з неї електронний цифровий підпис і інформацію про об'єкт, після чого роблять перевірку електронного цифрового підпису, і якщо підпис справжній, то проводять перевірку автентичності об'єкта шляхом порівняння зчитаної інформації про об'єкт із базою

даних інформації про справжні об'єкти, і якщо інформація збігається, то об'єкт ідентифікують як справжній (RU 2132569, G07D7/00, 27 06 99)

Недоліком даного способу є необхідність наявності в покупця пристрою, що зчитує штрих-код, пристрою порівняння електронних підписів, а також необхідність вести базу даних інформації про справжні об'єкти і недостатня захищеність штрих-коду, пов'язана з його візуальною відкритістю

Відомі також технічні рішення, що використовують різні засоби, що маркірують, (WO 97/19821 A1, 05 06 97, US 5318326 A, 07 08 94, FR 2564782 A1, 29 11 85, EP 0773505 A2 14 05 97), однак їхнім недоліком є низька вірогідність інформації, зв'язана з можливістю підробки маркування

Найбільш близьким до заявленого винаходу є спосіб визначення автентичності контрольованого об'єкта, що полягає в нанесенні на виріб чи етикетку коду виду виробу й індивідуального коду виробу, що формується за допомогою генератора випадкових чисел (RU 2181503, G06K9/00, G07D7/00, 20 04 2002). Нанесені коди покриваються непрозорою плівкою, що стирається. У базу даних служби контролю записують код виду виробу й індивідуальний код виробу. Після придбання товару покупець стирає непрозорий захисний шар і по

(13) A

(11) 58402

(19) UA

одному з зазначених на виробі номерів телефону чи Інтернет-адресі передає код виду виробу й індивідуальний код виробу в службу контролю. У базі даних служби контролю виконується порівняння отриманого коду та коду, що зберігається в базі даних, і у випадку збігу приймається рішення про дійсність виробу. Недоліками даного способу є

- необхідність зберігати в базі даних інформацію про всі коди виробів, що випускаються,

- необхідність захисту від несанкціонованого доступу до бази даних, що зберігає коди виробів, а також необхідність захисту каналу інформаційного зв'язку, по якому інформація про коди виробів надходить від виробника в службу контролю,

- використання генератора випадкових чисел для одержання індивідуальних кодів не дозволяє виключити збігу деяких кодів, і, отже, не дозволяє виключити можливість зловмиснику виробляти підроблену продукцію, коди якої збігаються з кодами одного з екземплярів оригінальної продукції.

Крім цього, прийняття рішення про автентичність виробу лежить цілком на службі контролю і забезпечить від людського фактора, так як інформація про автентичність надається у вигляді повідомлення, наприклад "Телевізор фірми SONY справжній" або "Вид товару та фірма невідомі - підробка", що може привести до деякої недовіри до даного способу з боку споживача. Перераховані вище недоліки приводять до недостатньої захищеності цього способу, а також до його високої експлуатаційної вартості.

В основу винаходу покладено завдання створити такий спосіб визначення автентичності виробу, у якому шляхом використання щонайменше двох кодів, пов'язаних між собою за допомогою криптографічних перетворень досягається підвищення ступеню захисту продукції і об'єктивності оцінювання її автентичності.

Для вирішення завдання запропонований спосіб визначення автентичності виробу, що включає нанесення на товар індивідуального коду, повідомлення його покупцем після придбання покупки в службу інформації, визначення відповідного коду та ідентифікація виробу, у якому, згідно з винаходом, додатково на виріб наносяться щонайменше один захисний код, що формується за допомогою алгоритмів криптографічних перетворень з індивідуального коду виробу, а визначення відповідного коду в службі інформації здійснюється за тим же алгоритмом криптографічних перетворень і при збігу його з захисним кодом, проставленим на виробі ідентифікують останній як автентичний.

Для виключення можливості підробки, індивідуальний код та/або захисний код виконані як візуально недоступні до придбання виробу. Вони можуть бути прикриті акцизною маркою або іншим непрозорим шаром, або виконані фарбою, яка проявляється в певних умовах.

На виріб можуть бути нанесені кілька захисних кодів.

Технічний результат заявленого винаходу полягає в підвищенні захисту продукції завдяки використанню щонайменше двох кодів, пов'язаних між собою за допомогою криптографічних пере-

творень, що дозволяє розцінювати їх як електронний цифровий підпис виробника та в наданні покупцю відомостей, достатніх для самостійного прийняття рішення про автентичність продукції, а також у можливості виявлення випадків поширення підробленої продукції.

Як індивідуальний код виробу використовують простий числовий або текстовий вираз, до якого можуть бути застосовані криптографічні перетворення. Наприклад, як алгоритм криптографічних перетворень може бути використаний стандарт Росії - ДСТ 28147-89. ДСТ 28147-89 - це блоковий шифр із 256-бітним ключем і 32 циклами перетворення, що оперує 64-бітними блоками. Силова атака на ДСТ абсолютно безперспективна. Також, завдяки великій кількості циклів перетворення, даний стандарт має високу стійкість до диференційного та лінійного криптоаналізу. Крім цього, алгоритм ДСТ 28147-89 добре підходить для програмної реалізації, що дозволяє його рекомендувати на використання в даному способі визначення автентичності виробу.

Далі до індивідуального коду можуть бути включені код виду виробу, що дозволить при перевірці визначити вид товару, і відмітка часу. Як відмітка часу, наприклад, може використовуватися порядковий номер тижня, починаючи з якої-небудь фіксованої дати. Це дозволить змінювати ключ шифрування щотижня, і при розшифровці, знаходити його в збереженому списку ключів за допомогою відмітки часу. Індивідуальний код наноситься на виріб, етикетку чи упаковку, та може бути захищений від візуального перегляду до придбання виробу.

Над індивідуальним кодом виконуються криптографічні перетворення для одержання одного чи кількох захисних кодів. Захисний код являє собою інформацію, яку практично неможливо підробити без знання ключа шифрування та індивідуального коду. Захисний код наноситься на виріб чи етикетку, та також може бути захищений від візуального перегляду до придбання виробу.

Таким чином, стійкість від підробки отриманої комбінації індивідуального коду та коду захисту буде визначатися криптостійкістю обраного алгоритму шифрування і використовуваною схемою керування ключами.

Після придбання виробу покупець може переглянути індивідуальний код і передати його за допомогою телекомунікаційних засобів зв'язку в службу інформації. Номери телефонів, адреси електронної пошти чи Інтернет-адреса служби інформації наносяться на виріб чи етикетку або доводяться до відома покупців за допомогою засобів масової інформації. Служба інформації зберігає відомості про усі види продукції, що захищається, і про всі ключі шифрування, що використовувалися. По отриманим даним в службі інформації може бути визначена наступна інформація - вид виробу, приблизна дата його виготовлення та захисний код виробу. Ця інформація за допомогою тих же телекомунікаційних засобів зв'язку повідомляється покупцю. У випадку якщо вона цілком збігається з зазначеною на виробі, покупець може бути упевнений у справжності виробу.

Даний спосіб дозволяє формувати індивідуальні коди шляхом, наприклад, шифрування порядкових або серійних номерів виробів, завдяки чому цілком виключається збіг індивідуальних кодів для двох чи більш одиниць продукції. Також цілком виключається збіг захисних кодів виробів. Ця властивість виключає можливість генерації цих кодів злоумисником, але не виключає можливості копіювання кодів з оригінальних виробів на підроблені. Для виявлення випадків продажу таких підроблених виробів кожен запит на перевірку дійсності фіксується в службі інформації. При повторному звертанні іншого покупця з перевіркою такого ж індивідуального коду, що і раніше, робиться висновок про продаж підробленої продукції і можуть бути прийняті відповідні міри.

Розглянемо дію способу більш детально на прикладі виробництва коньячної продукції. По-перше визначається індивідуальний код. Для цього береться код виду товару, наприклад 01, до нього додається відмітка часу, наприклад 17, що означає 17-й тиждень виробництва від початку впровадження способу. Далі береться порядковий номер виробу, наприклад 123456, шифрується за допомогою ключа, який відомий лише виробнику та інформаційному центру. Одержуємо, наприклад номер 98A35B. Код виду товару, відмітка часу та зашифрований порядковий номер разом складають індивідуальний код, у нашому випадку це - 01 17 98A35B, який наноситься на кришечку виробу, та при необхідності закривається від перегляду захисним шаром або акцизною маркою. Код захис-

ту отримується за допомогою криптографічних перетворень, де номер виробу є або ключем шифрування або текстом для шифрування.

Отриманий код захисту, наприклад 465A85674, розцінюється як цифровий підпис виробника, та наноситься на етикетку виробу.

Після придбання виробу покупець відкриває номер виробу - 01 17 98A35B, та повідомляє його за допомогою SMS-повідомлення до обчислювального центру. В обчислювальному центрі до отриманого індивідуального коду застосовують ті ж самі криптографічні перетворення, що й при виготовленні виробу, та отримують відповідний захисний код. Далі, по коду 01, з допомогою бази даних визначають вид товару та інформують покупця повідомленням виду "Коньяк Шустов, 0.5л, виготовлений - Липень 2003, код захисту - 465A85674". Якщо ця інформація цілком збігається з реальною, покупець визнає автентичність виробу.

Усі запити покупців про перевірку автентичності фіксуються в службі інформації. При повторному отриманні службою інформації індивідуального коду 011798A35B, покупцю повідомляється наприклад "Коньяк Шустов, 0.5л, виготовлений - Липень 2003, код захисту - 465A85674, повторний запит". Це дає змогу покупцю виявити підробку, у випадку, якщо він повідомляє цей індивідуальний код вперше.

Широке впровадження даного способу дозволить звести до мінімуму виробництво і поширення підробленої продукції.