



УКРАЇНА

(19) **UA** (11) **86753** (13) **U**  
(51) МПК (2013.01)  
**G07C 13/00**  
**H04N 7/15** (2006.01)

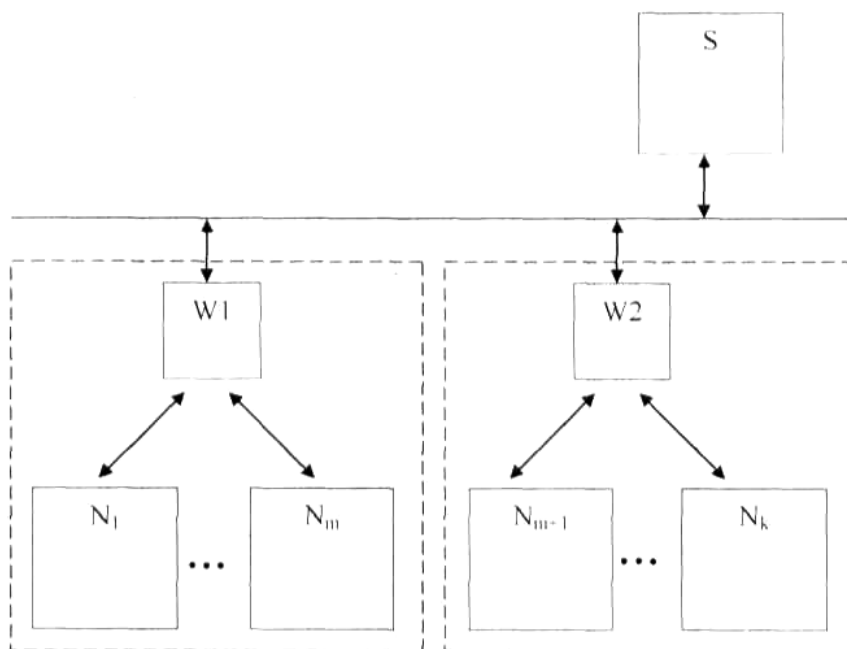
ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

**(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ**

(21) Номер заявки: <b>u 2013 08533</b>	(72) Винахідник(и): <b>Казимир Володимир Вікторович (UA), Зайцев Сергій Васильович (UA), Риндич Євген Володимирович (UA)</b>
(22) Дата подання заявки: <b>08.07.2013</b>	
(24) Дата, з якої є чинними права на корисну модель: <b>10.01.2014</b>	(73) Власник(и): <b>ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ, вул. Шевченка, 95, м. Чернігів, 14027 (UA)</b>
(46) Публікація відомостей про видачу патенту: <b>10.01.2014, Бюл.№ 1</b>	

**(54) ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ЗАХИЩЕНОЇ СИСТЕМИ ГОЛОСОВОГО КОНФЕРЕНЦ-ЗВ'ЯЗКУ В IP-МЕРЕЖАХ****(57) Реферат:**

Програмно-апаратний комплекс захищеної системи голосового конференц-зв'язку в IP-мережах містить сервер (S), який з'єднаний з дротовим (W1) та бездротовим (W2) маршрутизаторами, які в свою чергу з'єднані з робочими місцями абонентів ( $N_1 \dots N_m$ ) при дротовому підключенні та ( $N_{m+1} \dots N_k$ ) при бездротовому підключенні.

**UA 86753 U**



Корисна модель належить до інформаційно-обчислювальної техніки і може бути використана для проведення захищеного голосового конференц-зв'язку. Технічним результатом є створення комплексу багатоабонентської захищеної передачі даних в IP-мережах в режимі реального часу.

Сучасний етап розвитку конференц-систем та їх висока гетерогенність вимагають від мережевого обладнання чіткої взаємодії й можливості в реальному часі гарантувати якісну передачу даних з одного сегмента мережі в інший. Одним із найперспективніших на сьогодні напрямів у розвитку конференц-систем є розробка корпоративних конференц-систем на базі протоколу IP, які дозволяють створювати голосові конференції з дотриманням вимог конфіденційності інформації, що передається. Існує багато інформаційних технологій, направлених на досягнення цієї мети, але більшість з них не може забезпечити достатній рівень безпеки передачі даних при дотриманні потрібної якості зв'язку.

В основу корисної моделі, що пропонується, поставлена задача створення програмно-апаратного комплексу захищеної системи голосового конференц-зв'язку в IP-мережах, який дозволить організовувати багатоабонентський захищений зв'язок в IP-мережах. Цей комплекс реалізується на основі персональних комп'ютерів, флеш-накопичувачів для зберігання ключової інформації, спеціалізованого програмного забезпечення, яке дозволяє підключення абонентських терміналів до сервера, провідної чи безпроводної IP-мережі. Такий комплекс дозволить створювати та проводити захищені конференції як в локальних, так і в глобальних IP-мережах.

Основною задачею комплексу є ідентифікація та автентифікація абонентів, розподіл ключової інформації від сервера до абонентів, створення багатоабонентських захищених аудіоконференцій.

Відома система для управління конференціями дозволяє приймати участь одному або декільком учасникам у одній або декількох конференціях [1].

Також відомий спосіб управління сеансами захищеного відеоконференцзв'язку в мережах шифрованого зв'язку, який дозволяє підвищити захищеність системи захищеного відеоконференцзв'язку за допомогою розподіленого контролю доступу, використовуючи механізми управління сеансами на основі аналізу потоків даних, що передаються IP-мережею [2].

Найбільш близьким до запропонованої моделі по технічній сутті і задачі є технологія організації аудіоконференцій [3]. В способі наведено етапи забезпечення організації аудіоконференцій. Основним етапом є мікшування і вирівнювання рівня звуку на виході. Забезпечується виведення на локальний аудіоінтерфейс, телефонну мережу загального користування (PSTN), бездротовий інтерфейс навушників або гарнітур.

Але наведені способи не дозволяють організувати захищену голосову конференцію в глобальних або локальних відкритих комп'ютерних IP-мережах. Тому використання зазначеного способу все одно потребує великих організаційних затрат. Необхідність шифрування для організації захищених конференцій наведена в [2]. Використання IP-мережі, у запропонованій корисній моделі, дозволяє уникнути великих часових, організаційних та матеріальних затрат на підготовку та проведення аудіоконференцій.

Програмно-апаратний комплекс захищеної системи голосового конференц-зв'язку на основі IP-мережі базується на використанні персональних комп'ютерів як пристроїв для створення захищених пакетів голосових даних та забезпечення їх передачі провідною або безпроводною IP-мережею.

Програмно-апаратний комплекс захищеної системи голосового конференц-зв'язку забезпечує виконання таких функцій:

- ідентифікацію абонентів;
- автентифікацію абонентів;
- управління ключами;
- створення та управління конференціями;
- відображення учасників конференції.

Для ілюстрації запропонованої моделі приведена блок-схема програмно-апаратного комплексу захищеної системи голосового конференц-зв'язку в IP-мережах. Комплекс складається з робочих місць абонентів (елементи  $N_1 \dots N_k$ ), які об'єднуються в мережу за допомогою дротового (елементи  $N_1 \dots N_m$ ) або бездротового (елементи  $N_{m+1} \dots N_k$ ) підключення. Робоче місце абонента включає в себе термінал - персональний комп'ютер або мобільний пристрій, який підтримує IP-мережу. На терміналі встановлено спеціальне клієнтське програмне забезпечення, яке дає змогу під'єднатися до сервера та прийняти участь в захищеній

аудіоконференції. В склад комплексу також входить сервер (елемент S),  $W_1$  - дротовий маршрутизатор,  $W_2$  - бездротовий маршрутизатор.

Комплекс працює наступним чином: після включення терміналу абонент проходить процес ідентифікації та автентифікації. Після цього абонент отримує доступ до дозволених конференцій або, якщо має право, створює власну конференцію. Після успішної автентифікації між абонентом та сервером встановлюються сеансові ключі, які використовуються для шифрування.

Відмінною ознакою програмно-апаратного комплексу захищеної системи голосового конференц-зв'язку, що заявляється, є те, що як мережа передачі даних може використовуватися як дротова, так і бездротова глобальна або локальна IP-мережа, при передачі голосових даних використовується алгоритм шифрування ГОСТ 28147-89, голосові потоки обробляються, мікшуються, шифруються за допомогою встановлених ключів на сервері. Це дає можливість забезпечити конфіденційність зв'язку, використовуючи відкриті глобальні IP-мережі.

Список використаної літератури

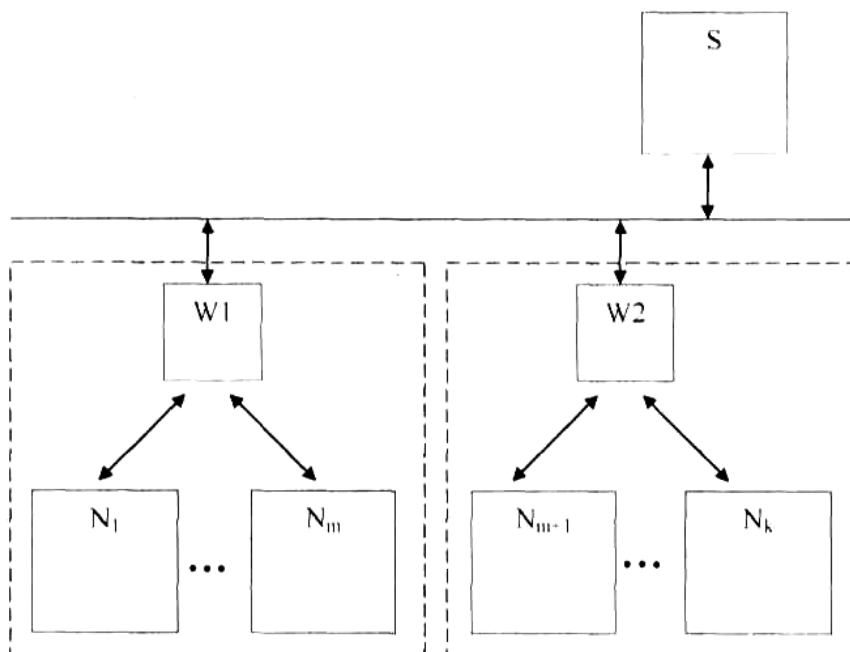
1. Патент RU 2293368 C2, Способ (варианты) для управления конференциями и блок управления для многоточечной мультимедийной/речевой системы / Потехин С, Кнац Э., Эльбац М.; заявители и патентообладатели: Потехин С., Кнац О., Эльбац М. - 2003134945/09; заявл. 09.05.2002; опубл. 10.02.2007, бюл. № 4.

2. Патент RU 2460235 C2, Средство управления сеансами защищенной видеоконференцсвязи в сети шифрованной связи / Архангельский В.Г., Зегжда Д.П., Зегжда П.Д., Котылевский А.С., Лукомский Н.А.; заявители и патентообладатели: Архангельский В.Г., Зегжда Д.П., Зегжда П.Д., Котылевский А.С., Лукомский В.А. 2008145007/07; заявл. 10.11.2008; опубл. 27.08.2012, бюл. № 24.

3. Патент US 7899445 B2 США, Mobile conferencing and audio sharing technology / Guccione D.; заявители и патентообладатели: Guccione D. - 12/785,267; заявл. 21.05.2010; опубл. 09.09.2010, бюл. №11.

#### ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Програмно-апаратний комплекс захищеної системи голосового конференц-зв'язку в IP-мережах, що містить дротовий ( $W_1$ ) та бездротовий ( $W_2$ ) маршрутизатори, які в свою чергу з'єднані з робочими місцями абонентів ( $N_1...N_m$ ) при дротовому підключенні та ( $N_{m+1}...N_k$ ) при бездротовому підключенні, який **відрізняється** тим, що додатково містить сервер (S), який з'єднаний з дротовим ( $W_1$ ) та бездротовим ( $W_2$ ) маршрутизаторами.



---

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