



УКРАЇНА

(19) UA (11) 40359 (13) U

(51) МПК (2009)

G06F 12/14

G06F 12/16

H04L 9/32

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту

(54) СПОСІБ ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ПЕРСОНАЛЬНОГО ЕЛЕКТРОННОГО ПРИСТРОЮ

1

2

(21) u200810133

(22) 06.08.2008

(24) 10.04.2009

(46) 10.04.2009, Бюл. № 7, 2009 р.

(72) КАРИМАН АЛЕКС, US/UA, БАРДАЧЕНКО АНДРІЙ ВІТАЛІЙОВИЧ, UA, РАШКЕВИЧ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ, UA

(73) СОФТ РЕСОРЧЕЗ ЛЛС

(57) 1. Спосіб визначення місцезнаходження персонального електронного пристрою, що включає встановлення спеціального програмного забезпечення на персональний електронний пристрій, за допомогою якого формують ідентифікаційні дані персонального електронного пристрою, визначають поточні IP-адреси, формують та надають звіт за допомогою засобів зв'язку, який **відрізняється** тим, що за допомогою спеціального програмного забезпечення визначають зовнішні та внутрішні поточні IP-адреси персонального електронного пристрою, отриману інформацію обробляють, формують електронне повідомлення, яке містить зовнішні та внутрішні IP-адреси, що визначені спеціальним програмним забезпеченням, надсилають сформоване електронне повідомлення на заздалегідь визначену користувачем електронну адресу, яка являє собою конфіденційний ідентифікатор персонального електронного пристрою та доступ до якої мають лише користувач персонального електронного пристрою та спеціальне програмне

забезпечення персонального електронного пристрою, а користувач персонального електронного пристрою, за власним рішенням та за умови наявного з'єднання з мережею Internet, надсилає повідомлення персональному електронному пристрою, на якому встановлено спеціальне програмне забезпечення, команди щодо дистанційного керування роботою персонального електронного пристрою на заздалегідь визначену користувачем електронну адресу.

2. Спосіб визначення місцезнаходження пристрою за п. 1, який **відрізняється** тим, що повідомлення та команди, якими обмінюються користувач персонального електронного пристрою та спеціальне програмне забезпечення, попередньо кодується ключем кодування, що відомий лише користувачу персонального електронного пристрою та спеціальному програмному забезпеченню.

3. Спосіб визначення місцезнаходження пристрою за п. 1, який **відрізняється** тим, що для кожного персонального електронного пристрою, який є частиною корпоративної комп'ютерної мережі, спеціальне програмне забезпечення складається з персональної та корпоративної частин, де корпоративна частина спеціального програмного забезпечення додатково веде облік будь-яких даних, що одержані від кожного персонального електронного пристрою, як в межах корпоративної комп'ютерної мережі, так і поза її межами.

Корисна модель відноситься до способів визначення місцезнаходження персонального електронного пристрою (комп'ютера, ноутбука, мобільного телефону, тощо) для запобігання несанкціонованого доступу до нього та/або викрадення.

Відомий захисний пристрій та спосіб [Патент США №US 5,764,892, G06F 1/00, G06F 21/00, H04L 12/24, H04M 003/00, G08B 013/22, від 09.06.1998 р.], які разом утворюють захисну систему персонального комп'ютера. Суть цієї системи полягає в тому, що на персональний комп'ютер таємно або явно встановлюють спеціальне програмне забез-

печення, яке періодично передає до централізованої станції рапорт про його закодований серійний номер з одночасним наданням цих рапортів користувачу персонального комп'ютера за допомогою засобів зв'язку. Централізована станція отримує рапорти від персонального комп'ютера, порівнює їх із встановленим закодованим серійним номером та приймає або відхиляє такі рапорти.

Недоліком відомої системи є той факт, що вона залежна від певного каналу зв'язку, а саме від телефонної лінії, за допомогою якої відбувається відслідковування місцезнаходження певного комп'ютера. Така система передбачає також блоку-

(13) U

(11) 40359

(19) UA

вання роботи комп'ютера без рішення його власника, навіть, якщо переміщення комп'ютера відбулося з відома власника але без попередження централізованої станції, а комп'ютер в свою чергу не був завчасно приєднаний за допомогою модему до телефонної лінії. Таким чином, запропонований спосіб не відповідає нагальним технічним можливостям користувачів персональних комп'ютерів.

Відомий спосіб [Патент США №US 6,300,863, G06F 11/00, H04L 12/24, G06F 1/00, G06F 21/00, H04L 12/26, H04Q 7/32, G06F 007/00, від 09.10.2001 р.], який представляє собою захисну систему персонального комп'ютера. Суть цієї системи полягає в тому, що на персональний комп'ютер таємно або явно встановлюють спеціальне програмне забезпечення, яке періодично передає до моніторингової станції рапорт про його задований ідентифікаційний номер. Моніторингова станція отримує через будь-який канал зв'язку рапорти від персонального комп'ютера, порівнює їх із встановленим закодованим ідентифікаційним номером та приймає або відхиляє такі рапорти. Цією системою передбачається надавання звітів про місцезнаходження персонального комп'ютера на адресу його власника з залученням електронної пошти та/або телефону.

Недоліком відомої системи є той факт, що запропонована система в цілому є досить громіздкою бо має моніторингову станцію, яка є зайвою ланкою у сповіщенні власника про місцезнаходження комп'ютера.

Найближчим до способу, що заявляються, є спосіб для створення мережі місцезнаходження користувача [Патент США №US 7,100,204, G06F 12/14, H04L 9/32, від 29.08.2006 р.]. Цей спосіб полягає в тому, що на персональний комп'ютер встановлюється спеціалізоване програмне забезпечення, яке визначає фізичне місцезнаходження комп'ютера за допомогою IP-адреси. Спосіб передбачає наявність постійного зв'язку з глобальною комп'ютерною мережею Internet та певного посередника, який володіє відповідною базою даних. Посередник за допомогою спеціалізованої бази даних відслідковує фізичне місцезнаходження комп'ютера шляхом періодичного звіряння IP-адреси комп'ютера. Отриману інформацію про переміщення комп'ютера посередник класифікує, фіксує на спеціально утвореній мапі та розміщує на спеціальному сайті. Переміщення комп'ютера підтверджується в режимі on-line з боку його власника шляхом підтвердження IP-адреси, як прийнятої. Якщо переміщення комп'ютера не підтверджується його власником на мапі спеціального сайту, тоді робота комп'ютера блокується.

Недолік відомого способу полягає в тому, що наявність спеціалізованого сайту вимагає підтримання постійного зв'язку в режимі on-line, наражає власника комп'ютера на додаткові грошові витрати та відволікає від користування комп'ютером.

Технічною задачею корисної моделі, що заявляється, є вдосконалення способу визначення місцезнаходження персонального електронного пристрою (комп'ютера, ноутбука, мобільного телефону, тощо), що має доступ до мережі Internet, для запобігання несанкціонованого доступу до

нього та/або викрадення за допомогою визначення IP-адреси. Вдосконалення способу, що заявляється, полягає у спрощенні відомих аналогічних способів та систем з метою запобігання несанкціонованого доступу до даних, що знаходяться на персональному електронному пристрої, та сприяння у визначенні місцезнаходження персонального електронного пристрою (комп'ютера, ноутбука, мобільного телефону, тощо), що має доступ до мережі Internet.

Суть корисної моделі полягає в тому, що на персональний електронний пристрій встановлюють спеціальне програмне забезпечення (СПЗ), яке визначає зовнішні та внутрішні поточні IP-адреси персонального електронного пристрою, обробляє отриману інформацію, формує електронне повідомлення, що містить зовнішні та внутрішні поточні IP-адреси та надсилає сформоване електронне повідомлення на заздалегідь визначену користувачем електронну адресу. Доступ до електронної адреси, яка заздалегідь визначена користувачем та являє собою конфіденційний ідентифікатор персонального електронного пристрою, мають лише користувач персонального електронного пристрою та СПЗ персонального електронного пристрою.

Технічний результат досягається тим, що на персональний електронний пристрій встановлюють спеціальне програмне забезпечення (СПЗ), яке присвоює персональному електронному пристрою персональні ідентифікаційні дані, визначає зовнішні та внутрішні поточні IP-адреси персонального електронного пристрою, обробляє отриману інформацію та формує електронне повідомлення, що містить зовнішні та внутрішні IP-адреси. Електронне повідомлення, що містить зовнішні та внутрішні IP-адреси, на заздалегідь визначену користувачем електронну адресу, доступ до якої мають лише користувач персонального електронного пристрою та СПЗ персонального електронного пристрою. Таким чином, спосіб, що заявляється, забезпечує конфіденційність даних, які містяться у повідомленнях, та дає можливість користувачеві ідентифікувати повідомлення, що надійшли на вказану електронну адресу, як повідомлення від СПЗ, отримати із повідомлень поточні IP-адреси персонального електронного пристрою та за допомогою цих IP-адрес визначити ймовірне місцезнаходження персонального електронного пристрою.

Користувач персонального електронного пристрою та СПЗ, що встановлене на персональному електронному пристрої, за умови наявного з'єднання з мережею Internet можуть за допомогою вищезазначеної електронної адреси обмінюватися повідомленнями та командами, які кодуються ключем кодування, що відомий лише СПЗ та користувачу персонального електронного пристрою. Таким чином, спосіб, що заявляється, забезпечує конфіденційність, цілісність та автентичність даних, які містяться у цих повідомленнях.

На фігурі 1 (Спосіб визначення місцезнаходження персонального електронного пристрою) зображена загальна схема реалізації способу для індивідуального користувача.

На фігурі 2 (Спосіб визначення місцезнаходження персонального електронного пристрою) зображена загальна схема реалізації способу для колективного користувача.

Приклади реалізації рішення, що заявляється.

Приклад 1

На персональний електронний пристрій встановлюють спеціальне програмне забезпечення (СПЗ), яке присвоює персональному електронному пристрою персональні ідентифікаційні дані, визначає зовнішні та внутрішні поточні IP-адреси персонального електронного пристрою, обробляє отриману інформацію, формує електронне повідомлення, яке містить зовнішні та внутрішні IP-адреси, та надсилає сформоване електронне повідомлення на заздалегідь визначену користувачем електронну адресу (електронну скриньку). Доступ до цього електронного адресу мають лише користувач персонального електронного пристрою та СПЗ персонального електронного пристрою. Таким чином, спосіб, що заявляється, забезпечує конфіденційність даних, які містяться у повідомленнях, та дає можливість користувачеві ідентифікувати повідомлення, що надійшли на вказану електронну адресу, як повідомлення від СПЗ, отримати із повідомлень поточні IP-адреси персонального електронного пристрою та за допомогою цих IP-адрес визначити ймовірне місцезнаходження персонального електронного пристрою.

Користувач персонального електронного пристрою та СПЗ, що встановлено на персональному електронному пристрої, за умови наявності з'єднання з мережею Internet можуть обмінюватися повідомленнями та командами, які кодуються ключем кодування, що відомий лише СПЗ та користувачу персонального електронного пристрою. Таким чином, спосіб, що заявляється, забезпечує конфіденційність, цілісність та автентичність даних, які містяться у цих повідомленнях. Надходження повідомлень СПЗ на електронну адресу за вказівкою користувача може дублюватися попереджувальним SMS-повідомленням, що надсилається засобами мобільного зв'язку.

Користувач, у разі невизначеного місцезнаходження його персонального електронного пристрою, має можливість на свій розсуд та за власним рішенням активувати відповідні команди, що містяться у створеному користувачем спеціальному повідомленні для СПЗ, блокувати живлення персонального електронного пристрою та/або знищити дані, які знаходяться на персональному електронному пристрої і заздалегідь визначені користувачем, як такі, що підлягають знищенню у разі несанкціонованого доступу до них. СПЗ має можливість ідентифікувати повідомлення, що надійшли на заздалегідь визначену користувачем електронну адресу, як повідомлення від користувача.

Приклад 2

На персональний електронний пристрій, який є частиною корпоративної комп'ютерної мережі, встановлюють спеціальне програмне забезпечення (СПЗ), яке визначає зовнішні та внутрішні поточні IP-адреси персонального електронного пристрою, обробляє отриману інформацію, формує

електронне повідомлення, яке містить зовнішні та внутрішні IP-адреси, та надсилає сформоване електронне повідомлення на заздалегідь визначену адміністратором корпоративної комп'ютерної мережі електронну адресу (електронну скриньку). На корпоративний сервер встановлюють спеціальне серверне програмне забезпечення (корпоративна частина СПЗ), яке має базу даних усіх електронних адрес, які використовуються для обміну даними з персональними електронними пристроями. Таким чином, корпоративна частина СПЗ має можливість автоматично або за спеціальною командою адміністратора корпоративної комп'ютерної мережі централізовано отримувати повідомлення з усіх електронних адрес (від усіх персональних електронних пристроїв), а також централізовано відправляти повідомлення, що містяться у повідомленнях, та дає можливість корпоративній частині СПЗ та/або адміністратору корпоративної комп'ютерної мережі ідентифікувати повідомлення, що надійшли на вказану електронну адресу, як повідомлення від приватної частини СПЗ, отримати із повідомлень поточні IP-адреси персонального електронного пристрою та за допомогою цих IP-адрес визначити ймовірне місцезнаходження персонального електронного пристрою.

Корпоративна частина СПЗ, що встановлене на корпоративному сервері, та приватна частина СПЗ, що встановлене на персональному електронному пристрої, можуть за допомогою вищезгаданої електронної адреси обмінюватися повідомленнями та командами, які кодуються ключем кодування, що відомий лише корпоративній частині СПЗ (зберігається в базі даних корпоративного сервера) та приватній частині СПЗ, що встановлене на персональному електронному пристрої. Таким чином, спосіб, що заявляється, забезпечує конфіденційність, цілісність та автентичність даних, які містяться у цих повідомленнях.

Адміністратор корпоративної комп'ютерної мережі, у разі невизначеного місцезнаходження корпоративного персонального електронного пристрою, має можливість на свій розсуд та за власним рішенням активувати відповідні команди, що містяться у створеному адміністратором спеціальному повідомленні для персональної частини СПЗ, блокувати живлення персонального електронного пристрою та/або знищити дані, які знаходяться на персональному електронному пристрої і заздалегідь визначені адміністратором, як такі, що підлягають знищенню у разі несанкціонованого доступу до них. Корпоративна частина СПЗ, у разі невизначеного місцезнаходження корпоративного персонального електронного пристрою, має можливість автоматично активувати відповідні команди, що містяться у створеному корпоративною частиною СПЗ спеціальному по-

відомленні для персональної частини СПЗ, блокувати живлення персонального електронного пристрою та/або знищити данні, які знаходяться на персональному електронному пристрої і заздалегідь визначені адміністратором, як такі, що підлягають знищенню у разі несанкціонованого доступу до них. Персональна частина СПЗ має можливість ідентифікувати повідомлення, що надійшли на заздалегідь визначену користувачем (системним

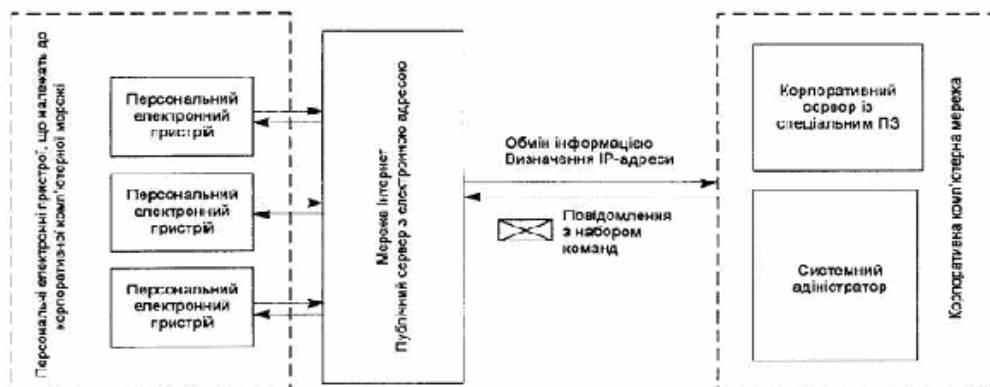
адміністратором) електронну адресу, як повідомлення від системного адміністратора та/або від корпоративної частини СПЗ.

Таким чином, спосіб, що заявляється, може бути реалізованим для будь-яких персональних електронних пристроїв, що можуть бути під'єднані до мережі Internet, а також для сукупності таких пристроїв, що належать до корпоративної комп'ютерної мережі.



Фіг. 1

Загальна схема реалізації способу для індивідуального користувача.



Фіг. 2

Загальна схема реалізації способу для колективного користувача.