



УКРАЇНА

(19) UA (11) 44864 (13) U
(51) МПК (2009)
G06Q 20/00
G06Q 30/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА

1

(21) u200908678
(22) 18.08.2009
(24) 12.10.2009
(46) 12.10.2009, Бюл.№ 19, 2009 р.
(72) СІДЕЛЬОВ ПАВЛО АНАТОЛІЙОВИЧ
(73) СІДЕЛЬОВ ПАВЛО АНАТОЛІЙОВИЧ, ЗОЛО-
ТУХІН ОЛЕКСАНДР ВІКТОРОВИЧ
(57) 1. Спосіб ідентифікації користувача, під час
якого застосовують його мобільний термінал (MT),
який **відрізняється** тим, що для ідентифікації ко-
ристувача використовують канал бездротового
зв'язку між MT користувача та ідентифікаційною
системою (IC), по якому передається унікальний
номер пристрою бездротового зв'язку MT, причому
цей номер попередньо реєструють в IC, оснащеної
програмним забезпеченням, що може зіставляти
попередньо зареєстрований номер пристрою без-
дротового зв'язку MT з переданим через канал
бездротового зв'язку в процесі ідентифікації.
2. Спосіб за п. 1, який **відрізняється** тим, що як
MT застосовують мобільний телефон, ноутбук,

2

кишеньковий комп'ютер або інший мобільний при-
стрій, що має пристрій для бездротового зв'язку.
3. Спосіб за п. 1 або п. 2, який **відрізняється** тим,
що для бездротового зв'язку використовують тех-
нологію Bluetooth.
4. Спосіб за п. 3, який **відрізняється** тим, що для
ідентифікації додатково використовують PIN на
процедуру стикування між двома Bluetooth при-
строями MT та терміналом IC.
5. Спосіб за п. 4, який **відрізняється** тим, що PIN
на процедуру стикування передають за допомогою
повідомлення на телефон користувача або через
Інтернет-сайт IC.
6. Спосіб за п. 1, який **відрізняється** тим, що для
бездротового зв'язку використовують технологію
WiFi або NFC.
7. Спосіб за будь-яким з пп. 1-6, який **відрізняєть-
ся** тим, що номер пристрою бездротового зв'язку
MT реєструють в IC через її Інтернет-сайт або на
терміналах самообслуговування.

Корисна модель належить до галузі обробки
даних, спеціально призначених для комерційного
та управлінського застосування. Корисна модель
дозволяє ідентифікувати користувачів за допо-
могою застосування їх мобільних терміналів під
час здійснення торговельних операцій, надавання
різноманітних послуг без безпосереднього контак-
ту користувачів з ідентифікаційною системою (IC).

В контексті опису до корисної моделі, що за-
являється під поняттям «користувач» необхідно
розуміти будь-яку людину, що отримує послугу
платно або безплатно, купує товар, отримує до-
ступ до приміщення тощо.

Під поняттям «мобільний термінал» (Далі -
MT) розуміють будь-який мобільний засіб, осна-
щений пристроєм бездротового зв'язку. Напри-
клад, мобільний телефон, ноутбук або кишенько-
вий комп'ютер.

Під поняттям «ідентифікаційна система» (Далі
- IC) розуміють один пристрій або комплекс з декі-
лькох пристроїв, що оснащено програмним забез-
печенням, що може зіставляти попередньо зареє-

стрований номер пристрою бездротового зв'язку
MT з номером переданим через канал бездрото-
вого зв'язку в процесі ідентифікації. Зокрема це
може бути відповідно оснащений персональний
комп'ютер, торговельний термінал, термінал кон-
трольно-пропускного пункту.

З рівня техніки відомі способи, за якими пе-
редбачається використання MT для здійснення
торговельних операцій.

Наприклад, з патенту UA 72846 C2, 15.04.2005
відомий спосіб здійснення електронних розраху-
нків відносяться до виконання розрахунків за допо-
могою автоматизованих систем та баз даних, що
включає проведення платіжної транзакції за елек-
тронним повідомленням щодо платіжної транзак-
ції, надісланим з мобільного телефону абонента
мобільного зв'язку через мережу передачі даних
до центру обробки транзакцій. При цьому платіжну
транзакцію проводять між особистими рахунками
абонентів мобільного зв'язку за допомогою білін-
гової системи принаймні одного оператора мобі-
льного зв'язку, зв'язаної з центром обробки тран-

(13) U

(11) 44864

(19) UA

закцій. Платіжну транзакцію проводять після встановлення умови, чи є абоненти клієнтами білінгової системи, і умови щодо коштів на особистому рахунку абонента мобільного зв'язку, від якого надходить електронне повідомлення щодо платіжної транзакції. Запропонований спосіб здійснюється з використанням системи, що включає центр обробки платіжних транзакцій, зв'язаний через мережу передачі даних з мобільними телефонами клієнтів, і з білінговою системою принаймні одного оператора мобільного зв'язку. Недоліком цього способу є залежність від принаймні одного оператора мобільного зв'язку, необхідність використання його білінгової системи, необхідність наявності коштів на рахунку користувача в момент його ідентифікації. Крім того, існує певна обмеженість засобів для використання способу, як МТ використовують тільки мобільний телефон.

Наприклад, з патенту UA 73179 C2, 15.06.2005 відомий спосіб надання споживачам доступу до продукту або низки продуктів, який містить етапи: надання споживачам через захищену мережу зв'язку коду до реєстраційного центру, причому згаданий код є особливим; передавання згаданого коду від реєстраційного центру до центру перевірки повноважень; витягування ідентифікатора продукту або низки продуктів із згаданого коду, шляхом запиту до бази даних, або розрахунку згаданого ідентифікатора; передавання центром перевірки повноважень коду авторизації до терміналу споживача, де згаданий код авторизації дозволяє доступ до продукту або низки продуктів.

Крім недоліків зазначених при описуванні першого аналога, цей спосіб дозволяє отримувати тільки одноразовий код, що не припускає задіяння системи знижок при багаторазовому отриманні послуги або багаторазового доступу до певної інформації тощо.

З патенту UA 21163 U, 15.03.06 відомий спосіб роботи інформаційної системи для надання доступу до послуг, при якому споживачам надають через захищену мережу зв'язку код до реєстраційного центру та передають згаданий код, після встановлення зв'язку інформаційної системи для надання доступу до послуг з мобільною відеоінформаційною системою споживача визначають та автоматично фіксують номер телефону мобільної відеоінформаційної системи споживача, за допомогою якого встановлено зв'язок, чи споживача просять вказати номер телефону мобільної відеоінформаційної системи споживача, котрий буде використаний при отримуванні споживачем доступу до послуги, а потім на мобільну відеоінформаційну систему споживача надсилають рекламне та/чи довідкове повідомлення, котре знаходиться в пам'яті інформаційної системи для надання доступу до послуг і в інтерактивному режимі, котрий може бути звуковим, споживачеві пропонують вибрати потрібну йому послугу та замовити її, відправивши відповідне електронне повідомлення інформаційній системі для надання доступу до послуг, а після вибору послуги споживачем, також в інтерактивному режимі, споживачеві вказують рахунок для оплати послуги та пропонують оплатити послуги з будь-якого рахунку чи використати скетч-карту, котра дозволяє платити

за вибрані споживачем послуги, а також вказати своє власне прізвище шляхом набору його на клавіатурі мобільної відеоінформаційної системи споживача, після цього перевіряють суму коштів, котрі перераховані споживачем за надавання послуги також за допомогою інформаційної системи для надавання доступу до послуг, а аж потім споживачеві на його власну мобільну відеоінформаційну систему відправляють персональний код доступу до послуги, а саму послугу споживачеві надають після отримання ним паперового посвідчення на отримання послуги, котре споживачеві видають за допомогою інформаційної системи для надавання доступу до послуг в автоматичному режимі, після посилення на неї відповідного сигналу з мобільної відеоінформаційної системи споживача, номер телефону якої при цьому фіксують автоматично, де споживачем вказаний персональний код доступу до послуги та номер пристрою, котрий видає паперові посвідчення на отримання послуги (автомат), до того ж весь обмін інформацією між відеоінформаційною системою споживача та інформаційною системою для надавання доступу до послуг здійснюють в шифрованому вигляді. Після встановлення зв'язку інформаційної системи для надавання доступу до послуг з стаціонарною відеоінформаційною системою споживача просять заповнити карту споживача на web-сторінці Інтернет-сайту, де просять вказати назву послуги та номер мобільної відеоінформаційної системи споживача, котрий буде використаний при отримуванні споживачем доступу до послуги в разі використання споживачем мобільної відеоінформаційної системи або отримання споживачем паперового посвідчення на отримання послуги, котре споживачеві видають за допомогою інформаційної системи для надавання доступу до послуг в автоматичному режимі, здійснюють після набору споживачем персонального коду доступу до послуги з використанням клавіатури самої інформаційної системи для надавання доступу до послуг.

Недолік цього способу також полягає в тому, що необхідно «прив'язуватися» до певного телефонного номеру, що обумовлює залежність від певного оператора та не допускає використання іншого приладу, ніж мобільний телефон.

Найбільш близьким аналогом заявленого способу є спосіб ідентифікації користувача, що передбачає застосування його мобільного терміналу, за яким на мобільний телефон користувача попередньо відправляється штрих-код (ШК), який під час ідентифікації зчитують з мобільного телефону користувача. При цьому ШК надсилається користувачу, що відправив свій ідентифікаційний код за допомогою короткого повідомлення (SMS) до IC та зареєстрував там свій номер мобільного телефону. [Див., наприклад, Матеріали проекту "Розбудова демократії та можливостей державної служби в Україні" тренінг: «Демократія та модернізація державного сектора через створення електронного уряду», 29 січня 2 лютого 2007, с.55-56 http://napa-portal.academy.gov.ua:8101/egov/Shared%20Documents/E-Government_02.doc].

Перевагою цього способу, у порівнянні з аналогами, є менша залежність користувача від опе-

ратору мобільного зв'язку. Наприклад, отримавши ШК можна покинути зону дії оператора. Збережений ШК IC читає у будь-якому місці, де є відповідний термінал зі сканером. Ця система, зокрема була застосована у 2004 році під час проведення виборів в Південній Африці. Її зручність доведена тим, що кількість зареєстрованих виборців збільшилася приблизно на 2,5млн. порівняно з попередніми виборами, а явка виборців склала 77%.

Однак незважаючи на переваги цього способу, йому притаманний суттєвий недолік - для ідентифікації необхідно підносити екран мобільного телефону до сканеру ШК. Зчитування ШК може бути неправильним, оскільки екран телефону може бути подряпанним або відсвічувати. Для отримання ШК користувачу необхідно налагодити свій телефон на GPRS, сплатити кошти за трафік. Момент переданий особистого телефону у чужі руки для багатьох користувачів є неприємним.

В основу заявленої корисної моделі поставлено завдання розробити спосіб ідентифікації користувача, під час якого застосовують його МТ, що не залежить ані від оператора мобільного зв'язку, ані від типу певного МТ, та що дозволить проводити ідентифікацію безконтактно.

Поставлене завдання вирішується тим, що у спосіб ідентифікації користувача, під час якого застосовують його мобільний термінал (МТ), відповідно до корисної моделі, для ідентифікації користувача використовують канал бездротового зв'язку між МТ користувача та ідентифікаційною системою (IC), по якому передається унікальний номер пристрою бездротового зв'язку МТ, причому цей номер попередньо реєструють в IC, оснащеної програмним забезпеченням, що може зіставляти попередньо зареєстрований номер пристрою бездротового зв'язку МТ з переданим через канал бездротового зв'язку в процесі ідентифікації.

Унікальний номер пристрою бездротового зв'язку МТ, наприклад МЛС пристрою Bluetooth (ГБТ), слугує надійним ідентифікатором користувача. Передання його здійснюється на відстані від терміналу IC, безконтактно й передавати МТ в чужі руки не є необхідним.

Як МТ застосовують мобільний телефон, ноутбук, кишеньковий комп'ютер або інший мобільний пристрій, що має пристрій для бездротового зв'язку. Таким чином, залежність від певного оператора мобільного зв'язку відсутня.

Для бездротового зв'язку можливо використовувати технологію Bluetooth (<http://ru.wikipedia.org/wiki/Bluetooth>), яка на сьогодні є найбільш оптимальною тому, що більшість потенційних користувачів мають МТ, оснащені ГБТ. Крім того, під час ідентифікації можливо додатково використовувати PIN на процедуру стикування між двома ГБТ, МТ та терміналу IC. Це дозволяє ще більш підвищити секретність ідентифікації. При цьому PIN на процедуру стикування можливо передавати за допомогою повідомлення на телефон користувача або через Інтернет-сайт IC.

Альтернативно для бездротового зв'язку використовують технологію WiFi або NFC. Технологія WiFi

(http://ru.wikipedia.org/wiki/Near_Field_Communicatio

n) також достатньо розповсюджена і багато МТ, оснащені відповідними пристроями. Одним з стимулів для її застосування є те, що вона дозволяє здійснювати ідентифікацію на достатньо великій відстані («домашній варіант» до 45м). технологія Bluetooth в залежності від класу дозволяє розміщувати пристрої на відстані від 1 до 100м.

Технологія NFC (http://ru.wikipedia.org/wiki/Near_Field_Communicatio

n) навпаки вимушує підтримувати відстань між пристроями бездротового зв'язку до 0,2 метрів, однак вона динамічно розвивається і багато відомих виробників МТ, вже оснащують останні відповідними пристроями.

Унікальний номер пристрою бездротового зв'язку МТ попередньо реєструють в IC через її Інтернет-сайт або на терміналах самообслуговування. Зареєструвавшись в IC один раз можливо користуватися системою багаторазово і кожен день, до зміни МТ.

Більш наочно спосіб буде проілюстрований за допомогою прикладів, що наведені нижче.

Приклад 1

Користувач зареєстрував свій МТ, зокрема кишеньковий комп'ютер (КПК), оснащений ПБТ (ASUS 696) у терміналі IC. Як термінал IC використовували звичайний персональний комп'ютер (ПК), до якого через USB підключений ПБТ.ПК оснащений необхідним програмним забезпеченням для встановлення номеру ПБТ МТ (такі програми відомі <http://ptashechka.com/board/company/4093>) Отримавши унікальний номер ПБТ МТ (в даному випадку MAC), оператор ПК ввів дані користувача (прізвище, ім'я та фотографію) до IC.

Відтепер, коли до ПК надходить MAC - на екрані терміналу з'являється фотографія, прізвище та ім'я користувача. Це зроблено за допомогою програмного забезпечення, що розроблено відомим фахівцю засобом (SQL).

Дані скопіювали на інший термінал IC (по внутрішній комп'ютерній мережі підприємства), який розташований на вході у зону обмеженого доступу користувачів. Користувач отримав доступ до цієї зони на необхідний період.

На наступний день користувач підійшов до другого терміналу і на деякій відстані від нього активував ПБТ. Сигнал надійшов на ПБТ терміналу і охоронець, зіставивши користувача з фото допустив його до зони обмеженого доступу.

Звичайно, роботу охоронця може виконати простий електронний замок, до якого буде подаватися сигнал від терміналу.

Як можна побачити з цього простого прикладу спосіб можна реалізувати за допомогою недорогих розповсюджених засобів, він не залежить від оператора мобільного зв'язку і дозволяє швидко ідентифікувати користувача.

Приклад 2

Як МТ застосовано той же КПК (ASUS 696), що містить вбудований WiFi пристрій. Як термінал IC використаний ПК, який підключений до Інтернету через телефонну лінію за допомогою ADSL модему (Zyhel P-660HT), який створює мережу WiFi.

Користувач відвідав офіс, де встановлений термінал IC, включивши WiFi КПК автоматично

надіслав номер WiFi пристрою. Цей номер і дані про користувача були відіслані через Інтернет до віддаленого другого термінала IC, що аналогічний першому і який надає доступ до послуги або товару.

Згодом користувач відвідав місце, де надається послуга або товар і встановлений другий термінал. Ідентифікувався, включивши WiFi пристрій і отримав послугу або товар.

Звичайно терміналів може бути багато і тоді послугу або товар можливо буде отримувати в різних місцях.

Приклад 3

Користувач, зареєструвавши свій КПК (BTFI або WiFi пристрій) як описано у попередніх прикладах, заходить на Інтернет-сайт торгової системи і замовляє необхідні йому товари та послуги, сплачує за допомогою електронного гаманця їх вартість, отримує відповідно PIN на процедуру стикування між двома ПБТ або пароль для входу до мережі WiFi, який додатково використовує під час ідентифікації при отримванні товару або послуги у відповідному місці, де встановлений термінал IC.

Очевидно, що можна використовувати обидва пристрої (БТП або WiFi пристрій) по чергово, або одночасно.

Приклад 4

Як МТ використовувався мобільний телефон (NOKIA 6300), який має ПБТ. Як термінал IC ноут-

бук, що підключений до Інтернету. Користувач набрав комбінацію клавiш на телефоні (*#2820#), що діє як команда «показати MAC». Так був отриманий номер ПБТ, який оператор ноутбука ввів до сайту IC, також було введено ШБ користувача. В подальшому користувач замовив і сплатив через сайт послугу (відвідування кінотеатру), у місці надання послуги (кінотеатрі), яка має термінал для зчитування номеру ПБТ, включив ПБТ телефону і отримав доступ.

Комбінації клавiш залежать від виробника телефонів, але існують у всіх моделях.

Приклад 5

Все аналогічно прикладу 4, але користувач сам реєструється на терміналі самообслуговування.

Приклад 6

Все аналогічно прикладу 5, але користувач користується мобільним телефоном з NFC (Nokia 6131 NFCmesso) і відповідно ця технологія використовується терміналами IC.

Приклад 7

Все аналогічно прикладу 5, але додатково PIN на процедуру стикування передають за допомогою повідомлення на телефон користувача.

Заявлена корисна модель не обмежується наведеними прикладами, для фахівця очевидно, що можна її втілити і в інших модифікаціях.