



УКРАЇНА

(19) UA

(11) 88621

(13) C2

(51) МПК (2009)

H04L 12/46

H04L 29/06

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ВСТАНОВЛЕННЯ VPN-З'ЄДНАННЯ

1

(21) а200602940
(22) 17.08.2004
(24) 10.11.2009
(86) РСТ/NO2004/000249, 17.08.2004
(31) 20033655
(32) 18.08.2003
(33) NO
(46) 10.11.2009, Бюл.№ 21, 2009 р.
(72) КАЛЬВЕТ ХУАН КАРЛОС ЛОПЕС, NO
(73) ТЕЛЕНОР АСА, NO
(56) US 2003/070067 A1, 10.04.2003
EP 0944203 A, 22.09.1999
DE 10140446 A, 06.03.2003
(57) 1. Спосіб встановлення з'єднання типу "віртуальна приватна мережа" у мережі (110) зв'язку між першим комп'ютером (150) і другим комп'ютером (160), підключеними до зазначеної мережі, причому перший мобільний комунікаційний термінал (154) виконаний з можливістю встановлення локального зв'язку з першим комп'ютером (150), а другий мобільний комунікаційний термінал (164) має можливість встановлення локального зв'язку із другим комп'ютером (160), який відрізняється тим, що зазначений спосіб здійснюється за допомогою другого мобільного терміналу (164) і включає такі кроки:
здійснюють одержання (308) зашифрованого повідомлення-запиту від першого мобільного терміналу (154), причому повідомлення-запит містить такі компоненти:
інформація, що включає мережну адресу першого комп'ютера (150);
спільний секретний об'єкт;
здійснюють дешифрування (310) зазначеного повідомлення-запиту за допомогою закритого ключа (PrivKey), який належить другому мобільному терміналу (164);
здійснюють посилення (312) повідомлення конфігурації, що містить мережну адресу першого комп'ютера (150) та спільний секретний об'єкт, на другий комп'ютер (160);
здійснюють одержання (316) команди-відповіді від другого комп'ютера (160);
здійснюють передачу (318) повідомлення-відповіді, що містить інформацію, яка включає мережну адресу другого комп'ютера (160), на перший

2

мобільний термінал (154), виконувати після одержання команди-запиту,
в результаті чого перший комп'ютер (150) набуває можливості одержання мережної адреси другого комп'ютера (160); крім того, другий комп'ютер (160) набуває можливості одержання мережної адреси першого комп'ютера (150) і спільного секретного об'єкта, що, у свою чергу, дозволяє встановити з'єднання типу "віртуальна приватна мережа" між першим комп'ютером (150) та другим комп'ютером (160).

2. Спосіб за п. 1, який відрізняється тим, що закритий ключ (PrivKey) зберігається в модулі ідентифікації абонента, встановленого в другому мобільному терміналі (164).

3. Спосіб за п. 2, який відрізняється тим, що команда-відповідь містить у собі повідомлення-відповідь.

4. Спосіб за п. 3, який відрізняється тим, що повідомлення-запит надходить із мережі (120) мобільного зв'язку, причому повідомлення-відповідь посилається в мережу (120) мобільного зв'язку.

5. Спосіб за п. 4, який відрізняється тим, що мережа (120) мобільного зв'язку є мережею мобільного телефонного зв'язку, сумісною зі стандартом GSM, причому повідомлення-запит і повідомлення-відповідь є SMS-повідомленнями.

6. Спосіб за п. 5, який відрізняється тим, що повідомлення-запит шифрується за допомогою відкритого ключа (PubKey), який належить другому мобільному терміналу (164), а також тим, що повідомлення-відповідь шифрується за допомогою закритого ключа (PrivKey), який належить другому мобільному терміналу (164).

7. Спосіб за одним з пп. 1-6, який відрізняється тим, що локальна взаємодія між другим мобільним терміналом (164) та другим комп'ютером (160) здійснюється на основі бездротового з'єднання малої дальності, реалізованого у відповідності зі специфікацією Bluetooth.

8. Спосіб за одним з пп. 1-7, який відрізняється тим, що локальне з'єднання між першим мобільним терміналом (154) та першим комп'ютером (150) є бездротовим з'єднанням малої дальності, реалізованим у відповідності зі специфікацією Bluetooth.

(13) C2

(11) 88621

(19) UA

9. Спосіб за одним з пп. 1-7, який **відрізняється** тим, що перший мобільний термінал (154) і перший комп'ютер (150) об'єднані в один мобільний пристрій, наприклад персональний цифровий асистент, причому зазначена локальна взаємодія між першим мобільним терміналом (154) і першим комп'ютером (150) здійснюється усередині зазначеного мобільного пристрою на основі провідного з'єднання.

10. Мобільний комунікаційний термінал (164) для реалізації функції встановлення з'єднання типу "віртуальна приватна мережа" між першим комп'ютером (150) і другим комп'ютером (160) у мережі (110) зв'язку, який включає такі компоненти: радіочастотний компонент мобільного телефону, що забезпечує радіозв'язок;

комунікаційний інтерфейс, що забезпечує локальне з'єднання з комп'ютером, причому зазначений мобільний термінал виконаний з можливістю здійснення способу за одним з пп. 1-9.

11. Система для встановлення з'єднання типу "віртуальна приватна мережа" у мережі (110) зв'язку, яка включає перший комп'ютер (150) і другий комп'ютер (160), підключені до мережі (110), причому перший мобільний комунікаційний термінал (154) має можливість встановлення локального з'єднання з першим комп'ютером (150), а другий мобільний термінал (164) має можливість встановлення локального з'єднання із другим комп'ютером (160), яка **відрізняється** тим, що другий мобільний комунікаційний термінал (164) виконаний з можливістю здійснення способу за одним з пп. 1-9.

Даний винахід в основному належить до області захисту інформації і, зокрема, до області встановлення з'єднання типу "віртуальна приватна мережа" (Virtual Private Network, далі позначається як "VPN-мережа") у мережі зв'язку між першим і другим комп'ютерами, підключеними до цієї мережі.

Зокрема, перший мобільний комунікаційний термінал має функцію встановлення локального зв'язку з першим комп'ютером, другий мобільний комунікаційний термінал має функцію встановлення локального зв'язку із другим комп'ютером, і спосіб за винаходом здійснюється зазначеним другим мобільним терміналом.

Винахід також стосується мобільного комунікаційного терміналу, що має функцію здійснення зазначеного способу, і системи, компонентом якої є мобільний комунікаційний термінал, що має функцію здійснення зазначеного способу.

Віртуальна приватна мережа є приватною мережею, що функціонує на основі мережі загальної користування і, зокрема, її телекомунікаційної інфраструктури. VPN-мережі широко використовуються для надання мобільним і видаленим користувачам можливості підключення до внутрішніх локальних мереж своїх компаній.

В останні роки широко застосовується технологія забезпечення доступу до VPN-мереж, відома як IPsec (Internet Protocol Security, безпека IP-протоколів). Безпека, забезпечувана при використанні IPsec, базується на застосуванні протоколів тунелювання і процедур захисту.

Для встановлення з'єднання з використанням IPsec по VPN-тунелю між двома кінцевими або клієнтськими комп'ютерами, підключеними до Інтернету, має виконуватися така умова: на кожному комп'ютері повинні бути присутні певні конфігураційні дані, у тому числі IP-адреси обох комп'ютерів, і певний секретний об'єкт, спільний для цих комп'ютерів, наприклад, випадкове число або буквено-цифровий рядок. При наявності цієї інформації кожен комп'ютер може виконувати процес конфігурування, в результаті якого встановлюється з'єднання VPN.

Існує безпечний спосіб обміну інформацією в межах певної організації, промислової галузі або

країни, а також у світовому масштабі, відомий як PKI (Public Key Infrastructure, інфраструктура відкритого ключа). В PKI використовується спосіб асиметричного шифрування, також відомий як "спосіб з відкритим/закритим ключем", що застосовується для шифрування ідентифікаторів та документів/повідомлень. Орган видачі повноважень (certificate authority, CA) видає цифрові сертифікати (цифрові ідентифікатори), які служать для підтвердження легітимності осіб та організацій у загальнодоступних мережах, наприклад, в Інтернеті.

Задача, на рішення якої спрямований даний винахід, полягає в створенні способу, пристрою та системи, що реалізують встановлення з'єднання типу "віртуальна приватна мережа" у мережі зв'язку між першим та другим комп'ютерами, підключеними до цієї мережі.

Інша задача даного винаходу полягає в створенні способу, пристрою та системи, що є економічно ефективними і легкими в реалізації та користуванні.

Ще одна задача даного винаходу полягає в створенні способу, пристрою та системи, які використовують наявну інфраструктуру, наприклад, великомасштабну систему мобільного зв'язку, а також технології, що розвиваються, такі як зв'язок Bluetooth (технологія бездротового ближнього короткохвильового радіозв'язку, що дозволяє поєднувати пристрої різних типів для передачі мови і даних).

Ще одна задача даного винаходу полягає в створенні способу, пристрою та системи, що надають звичайним клієнтам можливості легкого встановлення VPN-з'єднань, які дозволяли б спростити впровадження нових методів електронної комерції та рішень з оплати в режимі on-line.

Рішення щонайменше деяких з перелічених вище задач досягається за допомогою способу, мобільного комунікаційного терміналу і системи, описаних у незалежних пунктах прикладеної формули винаходу. Інші істотні переваги реалізуються у варіантах здійснення, описаних в залежних пунктах формули винаходу.

Перелік Фігур креслень

Ознаки і переваги даного винаходу стануть зрозумілі з наведеного нижче опису, який містить

посилання на прикладені креслення, що ілюструють варіант здійснення винаходу, який не вносить жодних обмежень. На кресленнях:

на Фіг.1 наведена структурна схема системи для реалізації способу відповідно до даного винаходу;

на Фіг.2 наведена часова діаграма, що відображає весь процес встановлення VPN-з'єднання;

на Фіг.3 показана блок-схема способу відповідно до даного винаходу.

На Фіг.1 зображена структурна схема, що описує систему, в якій використовується спосіб за даним винаходом.

Перший клієнтський комп'ютер 150 (A) і другий клієнтський комп'ютер (B) на вихідному етапі підключаються до глобальної цифрової мережі 110 зв'язку, наприклад, Інтернету.

Задача винаходу полягає у встановленні VPN-з'єднання між A і B, тобто, між першим клієнтським комп'ютером 150 та другим клієнтським комп'ютером 160.

Кожному із клієнтських комп'ютерів 150, 160 призначається адреса (IP-адреса) у мережі 110. Крім того, на кожному клієнтському комп'ютері 150, 160 є програмне забезпечення, наприклад, Інтернет-браузер, що дозволяє одержувати доступ до World Wide Web за допомогою цього комп'ютера. Далі, кожен клієнтський комп'ютер 150, 160 має інтерфейс локального зв'язку, наприклад, радіочастотний Bluetooth-трансивер, призначений для забезпечення локального зв'язку малої дальності з видаленими периферійними пристроями.

Специфікація Bluetooth стосується області комп'ютерної техніки і телекомунікацій. Вона описує простий спосіб взаємодії між мобільними телефонами, комп'ютерами і персональними цифровими асистентами (personal digital assistants, PDAs) за допомогою локального (з малим радіусом дії) бездротового з'єднання. Типовий Bluetooth-пристрій є трансивером, виконаним у вигляді мікросхеми і здійснюючим приймання/передачу сигналу в частотному діапазоні 2,45ГГц. Кожен пристрій має унікальну 48-бітну адресу, що відповідає стандарту IEEE 802. З'єднання можуть бути двоточковими або багатоточковими. Максимальна дальність зв'язку становить 10 метрів. Використовуваний принцип стрибкоподібної зміни частот дозволяє встановлювати зв'язок між пристроями навіть у місцях з високим рівнем електромагнітних перешкод. При роботі Bluetooth-з'єднань малої дальності використовуються заздалегідь передбачені в Bluetooth функції шифрування і аутентифікації.

Далі, на кожному з клієнтських комп'ютерів 150, 160 є програмне забезпечення, призначене для взаємодії з видаленими периферійними пристроями за допомогою зазначеного інтерфейсу локального зв'язку.

Перший мобільний термінал 154 функціонує в парі з першим клієнтським комп'ютером 150. Перший мобільний термінал 150 має дві незалежні функції зв'язку. По-перше, мобільний термінал 154 має інтерфейс зв'язку, призначений для локальної взаємодії з першим клієнтським комп'ютером 150, який є, наприклад, радіочастотним Bluetooth-трансивером. По-друге, мобільний термінал 154

має функцію роботи в мережі 120 мобільного телефонного зв'язку на основі радіочастотного з'єднання з базовою станцією 122, в зоні покриття якої перебуває мобільний термінал 154. Зокрема, у цій мережі мобільного телефонного зв'язку надається послуга обміну повідомленнями, наприклад, послуга відправлення і приймання SMS, що дозволяє передавати цифрові повідомлення з мобільного терміналу 154 на інший мобільний термінал, який працює в мережі 120 мобільного телефонного зв'язку.

Аналогічно, другий мобільний термінал 164 функціонує в парі з другим клієнтським комп'ютером 160 на стороні B. Другий мобільний термінал 164 також має дві незалежні функції зв'язку. По-перше, мобільний термінал 164 має інтерфейс зв'язку, призначений для локальної взаємодії із другим клієнтським комп'ютером 160, який є, наприклад, радіочастотним Bluetooth-трансивером. По-друге, мобільний термінал 164 має функцію роботи в мережі 120 мобільного телефонного зв'язку на основі радіочастотного з'єднання з базовою станцією 124, в зоні покриття якої перебуває мобільний термінал 164. Послуга обміну повідомленнями, надавана в мережі 120 мобільного телефонного зв'язку, наприклад, послуга відправлення і приймання SMS, дозволяє передавати цифрові повідомлення з мобільного терміналу 164 на інший мобільний термінал, що працює в цій мережі, і приймати такі повідомлення. Як правило, мережа 120 мобільного телефонного зв'язку є GSM-мережею і дозволяє передавати і приймати SMS-повідомлення за допомогою терміналів мобільного зв'язку, підключених до мережі 120.

В кожному з мобільних терміналів 154, 164 є SIM-карта (Subscriber Identification Module, модуль ідентифікації абонента).

На Фіг.2 наведена часова діаграма, що ілюструє весь процес встановлення VPN-з'єднання між першим клієнтським комп'ютером 150 і другим клієнтським комп'ютером 160. При описі системи на Фіг.2 для наочності також використовуються посилання на Фіг.1.

Для встановлення VPN-тунелю між першим клієнтським комп'ютером 150 і другим клієнтським комп'ютером 160 необхідна наявність таких конфігураційних даних на кожному із клієнтських комп'ютерів 150, 160:

- (1) IP-адреси обох клієнтських комп'ютерів;
- (2) певний секретний об'єкт, спільний для обох комп'ютерів.

Подальший процес встановлення VPN-з'єднання або тунелю на основі зазначених конфігураційних даних відповідає звичайній процедурі, відомій фахівцям в даній області техніки, оснований на специфікації IPSec.

На початковому кроці 202 процесу користувач вводить запит на першому клієнтському комп'ютері 150. Запит містить у собі ідентифікатор другого мобільного терміналу 164, наприклад, його телефонний номер.

Потім, на кроці 204 генерації секретного об'єкта, перший клієнтський комп'ютер 150 генерує "спільний секретний об'єкт", наприклад, псевдовипадкове число або буквено-цифровий рядок.

Далі, на кроці 206 передачі команди-запиту, перший клієнтський комп'ютер 150 передає на перший мобільний термінал 154 команду-запит по першому локальному Bluetooth-з'єднанню 152. Вбудовані функції зв'язку стандарту Bluetooth забезпечують передачу даних у зашифрованій формі, що є істотним для збереження безпеки та конфіденційності. В зазначену команду входять дані, що представляють згенерований спільний секретний об'єкт, IP-адресу першого клієнтського комп'ютера 150 та ідентифікатор другого мобільного терміналу 164; за цією командою перший мобільний термінал А посилає повідомлення-запит на наступному кроці 208.

У відповідь на отриману команду-запит перший мобільний термінал ініціює крок 208 передачі повідомлення-запиту, протягом якого перший мобільний термінал 154 посилає повідомлення-запит, наприклад, SMS-повідомлення, на ідентифікований другий мобільний термінал 164 по мережі 120 мобільного зв'язку. Повідомлення-запит містить у собі спільний секретний об'єкт та IP-адресу першого клієнтського комп'ютера 150.

При виконанні кроків 206 і 208 перший мобільний термінал 154, краще, розглядається як "неінтелектуальний" мобільний термінал, керування функціями якого може здійснювати перший клієнтський комп'ютер 150 за допомогою Bluetooth-з'єднання. Генерація повідомлення-запиту в цьому випадку виконується першим клієнтським комп'ютером 150, і це згенероване повідомлення-запит буде міститися в команді-запиті, надісланій на кроці 206; після її одержання перший мобільний термінал 154 виконує пересилання повідомлення-запиту з його попереднім перетворенням на SMS.

Зазначене повідомлення-запит шифрується за допомогою відкритого ключа, який належить другому мобільному терміналу 164.

Після одержання SMS-повідомлення другий мобільний термінал 164 виконує крок 210 дешифрування запиту, що полягає в дешифруванні повідомлення-запиту за допомогою закритого ключа, який належить другому мобільному терміналу 164. Зазначений закритий ключ, краще, зберігається в SIM-карті (модулі ідентифікації передплатника), встановлений в другому мобільному терміналі. Для одержання доступу до закритого ключа, що зберігається в SIM-карті, оператору другого мобільного терміналу 164 необхідно ввести PIN-код на мобільному терміналі 164.

Після дешифрування повідомлення-запиту другий мобільний термінал 164 виконує крок 212 передачі повідомлення конфігурації; протягом цього кроку здійснюється передача конфігураційних даних, у тому числі IP-адреси першого клієнтського комп'ютера 150 та спільного секретного об'єкта, по Bluetooth-з'єднанню на другий клієнтський комп'ютер 160.

Другий клієнтський комп'ютер 160, що одержав повідомлення з конфігураційними даними, тобто, після надходження конфігураційних даних, що містять як IP-адресу першого клієнтського комп'ютера, так і спільний секретний об'єкт, ініціює процес 214 конфігурування, який включає конфігурування тунельного VPN-з'єднання між першим клієнтсь-

ким комп'ютером 150 та другим клієнтським комп'ютером 160.

Далі другий клієнтський комп'ютер 160 виконує крок 216 посилання команди-відповіді. На цьому кроці виконується посилання команди-відповіді другому клієнтському комп'ютеру по другому Bluetooth-з'єднанню 162.

У відповідь на одержання команди-відповіді другий мобільний термінал ініціює крок 218 передачі повідомлення-відповіді, протягом якого другий мобільний термінал 164 посилає повідомлення-відповідь, наприклад, SMS-повідомлення, на перший мобільний термінал 154 по мережі 120 мобільного зв'язку. Це повідомлення-відповідь містить IP-адресу другого клієнтського комп'ютера 160.

При виконанні кроків 216 і 218 другий мобільний термінал 164, краще, розглядається як "неінтелектуальний" мобільний термінал, керування функціями якого може здійснювати другий клієнтський комп'ютер 160 за допомогою Bluetooth-з'єднання. У цьому випадку другий клієнтський комп'ютер 160 генерує повідомлення-відповідь, і команда-відповідь, надіслана на кроці 216, буде містити згенероване повідомлення-відповідь; після його одержання другий мобільний термінал 164 виконує пересилання повідомлення-відповіді з його попереднім перетворенням на SMS.

Зазначене повідомлення-відповідь шифрується за допомогою закритого ключа, який належить другому мобільному терміналу 164 і розташований в його SIM-карті.

Після одержання повідомлення-відповіді першим мобільним терміналом 154 на кроці 218 виконується крок 220 дешифрування повідомлення-відповіді, на якому здійснюється дешифрування повідомлення-відповіді. Крок 220 дешифрування в основному відповідає описаному раніше кроку 210 дешифрування, виконуваному другим мобільним терміналом 164.

Після кроку 220 дешифрування перший мобільний термінал 154 виконує крок 222 передачі повідомлення конфігурації, протягом якого здійснюється передача конфігураційних даних, в тому числі IP-адреси другого клієнтського комп'ютера, по локальному Bluetooth-з'єднанню на перший клієнтський комп'ютер.

Таким чином, в цей момент на першому клієнтському комп'ютері є спільний секретний об'єкт та IP-адреса другого клієнтського комп'ютера, що дозволяє першому клієнтському комп'ютеру 150 ініціювати процес 224 конфігурування VPN-тунелю. Крім того, слід зазначити, що другий клієнтський комп'ютер 160 до цього моменту ініціює процес 214 конфігурування. Виконання процесів 214, 224 конфігурування забезпечує можливість створення VPN-тунелю між першим клієнтським комп'ютером 150 та другим клієнтським комп'ютером 160.

На Фіг.3 наведена схема процесу, що ілюструє спосіб за даним винаходом.

Повний процес, показаний на Фіг.2, включає кроки, виконувані різними сторонами. Спосіб, показаний на Фіг.3, в рамках вищеописаного спільного процесу стосується кроків, виконуваних другим мобільним терміналом 164.

Даний спосіб дозволяє встановлювати з'єднання типу "віртуальна приватна мережа", зокрема, тунель відповідно до специфікації IPsec, у мережі 110 зв'язку між першим комп'ютером 150 та другим комп'ютером 160, підключеними до цієї мережі.

При описі зазначеного способу також використовуються посилання на систему, зображену на Фіг.1. Більш конкретно: перший мобільний термінал 154 має функцію встановлення локального зв'язку (наприклад, Bluetooth) з першим комп'ютером 150, другий мобільний термінал 164 має функцію встановлення локального зв'язку (наприклад, Bluetooth) із другим комп'ютером 160. Крім того, мобільні термінали 154, 164 мають функцію взаємодії між собою по мережі 120 мобільного зв'язку.

Кроки описуваного способу виконуються другим мобільним терміналом 164. Вихідний етап способу позначений посиланням 301.

Спочатку, на кроці 308 одержання запиту, відбувається одержання зашифрованого повідомлення-запиту. Цей крок відповідає кроку 208 посилання запиту на Фіг.2, на якому відбувається посилання повідомлення-запиту першим мобільним терміналом 154. Це повідомлення-запит містить інформацію, яка включає мережну адресу (IP-адресу) першого комп'ютера 150 і спільний секретний об'єкт, згенерований першим клієнтським комп'ютером 150 на кроці 204 і переданий по локальному Bluetooth-з'єднанню на перший мобільний термінал 154 на кроці 206 (Фіг.2). Повідомлення-запит, краще, має форму SMS і передається/приймається за допомогою мережі 120 мобільного зв'язку. Зазначене повідомлення-запит шифрується за допомогою відкритого ключа, який належить мобільному терміналу 164.

На кроці 309 перевірки виконується перевірка факту одержання повідомлення запиту; процес за способом переходить до кроку 310 лише в тому випадку, якщо воно було отримано. У протилежному випадку очікується надходження цього повідомлення-запиту.

На кроці 310 дешифрування, що відповідає кроку 210 дешифрування на Фіг.2, другий мобільний термінал 164 здійснює дешифрування повідомлення-запиту за допомогою закритого ключа, який належить мобільному терміналу 164. Як описано вище з посиланнями на Фіг.2, цей закритий ключ, краще, зберігається в SIM-карті, встановленій в другому мобільному терміналі 164.

По закінченні кроку 310 дешифрування другий мобільний термінал 164 виконує крок 312 посилання повідомлення конфігурації, що відповідає кроку 212 на Фіг.2. На цьому етапі здійснюється передача конфігураційних даних, у тому числі IP-адреси першого клієнтського комп'ютера 150 та спільного секретного об'єкта, по локальному Bluetooth-з'єднанню на другий клієнтський комп'ютер 160.

Далі другий мобільний термінал виконує крок 316 одержання команди-відповіді, аналогом якого є крок 216 передачі команди-відповіді, виконуваний другим клієнтським комп'ютером (Фіг.2). На цьому кроці 316 відбувається одержання команди-відповіді від другого клієнтського комп'ютера 160 по другому Bluetooth-з'єднанню 162.

На кроці 317 перевірки виконується перевірка факту одержання команди-відповіді; процес переходить до кроку 318 посилання відповіді тільки в тому випадку, якщо вона була отримана. У протилежному випадку очікується надходження цієї команди-відповіді.

У відповідь на одержання команди-відповіді другий мобільний термінал ініціює крок 318 передачі повідомлення-відповіді, що відповідає кроку 218 на Фіг.2. На цьому кроці 318 другий мобільний термінал 164 посилає повідомлення-відповідь (SMS-повідомлення) на перший мобільний термінал 154 по мережі 120 мобільного зв'язку. Це повідомлення-відповідь містить IP-адресу другого клієнтського комп'ютера 160.

При виконанні кроків 316-318 другий мобільний термінал 164, краще, розглядається як "неінтелектуальний" мобільний термінал, керування функціями якого може здійснювати другий клієнтський комп'ютер 160 за допомогою Bluetooth-з'єднання. У цьому випадку другий клієнтський комп'ютер 160 генерує повідомлення-відповідь, і команда-відповідь, надіслана на кроці 316, буде містити згенероване повідомлення-відповідь; після його одержання другий мобільний термінал 164 виконує пересилання повідомлення-відповіді з його попереднім перетворенням на SMS.

Зазначене повідомлення-відповідь шифрується за допомогою закритого ключа, який належить другому мобільному терміналу 164 і розташований в його SIM-карті.

По завершенні описаних кроків, на кінцевій стадії 319, перший клієнтський комп'ютер 150 одержує IP-адресу другого комп'ютера 160, що міститься в переданому повідомленні-відповіді, від першого мобільного терміналу 154. Як показано в описі всього процесу на Фіг.2, при цьому передбачається, що перший мобільний термінал 154 виконав крок 220 дешифрування і крок 222 посилання конфігураційних даних. Крім того, другий клієнтський комп'ютер тепер може виконати крок 214 конфігурування VPN-тунелю із застосуванням даних з повідомлення конфігурації, переданого другим мобільним терміналом 164 на кроці 312.

Таким чином, в цей момент на обох клієнтських комп'ютерах 150 та 160 є всі конфігураційні дані, необхідні для встановлення VPN-тунелю між першим комп'ютером 150 та другим комп'ютером 160.

Даний винахід буде застосовним, зокрема, у тому випадку, коли мережа 110 підтримує функцію глобальної адресації, якій відповідає нова, дедалі ширше використовувана специфікація Інтернет-протоколів IPv6. Варіанти здійснення, основані на поширеній зараз специфікації IPv4, передбачають використання пристроїв трансляції мережних адрес (Network Address Translation, NAT). Недолік NAT-мереж на основі IPv4 полягає в тому, що в них використовуються адреси, які не є глобальними. Це означає, що комп'ютер посилає адресу, яка є дійсною лише в межах даної NAT-мережі, і доступ до нього ззовні неможливий. Двоточковий зв'язок встановити не можна; альтернатива полягає в створенні тунелю між двома NAT-серверами, але в цьому випадку встановлений зв'язок буде

повністю відкритим в межах NAT-мережі і його безпека буде порушена.

Розкриття винаходу у вищенаведеному описі оснований на окремому прикладі. Фахівцю в даній області техніки зрозуміло, що в межах області, описуваної пунктами прикладеної формули винаходу, можлива велика кількість можливих варіантів і альтернатив зазначеного детально описаного варіанта здійснення.

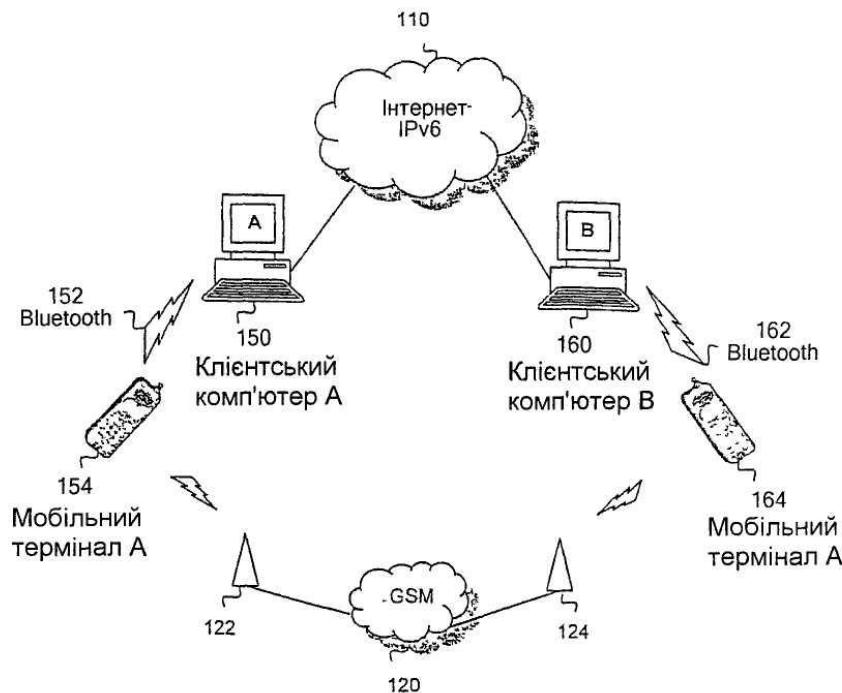
Наприклад, перший мобільний термінал 154 і перший комп'ютер 150, які описані як окремі пристрої, що взаємодіють за допомогою Bluetooth-з'єднання малої дальності, можуть бути об'єднані в один мобільний пристрій, наприклад, персональний цифровий асистент (Personal Digital Assistant, PDA). Локальний зв'язок між першим мобільним терміналом 154 і першим клієнтським комп'ютером 150 у цьому випадку функціонує усередині зазначеного мобільного пристрою.

Зазначене Bluetooth-з'єднання описано як краще рішення локального зв'язку малої дальності між клієнтським комп'ютером (150, 160) і відповідним мобільним терміналом (154, 164, відповідно), але фахівцю в даній області техніки буде також ясно, що можуть бути використані інші способи, такі як інфрачервоний зв'язок або провідне з'єд-

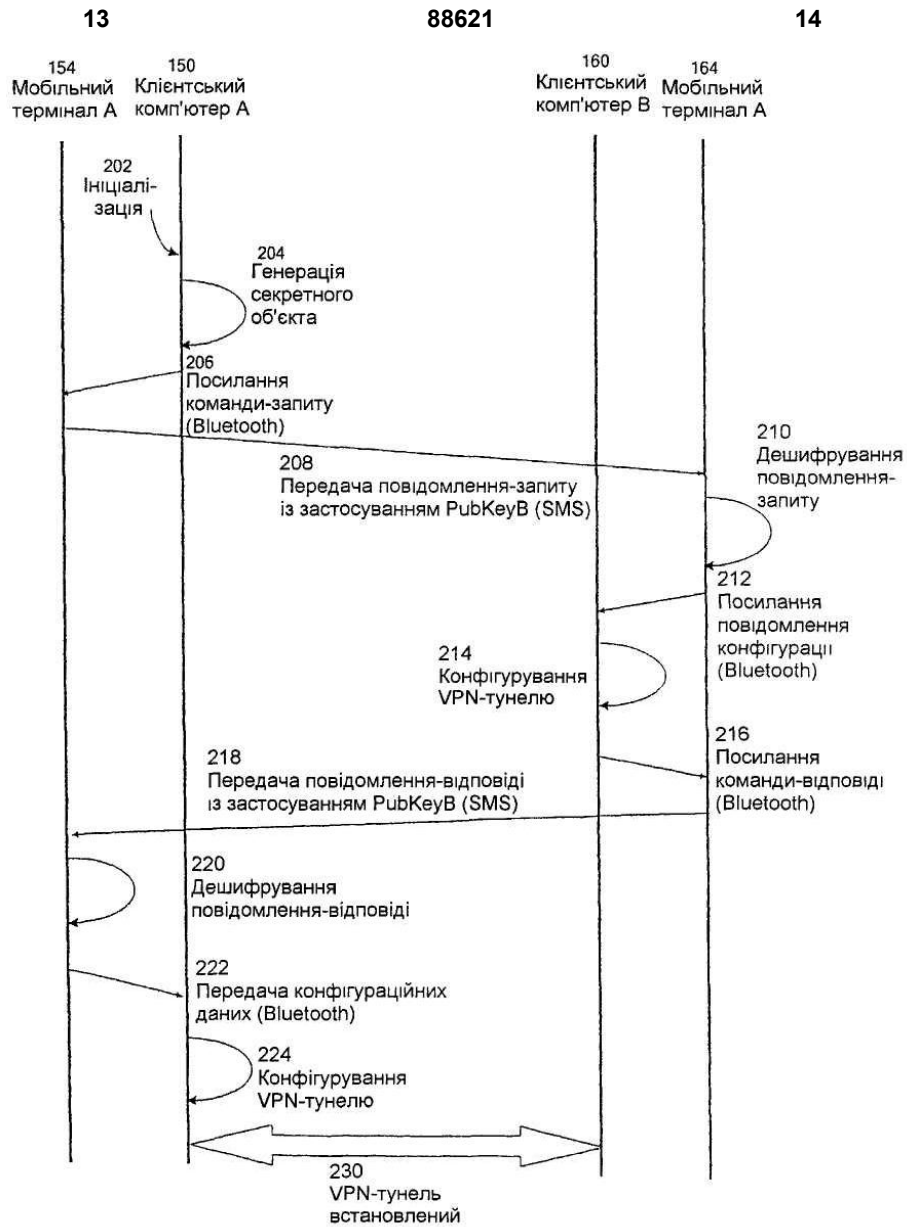
нання. В будь-якому випадку, локальний зв'язок повинен включати вбудовані схеми шифрування з метою збереження безпеки.

Як мобільні термінали можуть використовуватися звичайні мобільні телефони, наприклад, телефони GSM, обладнані додатковими засобами зв'язку малої дальності, наприклад, Bluetooth. З іншого боку, мобільні термінали можуть бути й більш складними пристроями зв'язку та обробки, такими як PDA, обладнані модулями мобільного зв'язку (наприклад, стандарту GSM) і, наприклад, Bluetooth-трансивером для забезпечення взаємодії.

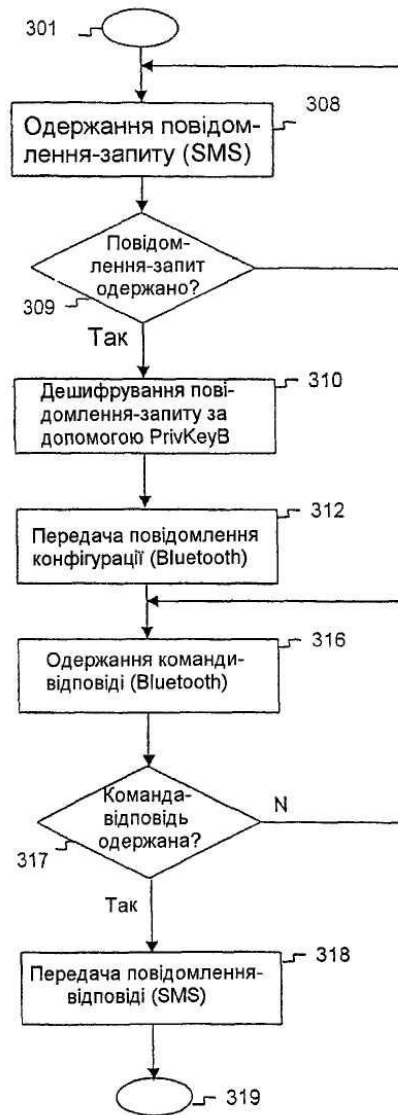
Процес на Фіг.2 в цілому ініціюється користувачем, що працює з першим клієнтським комп'ютером 150. Природно, можливо ініціювати цей процес за допомогою першого мобільного термінала 154, який потім встановлює зв'язок малої дальності з першим клієнтським комп'ютером 150. Крім того, можливо перенести функцію виконання кроку 204 генерації спільного секретного об'єкта на перший мобільний термінал 154. Зокрема, такий варіант може мати місце у випадку, коли описаний процес виконується пристроєм типу PDA або телефоном, що одночасно функціонує як клієнтський комп'ютер.



ФІГ. 1



ФІГ. 2



ФІГ. 3