



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA**

(11) **111969**

(13) **C2**

(51) МПК

H04M 1/57 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(21) Номер заявки:	а 2013 14488	(72) Винахідник(и):	Ібаско Алекс Д. (РН), Джосон Едуардо Рамон Дж. (РН), Ю Вільям Еммануель С. (РН)
(22) Дата подання заявки:	09.05.2012	(73) Власник(и):	ЕІННОВЕЙШНЗ ХОЛДІНГС ПТЕ. ЛТД., 100 Beach Road, #25-06 Shaw Towers, Singapore 189702, Singapore (SG)
(24) Дата, з якої є чинними права на винахід:	11.07.2016	(74) Представник:	Михайлюк Ганна Валентинівна, реєстр. №184
(31) Номер попередньої заявки відповідно до Паризької конвенції:	201103396-6	(56) Перелік документів, взятих до уваги експертизою:	US 2008152097 A1, 26.06.2008 US 2009186629 A1, 23.07.2009 US 2009136013 A1, 28.05.2009
(32) Дата подання попередньої заявки відповідно до Паризької конвенції:	12.05.2011		
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	SG		
(41) Публікація відомостей про заявку:	25.02.2014, Бюл.№ 4		
(46) Публікація відомостей про видачу патенту:	11.07.2016, Бюл.№ 13		
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	PCT/SG2012/000163, 09.05.2012		

(54) СИСТЕМА ТА СПОСІБ ВІДОБРАЖЕННЯ ІДЕНТИФІКАТОРА ДЖЕРЕЛА НА ПРИЙМАЛЬНОМУ ПРИБОРІ

(57) Реферат:

Розкриті система та спосіб відображення ідентифікатора джерела на приймальному пристрої, який має зв'язок з джерелом, причому вказана система містить базу асоціативних даних, що визначає щонайменше одне джерело, асоційоване з приймальним пристроєм; та менеджер обробки, призначений для обробки зв'язку від джерела до приймального пристрою та налаштований для отримання доступу до бази асоціативних даних для визначення наявності асоціювання джерела з приймальним пристроєм та, за наявністю асоціювання, для відображення встановленого ідентифікатора джерела, та, за відсутністю асоціювання, для визначення настрійок конфіденційності джерела та відображення додаткового ідентифікатора на приймальному пристрої згідно з визначеними настройками конфіденційності.

UA 111969 C2

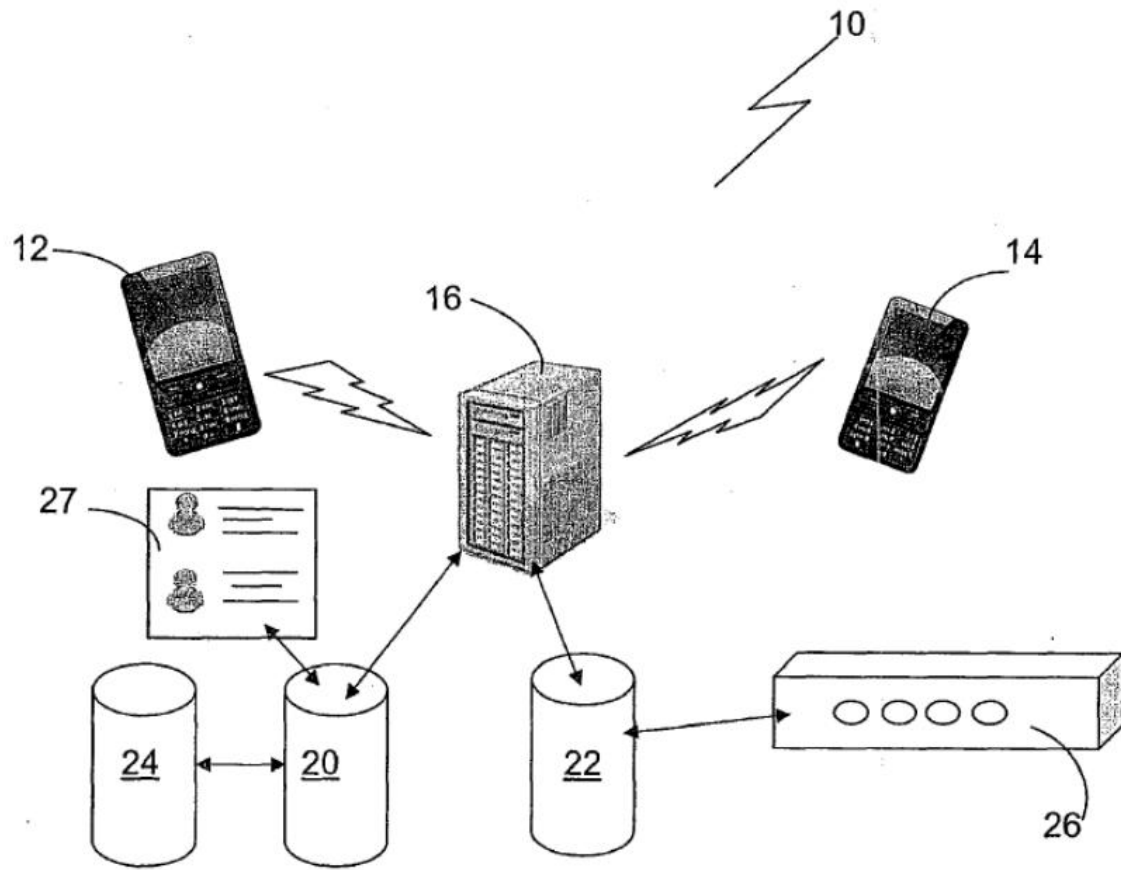


Fig. 1

Галузь техніки, до якої відноситься винахід

Даний винахід відноситься до системи та способу відображення ідентифікатора джерела на приймальному пристрої. Винахід особливо, але не виключно, підходить для відображення ідентифікатора, такого як ідентифікатор абонента, що робить виклик, на мобільному телефоні абонента, що отримує виклик.

Рівень техніки

Подальший опис рівня техніки, до якого відноситься винахід, призначений лише для полегшення розуміння даного винаходу. Слід розуміти, що цей опис не є визнанням або підтвердженням того, що будь-який матеріал, на який є посилання, є опублікованим, відомим або відноситься до загальновідомої інформації для спеціаліста в даній галузі у будь-якій юрисдикції, починаючи з дати пріоритету винаходу.

Номери комутованих телефонних мереж спільного користування (PSTN) зазвичай призначаються фізичним лініям, та цей номер залишається незмінним. Подібним чином, номери мобільних телефонів призначаються модулю ідентифікації абонента (SIM).

Один відомий спосіб призначення номерів PSTN та номерів мобільних телефонів заснований на рекомендації E.164 ITU-T, що визначає формат телефонних номерів та міжнародний план надання номерів зв'язку спільного користування, який використовується в PSTN та інших інформаційних мережах.

Однак, відчувається потреба в послугі, яка могла б надати динамічний та тимчасовий розподіл телефонних номерів, що дозволить створювати різні ідентифікатори абонента-джерела виклику для різних абонентів, що отримують виклик.

Хоча користувачі мобільних телефонів можуть використовувати ідентифікатор абонента, що робить виклик, та списки викликів, ці особливості є виключно інформативними та потребують від користувача регулярного оновлення та асоціювання абонентів, що роблять виклик, з контактом, наприклад, шляхом зберігання номеру кожного абонента, що робить виклик, в списку контактів або електронній телефонній книзі. В системі ідентифікатора абонента, що робить виклик, не існує активних зв'язків або автоматичного асоціювання між абонентом, що робить виклик, та особою, яка отримує виклик.

Відомий спосіб створення асоціювання між абонентом, що робить виклик, та особою, яка отримує виклик, полягає у створенні "соціального поєднання" або соціального зв'язку. Однак, подібні системи обмежені абонентами, що робить виклик, та особами, які отримують виклик, у межах однієї мережі через проблеми, пов'язані з дозволом/безпекою.

Крім того, хоча можливо виключити опцію ідентифікації абонента, що робить виклик, або приховати телефонний номер, багато сучасних телефонів та телефонних систем не підтримують приховування номерів через можливі зловживання кінцевими користувачами.

Мета даного винаходу полягає у частковому усуненні або покращенні вищезазначених недоліків.

У документі US 3787626 розкрита система для автоматичного надання ідентифікаційної інформації телефонного номера абонента, абонентові, що отримує виклик, яка відображає телефонний номер абонента, що робить виклик, на телефонному апараті абонента, що отримує виклик, при ініціюванні зв'язку між ними.

Суть винаходу

Згідно з першим аспектом даного винаходу надана система для відображення ідентифікатора джерела на приймальному пристрої, який має зв'язок з джерелом, причому вказана система містить базу асоціативних даних, що визначає список, який складається щонайменше з одного джерела, асоційованого з приймальним пристроєм; та менеджер обробки, призначений для обробки зв'язку від джерела до приймального пристрою та налаштований для отримання доступу до бази асоціативних даних для визначення наявності асоціювання джерела з приймальним пристроєм та, за наявністю асоціювання, для відображення встановленого ідентифікатора джерела, та за відсутністю асоціювання, для визначення налаштувань конфіденційності джерела та відображення додаткового ідентифікатора на приймальному пристрої згідно з визначеними налаштуваннями конфіденційності.

Найкраще, менеджер обробки інтегрований в пристрій джерела та/або в приймальний пристрій.

Найкраще, система додатково містить геолокаційну службу (LBS) для визначення місцезнаходження джерела. Переважно, додатково сконфігуровано LBS для визначення кількості зареєстрованих користувачів LBS, що знаходяться поблизу місцезнаходження джерела.

Найкраще, приймальний пристрій є мобільним пристроєм. Переважно, приймальний пристрій містить системний реєстр для визначення знаходження джерела в списку

спостереження або чорному списку. Переважно, якщо було визначено, що джерело знаходиться в списку спостереження або в чорному списку, зв'язок, ініційований джерелом, завершують або подають попереджувальний сигнал відповідно з подальшим завершенням зв'язку.

Найкраще, менеджер обробки адаптований для обміну даними з зовнішнім шлюзом для спрямування зв'язку від джерела до приймального пристрою, якщо було визначено, що пристрій джерела та приймальний пристрій не знаходяться в межах однієї комунікаційної мережі.

Найкраще, менеджер обробки призначений для отримання доступу до мережевої адресної книги для визначення асоціювання джерела з приймальним пристроєм.

Найкраще, настройки конфіденційності джерела визначають на основі наявності джерела в спільному списку, його відсутності у списку або прихованості ідентифікатора.

Згідно з другим аспектом даного винаходу наданий спосіб відображення ідентифікатора джерела на приймальному пристрої, який має зв'язок з джерелом, який містить наступні етапи: а. визначають список, який складається щонайменше з одного джерела, асоційованого з приймальним пристроєм; b. виконують обробку зв'язку від джерела до приймального пристрою; та c. визначають за допомогою списку наявність асоціювання джерела з приймальним пристроєм; та, за наявністю асоціювання, відображають встановлений ідентифікатор джерела, та, за відсутністю, асоціювання визначають настройки конфіденційності джерела та відображають додатковий ідентифікатор на приймальному пристрої згідно з визначеними настройками конфіденційності.

Найкраще, етап визначення настройок конфіденційності джерела містить визначення відсутності джерела в списку або визначення факту приховування його ідентифікатора.

Найкраще, якщо було визначено, що джерело та приймальний пристрій знаходяться в межах однієї комунікаційної мережі, спосіб додатково містить етап перевірки знаходження джерела в чорному списку або списку спостереження в межах комунікаційної мережі.

Найкраще, якщо джерело не знаходиться в чорному списку та списку спостереження, перевіряють настройки конфіденційності приймального пристрою для того, щоб визначити можливість відображення ідентифікатора джерела на приймальному пристрої.

Найкраще, якщо джерело знаходиться в списку спостереження, подають попереджувальний сигнал та зв'язок від джерела до приймального пристрою завершують.

Найкраще, якщо джерело знаходиться в чорному списку, зв'язок від джерела до приймального пристрою негайно завершують.

Найкраще, спосіб містить етап утворення маршруту між джерелом та приймальним пристроєм, причому етап утворення маршруту містить перевірку атрибуту ідентифікатора джерела для визначення походження ідентифікатора. Переважно, етап перевірки атрибуту ідентифікатора містить визначення перенаправлення, завантаження або ручного введення ідентифікатора в джерело.

Найкраще, спосіб містить етап визначення знаходження джерела та приймального пристрою в межах однієї комунікаційної мережі, та спрямування зв'язку від джерела, якщо було визначено, що пристрій джерела та приймальний пристрій не знаходяться в межах однієї комунікаційної мережі.

Найкраще, етап визначення наявності асоціації між джерелом та приймальним пристроєм містить отримання доступу до мережевої адресної книги.

Згідно з третім аспектом даного винаходу наданий приймальний пристрій, що містить менеджер обробки, призначений для обробки зв'язку від джерела до приймального пристрою; менеджер обробки налаштований для отримання доступу до бази асоціативних даних для визначення наявності асоціації джерела з приймальним пристроєм, база асоціативних даних визначає список, який складається щонайменше з одного джерела, асоційованого з приймальним пристроєм; при цьому, якщо визначено, що джерело асоційоване з приймальним пристроєм, відображають встановлений ідентифікатор джерела, та якщо визначено, що джерело не асоційоване з приймальним пристроєм, визначають настройки конфіденційності джерела та відображають додатковий ідентифікатор на приймальному пристрої згідно з визначеними настройками конфіденційності.

Стислий опис графічних матеріалів

Даний винахід далі буде описаний виключно за допомогою ілюстративного прикладу, з посиланням на супровідні графічні матеріали, на яких:

На фіг. 1 зображена блок-схема системи згідно з варіантом втілення винаходу.

На фіг. 2 зображена схема послідовності операцій, що ілюструє обробку телефонного виклику до абонента, що отримує виклик, згідно з варіантом втілення даного винаходу.

На фіг. 3 зображена схема послідовності операцій, що ілюструє спрямування телефонного виклику до абонента, що отримує виклик, згідно з варіантом втілення даного винаходу.

На фіг. 4 зображена схема послідовності операцій, що ілюструє ініціювання телефонного виклику від джерела до обраного абонента, який отримує виклик, при цьому джерело знаходиться в межах тієї ж мережі, що використовує варіант втілення даного винаходу.

На фіг. 5 зображена схема послідовності операцій, що ілюструє ініціювання телефонного виклику від джерела до обраного абонента в іншій мережі, та

На фіг. 6 зображена схема послідовності операцій, що ілюструє можливість використання варіанту втілення даного винаходу в "аварійному" інструменті з геолокаційною службою.

Опис варіантів втілення винаходу

Згідно з варіантом втілення винаходу, зображеним на фіг. 1, надана система 10 для відображення ідентифікатора джерела 12 на приймальному пристрої 14. В якості прикладів, джерело 12 та приймальний пристрій 14 є мобільними пристроями. Ідентифікатор джерела 12 може бути номером мобільного телефону, закріпленим за джерелом 12, або будь-якими іншими номерами або ідентифікаторами, закріпленими за джерелом 12 системою 10.

Система 10 містить менеджер 16 обробки, адаптований для обробки зв'язку, такого як телефонні виклики від джерела 12 до приймального пристрою 14. Менеджер 16 обробки може бути інтегрований в джерело 12 та/або приймальний пристрій 14, наприклад менеджер 16 обробки може містити один або обидва з використовуваних мобільних пристроїв 12, 14.

Система додатково містить базу 20 асоціативних даних та базу 22 даних прихованих номерів. База 20 асоціативних даних зазвичай є базою даних для пошуку та керування номерами. База 20 асоціативних даних визначає список джерел, асоційованих з приймальним пристроєм.

Менеджер 16 обробки призначений для отримання доступу до бази 20 асоціативних даних для визначення асоціювання джерела 12 з приймальним пристроєм 14.

База 20 асоціативних даних додатково містить базу 24 даних походження номерів. База 24 даних походження номерів встановлює походження будь-якого набраного номеру від джерела 12 виклику для визначення його належності до соціальної мережі приймального пристрою 14. База 22 даних прихованих номерів приєднана до зовнішнього шлюзу 26 для спрямування зовнішніх викликів. Будь-який телефонний виклик, який спрямовують з системи 10, є прихованим для того, щоб забезпечити його відповідність міжнародним стандартам, таким як рекомендація E.164 ITU-T.

База 20 асоціативних даних додатково підтримує мережеву адресну книгу 27 всіх абонентів в межах системи 10. Мережева адресна книга 27 приєднана до бази 22 даних прихованих номерів та бази 24 даних походження номерів. Мережева адресна книга 27 сконфігурована для подальшого встановлення/оновлення будь-яких соціальних зв'язків між абонентами в межах системи 10. Це можна досягнути шляхом виконання регулярної синхронізації між адресною книгою 27 та локальною телефонною книгою мобільного телефону абонента.

Коли з джерела 12 роблять виклик, відбувається автоматична генерація номера з діапазону номерів, зарезервованих з даною метою. Динамічна генерація номера може бути випадковою в межах діапазону номерів. Згенерований номер додають до бази 20 асоціативних даних. База 20 асоціативних даних надає прив'язку до карти оригінального телефонного номера та динамічно згенерованого (тобто прихованого) телефонного номера. Виконують пошук в базі 24 даних походження номерів для визначення ініціатора виклику. Подібна конфігурація забезпечує, щоб оригінальний телефонний номер від джерела 12 виклику був прихований та щоб лише оператор служби знав прив'язку до карти. Конфігурація додатково дозволяє приймальному пристрою 14 забороняти будь-яким сторонам викликати абонента, який отримує виклик, під час пошуку.

Менеджер 16 обробки також може містити інтерфейс користувача, що підтримує прив'язку до карти, відв'язування від карти та закріплення або керування системою.

Мобільний пристрій 12 джерела може бути будь-яким мобільним пристроєм, відомим в даній галузі техніки.

Мобільний пристрій 14, що отримує виклик, адаптований для надання користувачу можливості блокування джерела за допомогою чорного списку, з засобами встановлення попереджень та повідомлень для певних джерел, тобто створення списку спостереження; або можливості розірвання зв'язків у соціальних мережах. Приймальний пристрій 14 додатково сконфігурований для надання можливості блокування телефонних викликів.

Далі варіант втілення описано в контексті обробки телефонного виклику, ініційованого джерелом 12 виклику (який надалі буде позначений синонімічним терміном "абонент 12, що робить виклик") до абонента 14, що отримує виклик (етап 200). В якості прикладу, викликаний/набраний номер є ідентифікатором джерела.

Менеджер 16 обробки, за допомогою бази 24 даних походження номерів, перевіряє належність набраного номеру до соціальної мережі абонента, 12 що робить виклик (етап 202). Перевірка містить порівняння списку контактів або електронних телефонних книг абонента 12, що робить виклик, та абонента 14, що отримує виклик, у мережевій адресній книзі 27 для перевірки наявності соціального зв'язку між абонентом 12, що робить виклик, та абонентом 14, що отримує виклик (етап 204). Подальша перевірка може містити визначення наявності попереднього спілкування абонента 12, що робить виклик, з абонентом 14, що отримує виклик.

Якщо на етапі 204 визначено, що абонент 12, що робить виклик, та абонент 14, що отримує виклик, мають соціальний зв'язок, відбувається встановлення та під'єднання виклику (етап 206). З іншого боку, якщо визначено, що абонент 12, що робить виклик, та абонент 14, що отримує виклик, не мають соціального зв'язку, це може означати, що абонент 12, що робить виклик, та абонент 14, що отримує виклик, не мали попереднього спілкування або набраний номер було тільки що додано шляхом завантаження каталогу, перенаправленням візитної картки або за допомогою ручного вводу. В подібному випадку перевіряють настройку конфіденційності абонента 12, що робить виклик (етап 208). Перевірка містить визначення того факту, що джерело 12 не знаходиться у списку (етап 210) або що настройка конфіденційності перешкоджає виявленню номера абонента, що робить виклик. Якщо номер абонента, що робить виклик, не знаходиться в списку, то номер приховують за допомогою системної інформації, яка має щонайменше позначення того, що номер є прихованим (етап 212). Прихований номер потім стає номером абонента 12, що робить виклик, який потім буде відображений на приймальному пристрої 14.

З іншого боку, якщо настройки конфіденційності джерела 12 не вимагають анонімності, переважний ідентифікатор абонента, що робить виклик, встановлений для абонента 12, що робить виклик, асоціюють з викликом (етап 214). Переважний ідентифікатор потім буде відображений на приймальному пристрої 14.

Після етапу 212 або етапу 214 система 10 перевіряє факт знаходження абонента 12, що робить виклик, та абонента 14, що отримує виклик, в одній мобільній комунікаційній мережі (етап 216). Якщо вони не знаходяться в одній мобільній комунікаційній мережі, необхідно виконати спрямування виклику до зовнішнього шлюзу 26 до зовнішньої мережі, яка може бути незалежною мережею, не оснащеною системою даного винаходу. В даній ситуації виконують спрямування виклику (етап 222) з ідентифікацією абонента, що робить виклик (етап 218), асоційованою з викликом. Спрямування включає проходження через зовнішній шлюз 26, що включає перетворення внутрішнього сигнального протоколу системи 10 в протокол, що є сумісним з PSTN, ISDN зовнішньої комунікаційної мережі.

Однак, якщо було встановлено, що абонент 12, що робить виклик, та абонент 14, що отримує виклик, знаходяться в одній мобільній комунікаційній мережі, то виконують перевірку системних реєстрів (етап 220). Системні реєстри можуть зберігатися в приймальному пристрої 14 або в зовнішньому сервері. Системні реєстри перевіряють на наявність наступних фактів:

а. знаходження абонента 12, що робить виклик, в списку спостереження (етап 224), якщо визначено, що абонент 12, що робить виклик, знаходиться в списку спостереження, може бути поданий попереджувальний сигнал або повідомлення для ініціювання встановлення джерела виклику або подібні варіанти вибору для повідомлення сторони, яка запросила встановлення джерела виклику (етап 226). Потім виклик завершують (етап 228).

б. якщо визначено, що абонент 12, що робить виклик, не знаходиться в списку спостереження, перевіряють системні реєстри на предмет знаходження абонента 12, що робить виклик, в чорному списку (етап 230). Якщо визначено, що абонент 12, що робить виклик, знаходиться в чорному списку, його блокують та виклик негайно завершують (етап 228). Однак, якщо визначено, що абонент 12, що робить виклик, не знаходиться в чорному списку, то перевіряють настройки конфіденційності приймального пристрою 14 (етап 232) для того, щоб перевірити, чи дозволені анонімні виклики або виклики від абонента 12, що робить виклик, за межами соціальної мережі абонента, що отримує виклик (етап 234). Якщо настройки конфіденційності не дозволяють анонімні виклики або виклики ззовні соціальної мережі абонента, що отримує виклик, то виклик завершують (етап 228). З іншого боку, якщо абонент, що отримує виклик, дозволяє анонімний виклик або виклики ззовні соціальної мережі абонента, що отримує виклик, то утворюють маршрут (етап 236) та з'єднують виклик (етап 206).

Спрямування виклику (етап 236) є процесом, що містить наступні етапи:

Процес починається з перевірки атрибутів набраного номеру (етап 302), що включає перевірку того, чи був набраний номер перенаправлений від друга (етап 304), наприклад, шляхом спільного використання електронної візитної картки, завантажений (етап 306), наприклад, зі служби центрального каталогу, або набраний вручну (етап 308).

Якщо на етапі 304 система 10 визначила, що набраний номер перенаправлений від друга, то система 10 передає спільну інформацію з запису в телефонній книзі друга (етап 310) в мережеву адресну книгу 27. Після цього утворюють соціальну мережу між сторонами (етап 312).

Якщо на етапі 304 система 10 визначила, що набраний номер не був перенаправлений від друга, то система 10 потім перевіряє, чи є набраний номер завантаженим (етап 306).

Якщо на етапі 306 було визначено, що набраний номер можна вважати завантаженим, то використовують стандартний інформаційний запис щодо ідентифікатора абонента, що робить виклик, в службі центрального каталогу (етап 314). Після цього утворюють соціальну мережу між сторонами (етап 312).

Якщо на етапі 304 система 10 визначила, що набраний номер не був завантаженим, то система 10 потім перевіряє, чи був набраний номер введений вручну (етап 308).

Якщо на етапі 308 було визначено, що набраний номер введений вручну, то система 10 перевіряє наявність спільного вузла, тобто ідентифікованого спільного друга в мережевій адресній книзі 27. Потім система перевіряє, чи є набраний номер унікальним серед спільних вузлів (етап 318), та якщо він є унікальним, то використовують той номер та інформацію щодо асоційованого виклику (етап 320). З іншого боку, якщо набраний номер не є унікальним, тобто існує повторення номерів; то система використовує стандартну інформацію центрального каталогу щодо виклику для утворення зв'язку в соціальній мережі (етап 314).

Якщо на етапі 308 було визначено, що набраний номер не був введений вручну, то система логічним шляхом припускає, що дані зберігались в приймальному пристрої 14 та таким чином вони є результатом попереднього зв'язку в соціальній мережі з абонентом 14, що отримує виклик. Якщо номер не попадає в жодну з категорій, перевірених на етапах 304, 306 та 308, то це означає, що абонент 14, що отримує виклик, розірвав зв'язок в соціальній мережі з абонентом 12, що робить виклик, у деякий час перед викликом (322). Це може бути зроблено з однієї або декількох наступних причин: внесення до чорного списку, внесення до списку спостереження, соціальна ізоляція, або через нагальну потребу, таку як потреба звільнити місце в електронній телефонній адресній книзі, або навіть з банальної причини, наприклад абонент, що отримує виклик, не відчуває потреб у підтримуванні соціального зв'язку з абонентом, що робить виклик, та ін.

На основі вищезазначеної логіки, система 10 далі перевіряє, чи був абонент 12, що робить виклик, внесений до чорного списку (етап 324) або до списку спостереження (етап 328). Якщо було визначено внесення до чорного списку або до списку спостереження то виклик завершують (етап 326) або подають попереджувальний сигнал (етап 330), після чого відповідно завершують дзвінок.

Якщо абонент 12, що робить виклик, знаходиться в межах тієї ж мобільної комунікаційної мережі, то система 10 виконує наступні етапи, як зображено на фіг. 4, для утворення або спрямування виклику.

Якщо зроблено такий виклик (етап 402), то соціальну мережу, асоційовану з обраним приймальним пристроєм 14, перевіряють на предмет того, чи є номер, з якого виконують виклик, вузлом в соціальній мережі обраного абонента 14, що отримує виклик (етап 404). За умовчанням виконують спрямування виклику до ідентифікованого вузла в соціальній мережі. Якщо номер обраного абонента 14, що отримує виклик, не знаходиться в соціальній мережі джерела, то потім телефонну мережу перевіряють на предмет того, чи знаходиться обраний абонент 14, що отримує виклик, в межах тієї ж мережі (етап 406). Якщо обраний абонент 14, що отримує виклик, знаходиться в межах тієї ж мережі, то телефонний номер джерела 12 приховують (етап 408), як вказано джерелом 12, та з'єднують виклик (етап 410).

Якщо було визначено, що обраний абонент 14, що отримує виклик, знаходиться в іншій мережі, система 10 перевіряє, чи не внесено номер абонента 14, що отримує виклик, до певного списку (етап 412), та якщо номер абонента 14, що отримує виклик, не внесено до певного списку, то система 10 відправляє інформацію про мережевий ідентифікатор (етап 416) та виконує спрямування виклику (етап 418). Якщо номер абонента 14, що отримує виклик, внесено до певного списку, то інформацію про ідентифікатор абонента, що робить виклик, відправляють замість інформації про мережевий ідентифікатор (етап 420) та виконують спрямування виклику (етап 418).

Слід розуміти, що навіть якщо абонент 12, що робить виклик, точно визначає приховання свого номеру, якщо він або вона попередньо зв'язувались з обраним абонентом 14, що отримує виклик, то визначене приховання буде заміщене інформацією з попереднього встановленого зв'язку. Наприклад, якщо абонент 12, що робить виклик, мав попередній контакт (тобто встановив соціальний зв'язок) з абонентом 14, що отримує виклик, де абонент 12, що робить виклик, використовував номер n; та абонент 12, що робить виклик, згодом розірвав або

розірвала свій зв'язок з абонентом 14, що отримує виклик, та потім абонент 12, що робить виклик, намагається повторно встановити контакт з абонентом 14, що отримує виклик, використовуючи інший встановлений номер x , то цей номер x буде заміщений номером n та абонент 14, що отримує виклик, буде як і раніше бачити номер n абонента 12, що робить виклик, замість нового номера x . Слід розуміти, що номер абонента 12, що робить виклик, буде іншим для іншого абонента C , що отримує виклик, в соціальній групі AC , оскільки їхнє соціальне групування є іншим.

У випадку, якщо абонент 12, що робить виклик, знаходиться в зовнішній мережі та приймальний пристрій 14 знаходиться в межах мережі, система 10 виконує наступні етапи, як зображено на фіг. 5, для встановлення, завершення або виконання будь-яких необов'язкових дій, що відносяться до виклику.

Підчас ініціювання виклику (етап 502) виконують перевірку настройки конфіденційності абонента 12, що робить виклик (етап 504). Приклад способу перевірки настройки конфіденційності абонента 12, що робить виклик, включає перевірку знаходження абонента 12, що робить виклик, в спільному списку (етап 506). Якщо абонент 12, що робить виклик, надає ідентифікатор абонента, що робить виклик, або якщо він є в спільному списку, то виклик з'єднують (етап 522). Однак, якщо абонент 12, що робить виклик, не надає ідентифікатор абонента, що робить виклик, так що він не знаходиться в спільному списку, то виконують перевірку системних реєстрів (етап 508) для того, щоб визначити, чи знаходиться абонент 12, що робить виклик, в чорному списку (етап 510). Якщо номер абонента 12, що робить виклик, знаходиться в чорному списку, виклик завершують (етап 512) та система 10 надає варіант виконання подальших дій, таких як ініціювання встановлення походження виклику або подання попереджувального сигналу (етап 514) будь-яким обраним контактам для зв'язку в надзвичайних ситуаціях або соціальним контактам.

Якщо було встановлено, що номер абонента 12, який робить виклик, не заходиться в чорному списку, перевіряють настройку конфіденційності абонента, що отримує виклик (етап 516). Перевіряють сторону 14, що отримує виклик, та якщо анонімні виклики дозволені (етап 518), виклик реєструють за допомогою системи (етап 520) та потім з'єднують (етап 522). З іншого боку, якщо сторона, що отримує виклик, не дозволяє анонімні виклики, то виклик негайно завершують (етап 512). Як і раніше, система надає варіант виконання певних подальших дій, таких як ініціювання встановлення походження виклику або подання попереджувального сигналу (етап 514).

Підчас реєстрації виклику (етап 520) система 10 утворює пару номера, що робить виклик, з номером, що отримує виклик. Це утворення пари стає зв'язком віртуальної соціальної мережі, так що у разі подальшого виклику від того ж абонента 12, що робить виклик, та за відсутності негативної інформації, знайденої протягом перевірки реєстрів, тобто інформації про знаходження у чорному списку, виклик одразу ж з'єднують зі стороною, що отримує виклик. Однак, обраний абонент 14, що отримує виклик та який знаходиться в межах мережі, що використовує цей винахід, має варіант у будь-який час внести джерело 12 в чорний список та роз'єднати виклик, або розірвати зв'язок в соціальній мережі.

Варіант втілення, описаний вище, також може використовуватись разом з геолокаційною службою (LBS), наприклад в інструменті для надзвичайних ситуацій (ICE). В ілюстративному прикладі, зображеному на фіг. 6, припущено, що певні користувачі зареєстровані в якості волонтерів в службі допомоги у надзвичайних ситуаціях HELP. Ділові правила для цього можуть бути визначені організацією, що наглядає за телефонним номером служби допомоги у надзвичайних ситуаціях HELP або гарячої лінії HELPLINE.

Кінцевий користувач, який знаходиться у небезпеці, розпочинає процес гарячої лінії HELPLINE. Цей кінцевий користувач, який стає абонентом, що робить виклик, або джерелом 12, набирає обраний номер гарячої лінії HELPLINE, який в даному прикладі є номером 4357, що відповідає літерам HELP на клавіатурі звичайного телефону (етап 602). Слід розуміти, що якщо б це був виклик за номером 911, то було б виконано спрямування виклику в телефонний центр служби 911. Система служби допомоги в надзвичайних ситуаціях потім використовує LBS та визначає місцезнаходження джерела 12 (етап 604).

Потім менеджер 16 обробки перевіряє свою базу даних волонтерів (відомих як група HELP) та отримує їхні місцезнаходження (етап 606). У випадку закритої групи HELP, тобто якщо користувач визначає, які номери необхідно асоціювати з викликом HELP, система та LBS перевіряють місцезнаходження об'єднання волонтерів. Система ідентифікує волонтера, що знаходиться якнайближче до місцезнаходження джерела 12 (етап 608). Оскільки джерело 12 може знаходитись в компанії інших представників об'єднання волонтерів та вся ця компанія може знаходитись у біді, то якщо виклик буде спрямовано до них, це анулює мету сигналу про

допомогу. Отже, система служби допомоги в надзвичайних ситуаціях повинна визначити, що відносно місцезнаходження джерела та цільовий волонтер не є ідентичними до такої міри, яка знаходиться в межах погрішності, пов'язаної з LBS.

Після визначення найближчого волонтера система 10 спрямовує виклик до найближчого волонтера (етап 610). Якщо волонтер отримує виклик (етап 612), то встановлюють зв'язок в режимі діалогу (етап 614).

З іншого боку, волонтер може не отримати виклик через те, що волонтер не помітив виклик, наприклад пропустив виклик (етап 615), або через те, що волонтер не зацікавлений у відповіді на сигнал про небезпеку. Якщо волонтер ненавмисно пропустив виклик, система 10 виконує повторну пробу виклику (етап 616). З іншого боку, якщо виклик було навмисно проігноровано, телефонний номер сторони, що його проігнорувала, видаляють з об'єднання волонтерів (етап 618). Потім система визначає, хто з об'єднання волонтерів знаходиться найближче до сторони, що потрапила в біду, та намагається направити виклик тому волонтеру, тобто робить повторну пробу з включеними сторонами (етап 616). Етапи 610 - 618 можуть повторюватись, як було пояснено.

Крім того, може бути присутня особливість закінчення терміну, у разі якої, якщо виклики спрямовують до тих самих номерів та виклики залишаються без відповіді, виклик за умовчанням спрямовують до центральної гарячої лінії HELPLINE, яка може бути об'єктом, подібним до 911, або до іншого подібного варіанту реалізації, прийнятого населенням пунктом, оператором мобільного зв'язку або іншою подібною зацікавленою стороною.

База даних волонтерів може визначатися користувачами, тобто бути визначена користувачем, що потрапив в біду. Вона також може бути згенерована системою на основі існуючої служби каталогу, який є централізованою базою даних для всіх абонентів, а також онлайнною службою телефонного довідника фізичних осіб та підприємств та списком соціальної мережі. Вона також може бути соціальною, основою на записках в списку контактів або в телефонній книзі абонента, що робить виклик, або основою на частотності або тривалості взаємодії між абонентом, що робить виклик та абонентами, що знаходяться в його або її списку контактів, телефонній книзі, файлі реєстрації викликів або повідомлень.

Даний винахід надає особливість приховування номеру, яка виходить за межі лише утаювання або підмінування ідентифікатора джерела. Завдяки обробці викликів, як описано в різних прикладах та варіантах втілення, вказаних вище, особливість приховування номеру згідно даного винаходу є свідомою спробою зробити телефонні номери відповідними або не відповідними для осіб, використовуючи захищену інфраструктуру (тобто в межах комунікаційної мережі), яка перешкоджає шахрайству.

У порівнянні зі стандартами відомого рівня техніки, такими як RFC 3325, який дозволяє мережі довірених серверів стверджувати справжність авторизованих користувачів, де користувачі повинні знаходитись в довірєній мережі, даний винахід передбачає ситуацію поза визначенням RFC 3325, де одна сторона може знаходитись за межами довірєної мережі.

Перевага, асоційована з даним винаходом полягає в тому, що ідентифікатор, такий як Мобільний ідентифікаційний номер (MIN) ніколи не розкривається, що надає контрольовану конфіденційність завдяки перевіркам налаштувань конфіденційності пристрою джерела та приймального пристрою.

Крім того, враховуючи адресну книгу 27 соціальної мережі, яку підтримують в мережі системи, підміна номера мобільним абонентом, що робить виклик або абонентом, що отримує виклик, є неможливою, оскільки лише оператор у будь-який час володіє інформацією про ідентифікаційну прив'язку до карти.

Слід розуміти, що вищезазначені варіанти втілення надані лише в якості ілюстративних прикладів даного винаходу, таких як зазначені нижче, та що подальші модифікації та покращення винаходу, які стануть очевидними спеціалістам у відповідній галузі, вважаються такими, що знаходяться в межах широкого об'єму та діапазону даного описаного винаходу, в особливості:

- Пристрій 12 джерела та приймальний пристрій 14 можуть бути мобільними телефонами або будь-яким електронним приладом або пристроєм з можливістю підключення до мережі.

- Пристрій, що робить виклик, та приймальний пристрій можуть знаходитись у бездротовому зв'язку за допомогою мобільної мережі, тобто 3G, EDGE, GSM, радіо та ін.; за допомогою бездротових мереж, тобто Wi-Fi, WiMax, IrDA, Bluetooth, NFC, або за допомогою дротового з'єднання.

- Винахід може бути реалізований за допомогою інших інтерфейсів, таких як система інтерактивної голосової відповіді (IVR) або веб-сайт.

Крім того, хоча могли бути описані окремі варіанти втілення винаходу, передбачається, що винахід також охоплює комбінації зазначених варіантів втілення.

ФОРМУЛА ВИНАХОДУ

1. Система для відображення ідентифікатора джерела на приймальному пристрої, що знаходиться в зв'язку з джерелом, причому система містить:
 - базу асоціативних даних, призначену для підтримання мережевої адресної книги; та
 - менеджер обробки, призначений для обробки зв'язку від джерела до приймального
- 5 пристрою та налаштований для порівняння списку контактів джерела та списку контактів приймального пристрою у мережевій адресній книзі для визначення наявності асоціації джерела з приймальним пристроєм, та за наявності асоціації джерела з приймальним пристроєм, для відображення встановленого ідентифікатора джерела на приймальному пристрої, яка **відрізняється** тим, що
- 10 за відсутності асоціації джерела з приймальним пристроєм, перевіряють настройки конфіденційності приймального пристрою та, якщо настройки конфіденційності приймального пристрою дозволяють зв'язок за межами соціальної мережі приймального пристрою, система виконана з можливістю перевірки атрибуту ідентифікатора джерела для визначення
- 15 походження ідентифікатора приймального пристрою та подальшого утворення соціальної мережі між джерелом та приймальним пристроєм за допомогою інформації, що стосується походження ідентифікатора приймального пристрою.
2. Система за п. 1, яка **відрізняється** тим, що менеджер обробки інтегрований в пристрій джерела та/або приймальний пристрій.
3. Система за п. 1 або 2, яка **відрізняється** тим, що приймальний пристрій є мобільним
- 20 пристроєм.
4. Система за п. 1 або 2, яка **відрізняється** тим, що джерело є мобільним пристроєм.
5. Система за п. 1 або 2, яка **відрізняється** тим, що менеджер обробки містить інтерфейс користувача, який дозволяє отримувати доступ до керування системою.
6. Система за п. 1, яка **відрізняється** тим, що система додатково містить геолокаційну службу
- 25 (LBS) для визначення місцезнаходження джерела.
7. Система за п. 6, яка **відрізняється** тим, що LBS додатково сконфігурована для інформування рятівних служб про місцезнаходження джерела.
8. Система за п. 6, яка **відрізняється** тим, що LBS додатково сконфігурована для інформування щонайменше одного контакту з джерела.
- 30 9. Система за п. 8, яка **відрізняється** тим, що щонайменше один контакт вибраний джерелом в менеджері обробки.
10. Система за п. 8, яка **відрізняється** тим, що щонайменше один контакт з джерела є вибраним на підставі частоти взаємодії з джерелом.
11. Система за п. 8, яка **відрізняється** тим, що щонайменше один контакт з джерела є
- 35 вибраним на підставі тривалості взаємодії з джерелом.
12. Система за п. 6, яка **відрізняється** тим, що LBS додатково сконфігурована для отримання доступу до бази даних зареєстрованих користувачів та визначення кількості зареєстрованих користувачів LBS, що знаходяться найближче до місцезнаходження джерела.
13. Система за п. 12, яка **відрізняється** тим, що LBS додатково сконфігурована для
- 40 інформування всіх зареєстрованих користувачів LBS про місцезнаходження джерела.
14. Система за п. 12, яка **відрізняється** тим, що LBS додатково сконфігурована для інформування щонайменше одного зареєстрованого користувача, який знаходиться якнайближче до місцезнаходження джерела.
15. Система за п. 14, яка **відрізняється** тим, що LBS додатково сконфігурована для отримання
- 45 доступу до мережевої адресної книги та інформування щонайменше одного зареєстрованого користувача, не асоційованого з джерелом.
16. Система за п. 14, яка **відрізняється** тим, що LBS додатково сконфігурована для отримання доступу до бази даних зареєстрованих користувачів та відповідного оновлення вказаної бази даних на підставі дії щонайменше одного поінформованого зареєстрованого користувача.
- 50 17. Система за п. 16, яка **відрізняється** тим, що LBS додатково сконфігурована для отримання доступу до бази даних зареєстрованих користувачів та інформування щонайменше одного зареєстрованого користувача, який є другим за наближеністю до місцезнаходження джерела.
18. Система за п. 14, яка **відрізняється** тим, що LBS не здатна інформувати щонайменше одного зареєстрованого користувача щодо місцезнаходження джерела, та LBS додатково
- 55 сконфігурована для інформування рятівних служб про місцезнаходження джерела.

19. Система за п. 1, яка **відрізняється** тим, що приймальний пристрій містить системний реєстр для визначення знаходження джерела в списку спостереження або чорному списку.

20. Система за п. 6, яка **відрізняється** тим, що якщо було визначено, що джерело знаходиться в списку спостереження або в чорному списку, зв'язок, ініційований джерелом, завершують або

5

21. Система за п. 1, яка **відрізняється** тим, що менеджер обробки адаптований для обміну даними з зовнішнім шлюзом для спрямування зв'язку від джерела до приймального пристрою, якщо було визначено, що джерело та приймальний пристрій не знаходяться в межах однієї комунікаційної мережі.

10

22. Система за п. 1, яка **відрізняється** тим, що мережева адресна книга додатково сконфігурована для визначення наявності асоціювання джерела з приймальним пристроєм шляхом регулярного виконання синхронізації між мережевою адресною книгою та джерелом, та приймальним пристроєм.

15

23. Система за п. 1, яка **відрізняється** тим, що за відсутності асоціації джерела з приймальним пристроєм, менеджер обробки виконаний з можливістю визначення налаштувань конфіденційності джерела та відображення додаткового ідентифікатора на приймальному пристрої згідно з визначеними налаштуваннями конфіденційності джерела, причому налаштування конфіденційності джерела визначають на основі наявності джерела у спільному списку, його відсутності у списку або прихованості ідентифікатора.

20

24. Спосіб відображення ідентифікатора джерела на приймальному пристрої, що знаходиться в зв'язку з джерелом, який містить наступні етапи, на яких:

обробляють зв'язок від джерела до приймального пристрою;

порівнюють список контактів джерела та список контактів приймального пристрою у мережевій адресній книзі;

25

визначають наявність асоціації джерела з приймальним пристроєм;

за наявності асоціації джерела з приймальним пристроєм, відображають встановлений ідентифікатор джерела на приймальному пристрої, та

за відсутності асоціації джерела з приймальним пристроєм, перевіряють налаштування конфіденційності приймального пристрою та, якщо налаштування конфіденційності приймального пристрою дозволяють зв'язок за межами соціальної мережі приймального пристрою, перевіряють атрибут ідентифікатора джерела для визначення походження ідентифікатора приймального пристрою, та після цього утворюють соціальну мережу між джерелом та приймальним пристроєм за допомогою інформації, що стосується походження ідентифікатора приймального пристрою.

30

35

25. Спосіб за п. 24, який **відрізняється** тим, що містить етап, на якому, за відсутності асоціації джерела з приймальним пристроєм, визначають налаштування конфіденційності джерела та відображають додатковий ідентифікатор на приймальному пристрої згідно з визначеними налаштуваннями конфіденційності, причому етап, на якому визначають налаштування конфіденційності джерела, містить визначення відсутності джерела у спільному списку або факту приховування його ідентифікатора.

40

26. Спосіб за п. 24, який **відрізняється** тим, що, якщо було визначено, що джерело та приймальний пристрій знаходяться в межах однієї комунікаційної мережі, то додатково перевіряють знаходження джерела в чорному списку або списку спостереження в межах комунікаційної мережі.

45

27. Спосіб за п. 26, який **відрізняється** тим, що, якщо джерело не знаходиться в чорному списку та списку спостереження, перевіряють налаштування конфіденційності приймального пристрою для того, щоб визначити можливість відображення ідентифікатора джерела на приймальному пристрої.

50

28. Спосіб за п. 26, який **відрізняється** тим, що, якщо джерело знаходиться в списку спостереження, подають попереджувальний сигнал та зв'язок від джерела до приймального пристрою завершують.

29. Спосіб за п. 26, який **відрізняється** тим, що якщо джерело знаходиться в чорному списку, зв'язок від джерела до приймального пристрою завершують.

55

30. Спосіб за п. 24, який **відрізняється** тим, що містить етап утворення маршруту між джерелом та приймальним пристроєм.

31. Спосіб за п. 30, який **відрізняється** тим, що етап перевірки атрибуту ідентифікатора містить визначення перенаправлення, завантаження або ручного введення ідентифікатора в джерело.

32. Спосіб за п. 24, який **відрізняється** тим, що містить етап визначення знаходження джерела та приймального пристрою в межах однієї комунікаційної мережі та спрямування зв'язку від

джерела, якщо було визначено, що пристрій джерела та приймальний пристрій не знаходяться в межах однієї комунікаційної мережі.

33. Спосіб за п. 24, який **відрізняється** тим, що етап порівняння списку контактів джерела та списку контактів приймального пристрою у мережевій адресній книзі містить отримання доступу до мережевої адресної книги.

34. Спосіб за п. 33, який **відрізняється** тим, що мережеву адресну книгу регулярно синхронізують з джерелом та приймальним пристроєм.

35. Приймальний пристрій, який містить менеджер обробки, призначений для обробки зв'язку від джерела до приймального пристрою у системі;

при цьому менеджер обробки призначений для підтримання мережевої адресної книги та порівняння списку контактів джерела та списку контактів приймального пристрою у мережевій адресній книзі для визначення наявності асоціації джерела з приймальним пристроєм; та

за наявності асоціації джерела з приймальним пристроєм, приймальний пристрій відображає встановлений ідентифікатор джерела, який **відрізняється** тим, що

за відсутності асоціації джерела з приймальним пристроєм, перевіряють настройки конфіденційності приймального пристрою, та, якщо настройки конфіденційності приймального пристрою дозволяють зв'язок за межами соціальної мережі приймального пристрою, система виконана з можливістю перевірки атрибуту ідентифікатора джерела для визначення походження ідентифікатора приймального пристрою та подальшого утворення соціальної мережі між джерелом та приймальним пристроєм за допомогою інформації, що стосується походження ідентифікатора приймального пристрою.

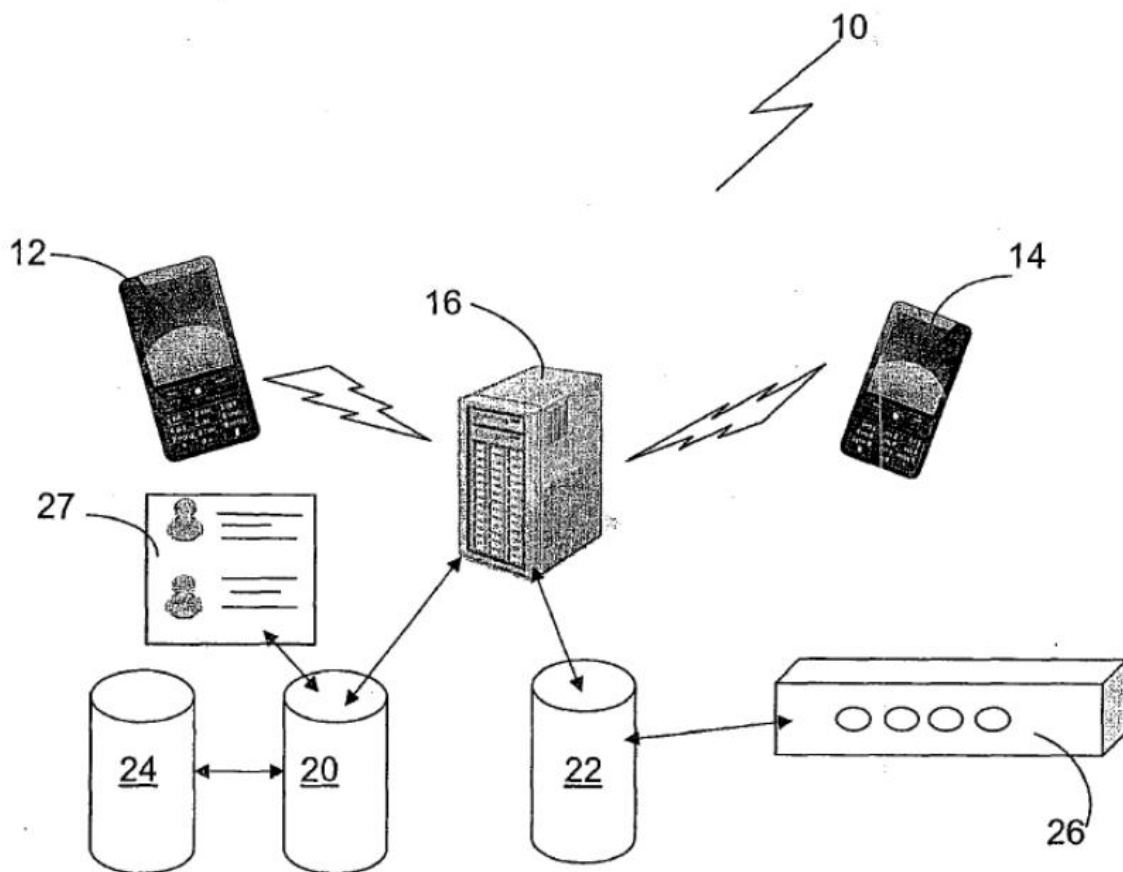


Fig. 1

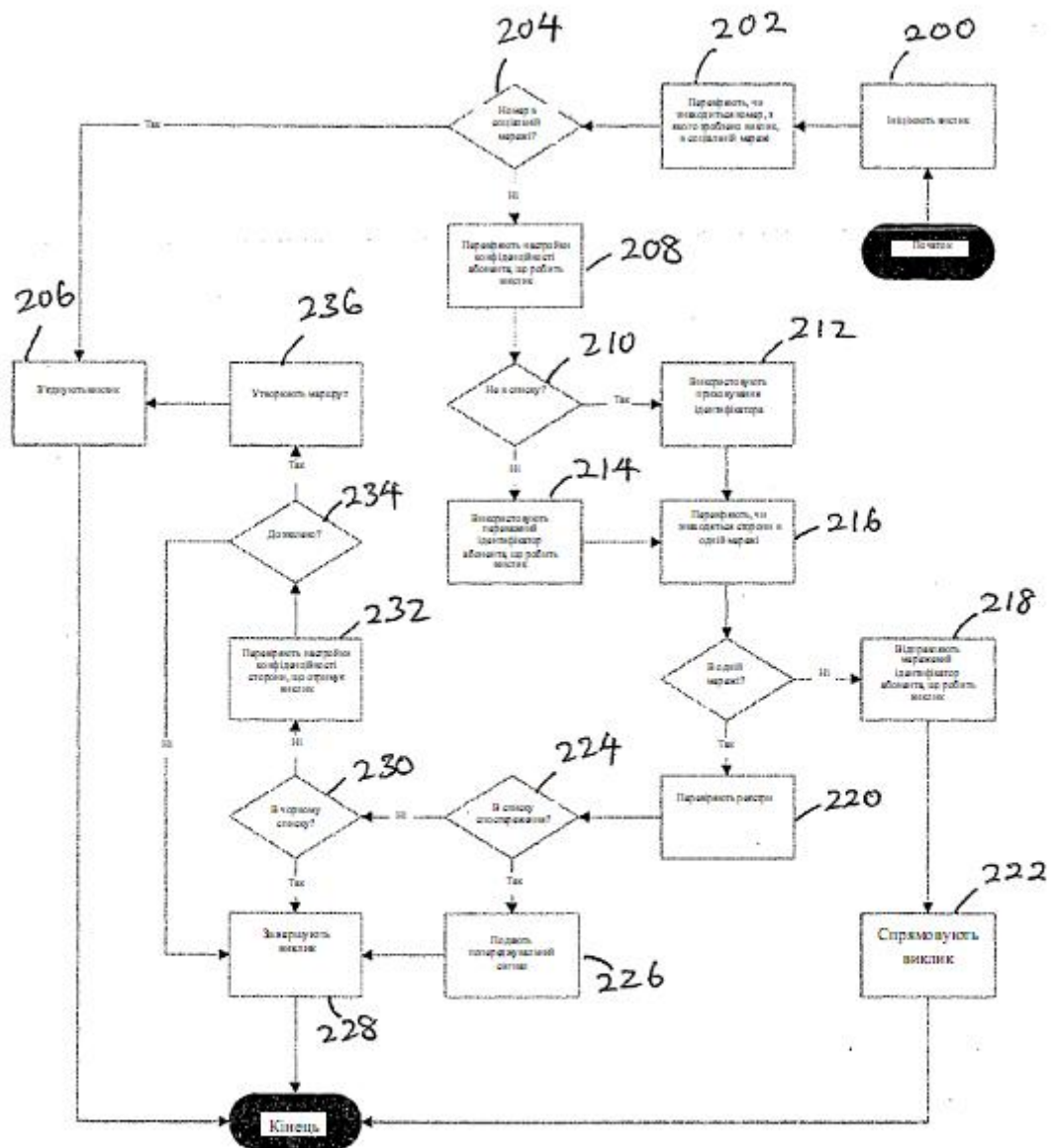


Fig. 2

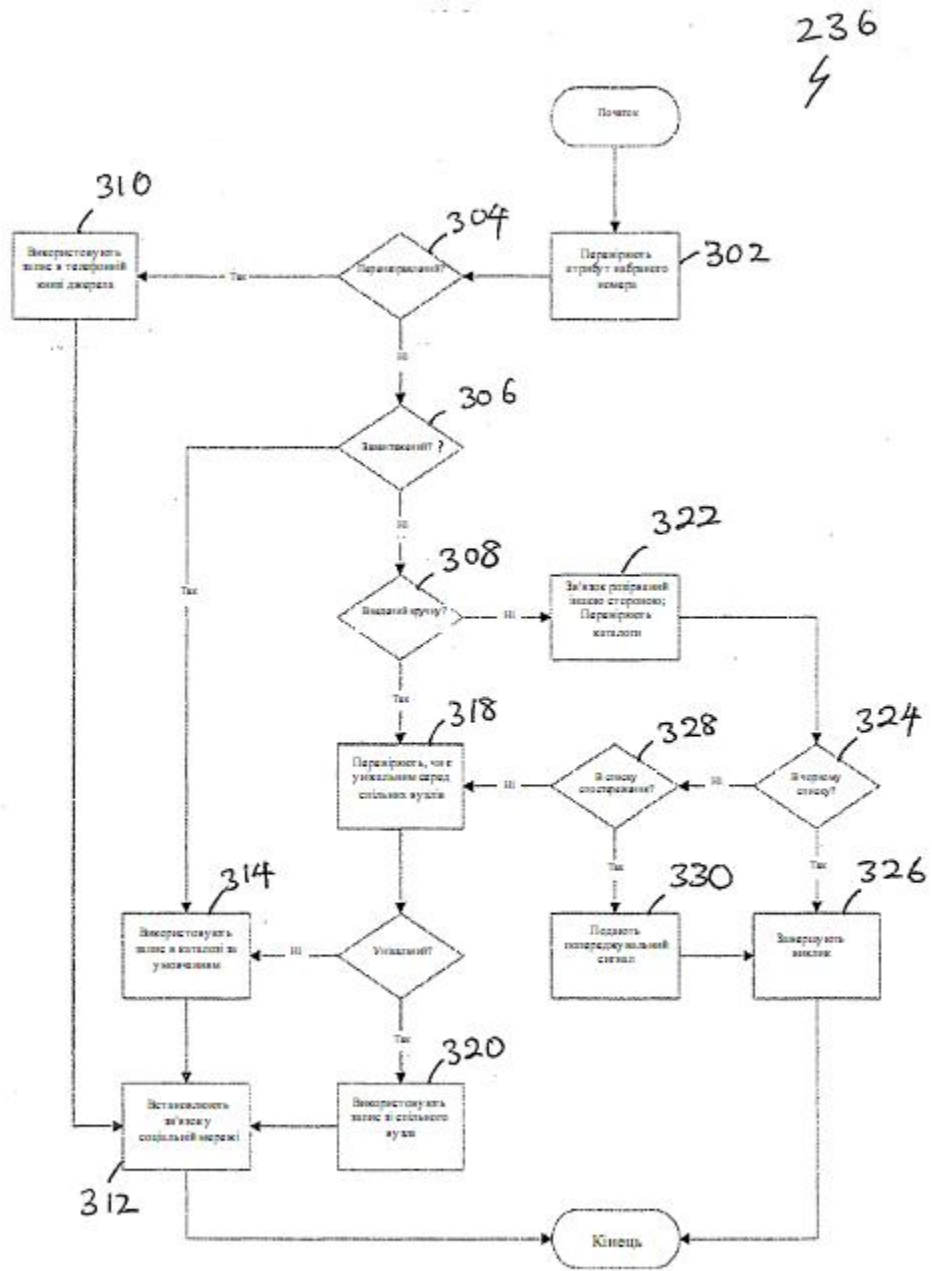
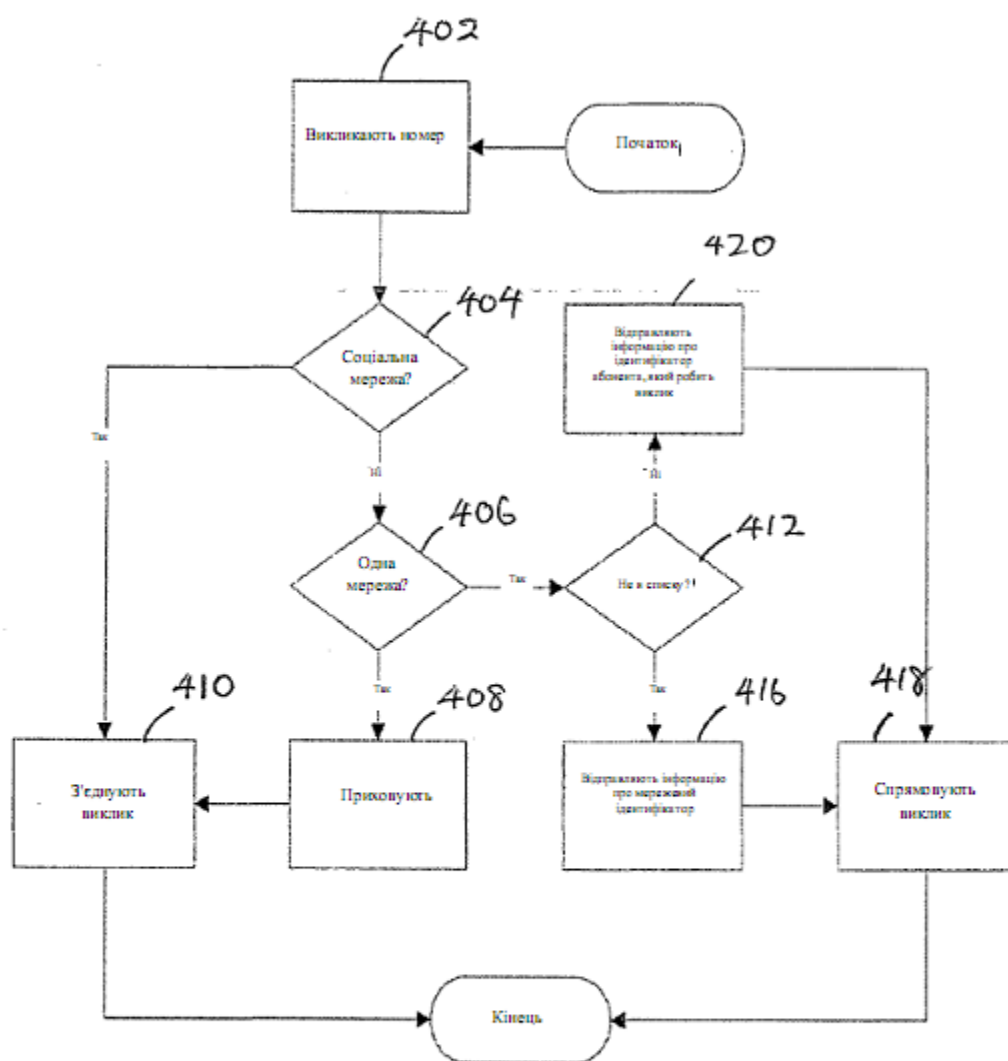


Fig. 3



Фіг. 4

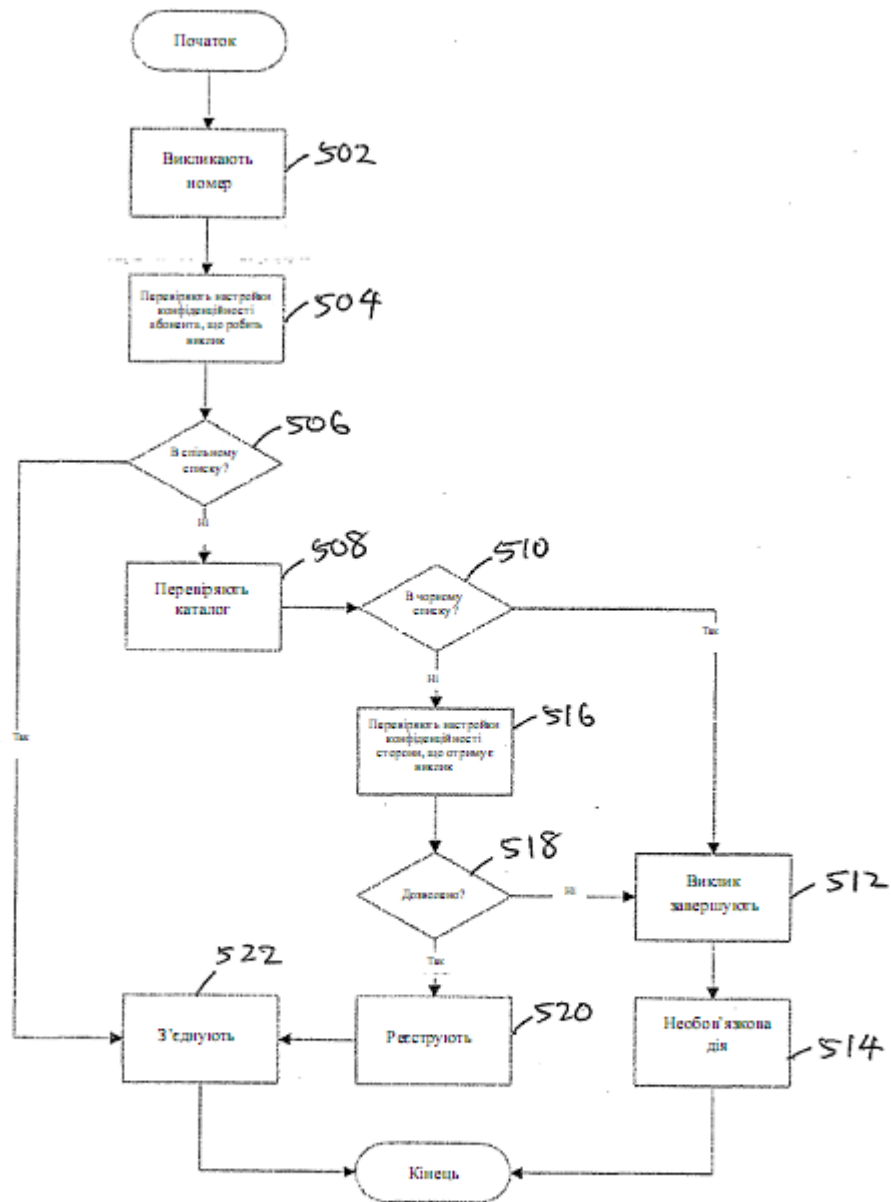
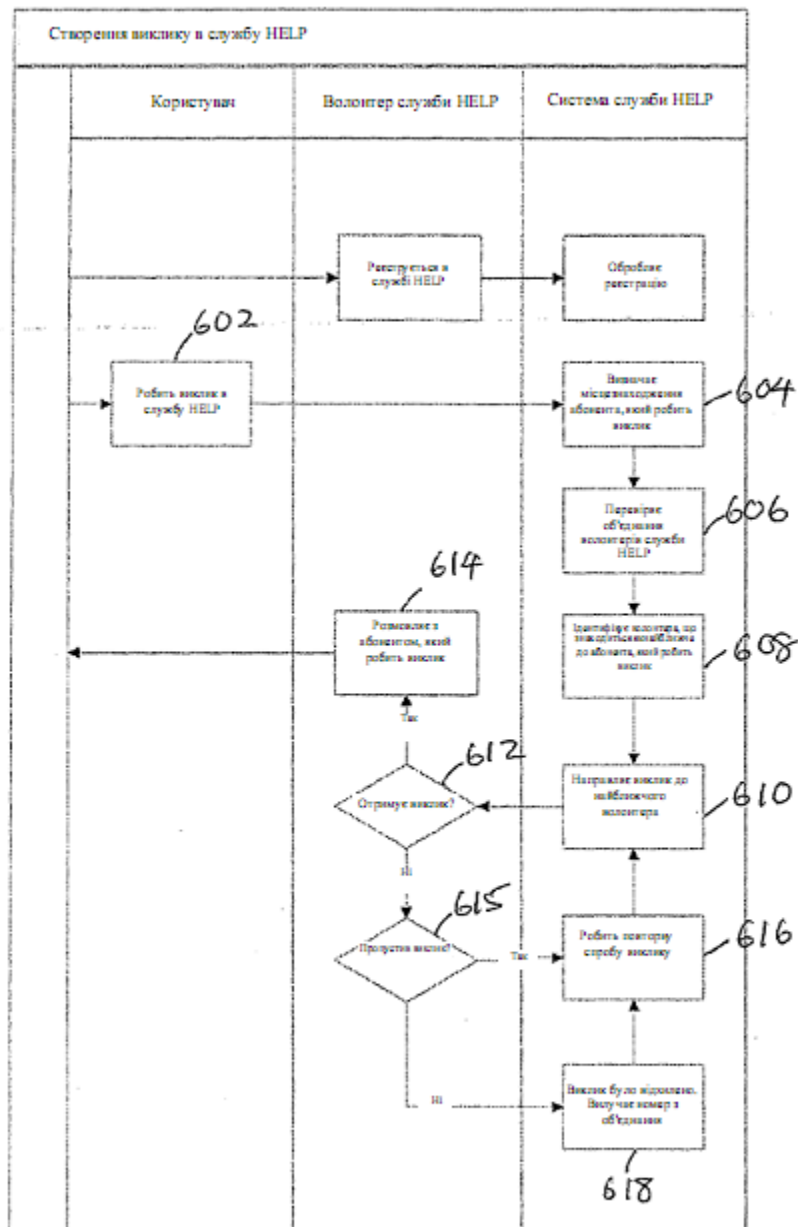


Fig. 5



Фіг. 6

Комп'ютерна верстка Д. Шеверун

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

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