



УКРАЇНА

(19) **UA** (11) **88678** (13) **U**
(51) МПК (2014.01)
H04W 12/00
G08B 13/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

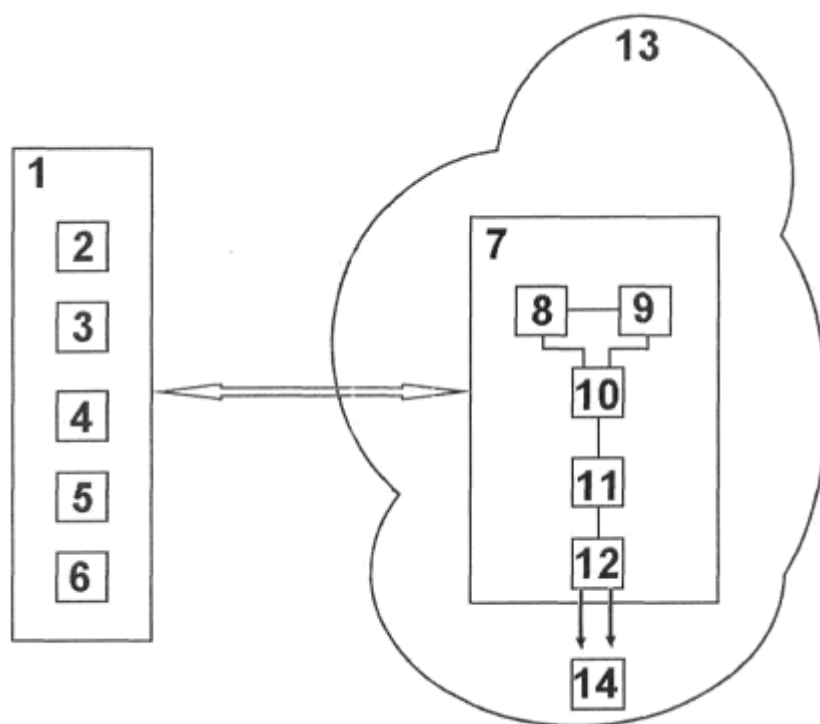
(21) Номер заявки:	u 2013 12668	(72) Винахідник(и):	Цимідан Георгій Анатолійович (UA)
(22) Дата подання заявки:	30.10.2013	(73) Власник(и):	Цимідан Георгій Анатолійович, кв. Молодіжний, 1-а, кв. 10, м. Ясинувата, Донецька обл., 86001 (UA)
(24) Дата, з якої є чинними права на корисну модель:	25.03.2014	(74) Представник:	Ортинська Марія Юріївна, реєстр. №358
(46) Публікація відомостей про видачу патенту:	25.03.2014, Бюл.№ 6		

(54) СИСТЕМА ДЛЯ ПОПЕРЕДЖЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО МОБІЛЬНОГО ПРИСТРОЮ КОРИСТУВАЧА ТА ВИЯВЛЕННЯ ОСІБ, ЯКІ ЗДІЙСНИЛИ НЕСАНКЦІОНОВАНИЙ ДОСТУП

(57) Реферат:

Система для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ, до складу якої входить стільниковий телефон або смартфон, або планшетний ПК з встановленими програмним забезпеченням та мобільним додатком, притому зазначені пристрої мають вбудовані фронтальну відеокамеру, мікрофон, динамік, WI-FI модуль, GSM модуль. Налаштування мобільного додатку забезпечують функцію включення фронтальної відеокамери та/або мікрофона, та/або динаміка мобільного пристрою, а система додатково забезпечена щонайменше одним Інтернет-сервером з встановленою на ньому базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем зберігання з програмними засобами, який зв'язаний з базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем формування повідомлень, модулем доставки повідомлень з засобами передачі повідомлень, причому налаштування мобільного додатку додатково забезпечують функцію збереження аудіо- та фото/відеофайлів в пам'яті мобільного пристрою та передачу їх Інтернет-серверу.

UA 88678 U



Корисна модель належить до систем захисту мобільних пристроїв користувачів від несанкціонованого доступу до його даних і функцій та використовується для виявлення осіб, які здійснили несанкціонований доступ.

Відомий мобільний телефон з функцією "допомога" (Патент України № 83534, МПК H04M 1/02, опубл. 10.09.2013, Бюл. № 17), що містить корпус з розміщеними на ньому органами керування у вигляді клавіатури, екран, мікрофон, звуковий динамік, систему супутникового зв'язку, цифрову фото/кінокамеру, систему вібраційного режиму та сонячну батарею, зв'язану з блоком живлення, який відрізняється тим, що оснащений додатковою малопомітною для третіх осіб кнопкою або клавішею аварійного виклику допомоги, розташованою на бічній поверхні мобільного телефона або у іншому зручному місці, проте не поряд з клавіатурою, а також містить додаткове джерело живлення у вигляді таблеткової батарейки або такої ж конструкції акумулятора невеликих розмірів, розташованого всередині корпусу телефона, причому при натисканні зазначеної кнопки, телефон вмикається разом з мікрофоном та підключається автоматично до пульта прийому сигналів служби безпеки, відключення якого можливо лише за умови набору певного коду на клавіатурі телефона, з якого надходить сигнал, та який періодично змінюється та відомий лише співробітникам служби безпеки, крім того, у разі виймання з телефона його традиційного блока живлення, він автоматично переключається на додаткове джерело живлення та продовжує роботу, навіть при вийманні sim-картки. Даний пристрій корисний тільки тоді, коли потрібно налагодити стійкий безперервний зв'язок з компетентними органами в надзвичайних випадках (напад, дорожньо-транспортна пригода, різко погіршився фізичний власника стан телефона).

Відома система захисту персонального пристрою від несанкціонованого доступу до його даних і функцій (Патент України № 66778, МПК G08B 13/00, H04B 7/00, опубл. 10.01.2012, Бюл. № 1, 2012 р.), що містить принаймні один радіоключ, що взаємодіє з персональним пристроєм за допомогою протоколу радіозв'язку, в якій радіоключ виконує функції принаймні часткового блокування функцій персонального пристрою, причому радіоключ виконаний з засобами блокування або відключення персонального пристрою. Недоліком даної системи є те, що при несанкціонованому користуванні персональним пристроєм (наприклад телефоном) даний пристрій повністю блокується і надсилає сигнали тривоги, а відеозапис подій не здійснюється.

Відома система охоронної сигналізації (Патент РФ № 102282, МПК H04M 11/04, H04M 1/11, опубл. 20.02.2011 р.), до складу якої входить стільниковий телефон, в якому використовується окремо виконаний командний пристрій у вигляді футляра для мобільного телефона, призначений для перетворення електричного сигналу, що надходить з електронного блока після спрацювання охоронного датчика, в механічну взаємодію за допомогою електромеханічного вузла на клавішу стільникового телефона для подачі сигналу тривоги, що представляє собою виклик абонента за допомогою функції стільникового телефона "швидкий виклик", при можливості використання GSM зв'язку з функцією "блокування всіх вхідних". Дане технічне рішення вибрано за прототип запропонованої корисної моделі. За допомогою даної системи здійснюється тільки фіксування обстановки всередині об'єкта, що охороняється, на фото- або відеокамеру стільникового телефона та передача сигналу тривоги з охоронюваного об'єкта до заздалегідь обраного абонента, а сам пристрій (стільниковий телефон) або доступ до його функцій, пам'яті не є захищеним.

В основу корисної моделі поставлено задачу створення системи для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ, в якій шляхом налаштувань мобільного додатка, встановленого на мобільний пристрій користувача, та використання Інтернет-сервера з конкретними базами даних та модулями, забезпечується попередження про несанкціонований доступ до мобільного пристрою користувача з наступною фіксацією даної події, збереженням файлів з записом даної події та надсилання посилань на збережені файли користувачу, що забезпечує недоторканість приватних та/або конфіденційних даних збережених в пам'яті мобільного пристрою від навмисного або випадкового доступу інших користувачів та виявлення осіб, які здійснили несанкціонований доступ.

Поставлена задача вирішується тим, що запропонована система для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ, до складу якої входить стільниковий телефон або смартфон, або планшетний ПК з встановленими програмним забезпеченням та мобільним додатком, притому зазначені пристрої мають вбудовані фронтальну відеокамеру, мікрофон, динамік, Wi-Fi модуль, GSM модуль, в якій, згідно з корисною моделлю, налаштування мобільного додатку забезпечують функцію включення фронтальної відеокамери та/або мікрофона, та/або динаміка мобільного пристрою, а система додатково забезпечена

щонайменше одним Інтернет-сервером з встановленою на ньому базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем зберігання з програмними засобами, який зв'язаний з базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем формування повідомлень, модулем доставки повідомлень з засобами передачі повідомлень, причому налаштування мобільного додатку додатково забезпечують функцію збереження аудіо- та фото/відеофайлів в пам'яті мобільного пристрою та передачу їх Інтернет-сервера.

Новим в даній корисній моделі є те, що налаштування мобільного додатку встановленого на мобільний пристрій користувача забезпечують:

- включення динаміка пристрою, який звуком сигналізує про розблокування пристрою не власником даного пристрою;
- включення роботи відеокамери, яка записує фотоінформацію та відеоінформацію, та мікрофона, який записує звук, після розблокування пристрою не власником даного пристрою;
- збереження аудіо- та фото/відеофайлів в пам'яті мобільного пристрою та передачу їх Інтернет-сервера.

Використання в системі Інтернет-сервера з встановленою на ньому базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем зберігання з програмними засобами, модулем формування повідомлень, модулем доставки повідомлень з засобами передачі повідомлень забезпечує збереженням файлів з записом події несанкціонованого доступу до мобільного пристрою користувача особою, яка не є власником даного пристрою, та надсилання посилань на збережені файли користувачу і виявлення осіб, які здійснили несанкціонований доступ.

Корисна модель пояснюється кресленням, де схематично зображено запропоновану систему для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ.

В склад запропонованої системи входить мобільний пристрій 1 з встановленим програмним забезпеченням та мобільним додатком, причому зазначені пристрої мають вбудовані фронтальну відеокамеру 2, мікрофон 3, динамік 4, WI-FI модуль 5, GSM модуль 6. Налаштування мобільного додатка забезпечують функцію включення фронтальної відеокамери 2 та/або мікрофона 3 та/або динаміка 4 мобільного пристрою 1 та забезпечують функцію збереження аудіо- та фото/відеофайлів в пам'яті мобільного пристрою 1 та передачу їх Інтернет-сервера 7, яким система додатково забезпечена. Інтернет-сервер 7 містить встановлену на ньому базу даних запитів 8 від мобільного додатка, базу даних збережених 9 аудіо- та фото/відеофайлів, модуль зберігання 10 з програмними засобами, який зв'язаний з базою даних запитів 8 від мобільного додатка, базою даних збережених 9 аудіо- та фото/відеофайлів, модуль формування повідомлень 11, модуль доставки повідомлень 12 з засобами передачі повідомлень на вказану адресу 14 (E-mail користувача, пошту користувача соціальної мережі, в якій зареєстрований користувач). Вся описана система функціонує в середовищі мережі Інтернет 13. А мобільному пристрою 1 користувача за допомогою WI-FI модуля 5 надається доступ в мережу Інтернет 13.

Мобільними пристроями 1 користувача можуть бути стільникові телефони або смартфони або планшетні ПК з операційною системою на базі платформи iOS, Android, Windows Phone та іншою, але є обов'язковим наявність фронтальної відеокамери 2 в даних пристроях.

В запропонованій системі під Інтернет-серверами 7 розуміють так названі хмарні сховища. Хмарне сховище даних (англ. cloud storage) - модель онлайн-сховища, в якому дані зберігаються на численних розподілених в мережі серверах, що надаються в користування клієнтам, в основному, третьою стороною. Дані зберігаються, а також і обробляються, в так званій хмарі, яка являє собою, з точки зору клієнта, один великий віртуальний сервер. Фізично ж такі сервери можуть розташовуватися віддалено один від одного географічно, аж до розташування на різних континентах (див. матеріали сайту <http://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D0%B0%D1%87%D0%BD%D0%BE%D0%B5%D1%85%D1%80%D0%BO%D0%BD%D0%B8%D0%BB%D0%B8%D1%89%D0%B5%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85>).

Наприклад для мобільних пристроїв з операційною системою на базі платформи iOS використовується сховище iCloud, для мобільних пристроїв з операційною системою на базі платформи Android використовується сховище Google Drive, а для мобільних пристроїв з операційною системою на базі платформи Windows Phone використовується сховище SkyDrive.

Сховище iCloud (див. матеріали сайту <http://uk.wikipedia.org/wiki/iCloud>) становить хмару зберігання і обслуговування даних від компанії Apple Inc. Сервіс дозволяє користувачам зберігати дані, такі як музика й iOS-додатки на віддалених серверах комп'ютера для

завантаження на різні пристрої, таких як iOS-пристрої під управлінням iOS 6, комп'ютера під управлінням OS X (починаючи з версії 10.7.2) або Microsoft Windows (Windows Vista Service Pack 2 або пізнішої версії).

5 Диск Google (англ. Google Drive) - сховище даних, яке належить компанії Google Inc., що дозволяє користувачам зберігати свої дані на серверах у хмарі і ділитися ними з іншими користувачами в Інтернеті (див. матеріали сайту [http://uk.wikipedia.org/wiki/Google Drive](http://uk.wikipedia.org/wiki/Google_Drive)).

Сховище SkyDrive (скорочено - SkyDrive) являє собою файл-хостинг, який базується на хмарній організації Інтернет-сервісу зберігання файлів з функціями файлообміну (див. матеріали сайту <http://ru.wikipedia.org/wiki/SkyDrive>).

10 Також користувач може вибирати будь-який з хмарних сервісів, які доступні для його мобільного пристрою 1.

Система для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ, працює наступним чином.

15 Користувач завантажує на свій мобільний пристрій 1 мобільний додаток. У випадку, коли користувач залишає свій мобільний пристрій 1 без нагляду або виникає можливість доступу до даного пристрою сторонніми особами, користувач може виконувати такі дії. Наступні приклади показують роботу системи, де мобільним пристроєм 1 є мобільний телефон.

Приклад 1.

20 Користувач включає роботу додатка, в налаштуваннях якого вибирає включення звукової сигналізації при наступному розблокуванні телефону 1. Вводить пін-код, тільки по якому можливо розблокувати телефон 1 без включення сигналізації. Блокує телефон. У випадку, коли стороння особа здійснює розблокування телефону 1 (без введення пін-коду), активується робота динаміка 4, який звуком (сигналом небезпеки) сигналізує про несанкціонований доступ до телефону 1.

25 Приклад 2.

Користувач включає роботу додатка, в налаштуваннях якого вибирає запуск роботи прихованої зйомки і запису звуку. Вводить пін-код, тільки по якому можливо розблокувати телефон 1 без включення режиму прихованої зйомки і запису звуку. Блокує телефон. У випадку, коли стороння особа здійснює розблокування телефону 1 (без введення пін-коду), активується режим роботи фронтальної відеокамери 2 та мікрофона 3. Тобто камера 2 починає діяти в режимі запису фото або відео, а мікрофон 3 - в режимі запису звуку. Дані записи зберігаються в окремій папці в пам'яті телефону 1 у вигляді фото/відео- та аудіофайлів. Одночасно програма мобільного додатка відправляє запит до Інтернет-сервера 7 про прийняття на збереження даних файлів на сервері 7. Даний запит зберігається в базі даних запитів 8 від мобільного додатка. У випадку, якщо в даний час телефон 1 користувача має з'єднання з мережею Інтернет 13, то дані файли автоматично зберігаються в базі даних 9 на Інтернет-сервері 7. У випадку, якщо телефон 1 користувача на даний час не має з'єднання з мережею Інтернет 13, то даний запит включається в чергу на збереження, яку контролюють програмні засоби модуля зберігання 10. При наявності з'єднання телефону 1 користувача з мережею Інтернет 13 або при появі з'єднання телефону 1 користувача з мережею Інтернет 13, засоби модуля зберігання 10 створюють на сервері папку даної події (несанкціонованого доступу), в властивостях якої прописані дата та час створення, тобто дата та час несанкціонованого доступу. В дану папку засоби модуля зберігання 10 поміщують всі аудіо- та фото/відеофайли, які є в базі даних 9 збережених аудіо- та фото/відеофайлів. Одночасно модуль формування повідомлень 11, формує повідомлення, в якому вказується посилання на збережені файли (місце де вони є збережені та їх можливо переглянути або завантажити), а засоби передачі повідомлень модуля доставки повідомлень 12 надсилають користувачу на вказану ним адресу 14 (E-mail користувача, пошту користувача соціальної мережі, в якій зареєстрований користувач) або іншу. В результаті, користувач отримує посилання на файли або файли, які містять аудіо- та фото/відеоінформацію, про випадок несанкціонованого доступу до його телефону. Тобто, користувач може проконтролювати, хто і коли здійснював втручання до його телефону, переглянувши свою пошту.

Приклад 3.

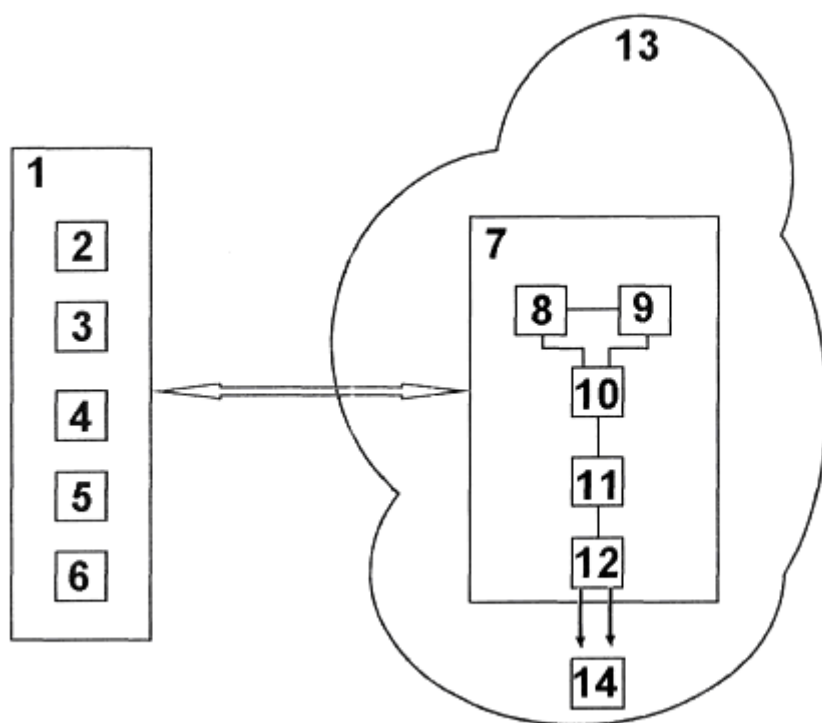
55 Користувач включає роботу додатка, в налаштуваннях якого вибирає запуск роботи прихованої зйомки, запису звуку та включення звукової сигналізації при наступному розблокуванні телефону 1. Наступні дії описані в вище вказаних Прикладах 1 та 2.

Запропонована корисна модель попереджує можливість користування мобільним пристроєм користувача іншими особами або надає факти такого несанкціонованого доступу.

60

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

- Система для попередження несанкціонованого доступу до мобільного пристрою користувача та виявлення осіб, які здійснили несанкціонований доступ, до складу якої входить стільниковий телефон або смартфон, або планшетний ПК з встановленими програмним забезпеченням та мобільним додатком, причому зазначені пристрої мають вбудовані фронтальну відеокамеру, мікрофон, динамік, WI-FI модуль, GSM модуль, яка **відрізняється** тим, що налаштування мобільного додатку забезпечують функцію включення фронтальної відеокамери та/або мікрофона, та/або динаміка мобільного пристрою, а система додатково забезпечена щонайменше одним Інтернет-сервером з встановленою на ньому базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем зберігання з програмними засобами, який зв'язаний з базою даних запитів від мобільного додатка, базою даних збережених аудіо- та фото/відеофайлів, модулем формування повідомлень, модулем доставки повідомлень з засобами передачі повідомлень, причому налаштування мобільного додатку додатково забезпечують функцію збереження аудіо- та фото/відеофайлів в пам'яті мобільного пристрою та передачу їх Інтернет-серверу.



 Комп'ютерна верстка І. Мироненко

 Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

 ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601
