УДК 004.7; 004.942

Є.В. Риндич, аспірант

Інститут проблем математичних машин та систем, м. Київ, Україна

АРХІТЕКТУРА КОРПОРАТИВНОЇ КОНФЕРЕНЦ-СИСТЕМИ НА ОСНОВІ IP-ПРОТОКОЛУ

Досліджено існуючі конференц-системи. Визначено загальні риси корпоративних конференц-систем та їх функціональність. Запропонована загальна архітектура та схема взаємодії її складових, метоид, що дозволяють використовувати IP-мережі загального користування для передачі комерційної або приватної інформації.

Вступ

Сучасні тенденції розвитку корпоративних інформаційних систем характеризується переходом до інтегрованої передачі даних і мовлення. Це забезпечується за допомогою конференц-систем, які дозволяють в режимі реального часу обмінюватися інформацією, проводити голосування, відео або голосові переговори в режимі, коли співрозмовники можуть говорити й слухати одночасно, а кількість абонентів більше або дорівнює трьом. Для більшості конференц-систем характерно вільне розповсюдження інформації, коли вона є відкритою [1].

Особливо це стосується веб-конференцій, які будуються на основі IP-протоколу. Саме ці інформаційні системи дозволяють в процесі свого функціонування проводити онлайн-презентації, спільно працювати з документами і додатками, синхронно переглядати сайти, відео файли і зображення в режимі, коли учасники територіально віддалені та знаходяться на своєму робочому місці за комп'ютером.

Як правило, веб-конференції для передачі даних використовують глобальну IP-мережу – Інтернет [2]. Однак, в таких системах не виконуються умови конфіденційності режиму спілкування та передачі даних, які характерні для корпоративних систем. Тому актуальною є задача по розробці конференц-системи, орієнтованої на корпоративне використання.

Метою статті є визначення принципів побудови сучасних корпоративних конференц-систем, які відображаються у відповідній архітектурі даної системи.

Корпоративні конференц-системи та їх визначення

Корпоративні конференц-системи (ККС) відносяться до класу корпоративних інформаційних систем (КІС), основними властивостями яких є:

1. Попередження несанкціонованого доступу.
2. Наявність засобів супроводження та адаптації.
3. Авторизація інформації.
4. Реєстрація операцій з інформацією.
5. Консолідація інформації на рівні підприємств, філіалів, дочірніх компаній.

Існуючі конфренц-системи, як правило, не задовольняють цим вимогам в повній мірі.

Так, конфернц-система Bosch DCN NG, хоча і є найбільш розповсюдженою, не може бути віднесена до класу ККС. Дана система призначена, перш за все, для створення локального конференц-залу та забезпечує:

1. автоматичне управління ходом конференції у обраному режимі роботи;
2. можливість відключати активні мікрофони;
3. реєстрація учасників за допомогою карток ідентифікації;
4. голосування;

5. синхронний переклад доповідача;
6. автоматичне наведення відеокамер на доповідача.

Напрямком розвитку даної системи є автоматизація проведення локальної конференції, а саме включення до цієї системи функцій управління побутовими пристроями та освітленням[3]. Використання цієї системи в якості розподіленої або територіально рознесеної системи неможливе. До того ж, вона використовує аналогові канали передачі даних.

Інша конференц-система – Brahler Digimix – використовує цифрову кабельну та безпровідну технологію передачі даних, а для проведення голосування додатково використовується інша система – Brahler Digivote III. Голосування проводиться з спеціальних пультів, які з'єднуються з сервером за допомогою безпровідних каналів зв'язку. Об'єднання системи Brahler Digimix та Brahler Digivote III дозволяє створити ККС. Проте, виробник не пропонує жодних варіантів створення розподіленої ККС, в якій буде циркулювати комерційна інформація. Дана система розгортується в межах одного підприємства [4].

Конференц-система DNCA (Data Naught Conference Appliance) підтримує створення відкритих голосових конференцій в мережі Інтернет.

Загальна порівняльна характеристика розглянутих вище конференц-систем наведена в таблиці 1.

Таблиця 1

Назва системи	режим багатопоточної конференції	режим «один до одного»	модерація та адміністрування	використання глобальних мереж	Ідентифікація	автентифікація	передача даних	голосування	архівація	управління користувачами
Bosch DCN NG	+	-	+	-	+	-	-	+	+	+
Digimix Brahler	+	-	+	-	+	-	+	+	+	+
DNCA	+	+	+	+	+	-	-	-	+	+

Слід зазначити, що, незважаючи на деякі відмінності, їм притаманні такі загальні риси: модульність, наявність центрального елементу, ідентифікація користувачів під час проведення голосування.

Принципи побудови ККС

Виходячи з властивостей ККС, можна виділити такі принципи їх побудови:

1. функціональна повнота;
2. розподіленість;
3. робота в режимі реального часу;
4. конфіденційність.

Розглянемо ці принципи більш детально.

Функціональна повнота відносно ККС повинна відображати реалізацію властивостей, пов'язаних з виконанням специфічних функцій. Ці функції обумовленні основною метою створення цього класу систем – оперативним обміном мультимедіа інформацією та прийняттям рішення в режимі реального часу. З огляду на це, обов'язковими для таких систем виділяють наступні специфічні функції:

1. створення конференцій;
2. прослуховування конференцій;
3. розмова в режимі конференції;
4. модерація конференцій;
5. розмова в режимі «один до одного»;
6. передача та обробка даних;
7. передача повідомлень;
8. управління користувачами системи;
9. архівація та запис даних, які створюються та розповсюджуються в ККС;
10. контроль працездатності;
11. обробка інформації та її відображення;
12. голосування;
13. адміністрування;
14. забезпечення конфіденційності.

Принцип розподіленості обумовлений специфікою використання ККС, які найчастіше застосовуються в банківській сфері, телемедицині, для організації нарад та семінарів. В жодній з цих сфер діяльності неможливо створити ККС без підключення віддалених користувачів, причому з найменшими витратами та за короткий час. Цього можна досягти лише використовуючи розподілені комп'ютерні системи та мережі, що функціонують на основі IP-протоколу, в тому числі глобальну IP-мережу – Інтернет.

Виходячи з третього принципу, при розробці ККС необхідно забезпечити її роботу в реальному масштабі часу. Для цього слід визначити типові ролі користувачів та режими їх функціонування. ККС повинна підтримувати участь в конференції або голосуванні таких ролей користувачів: адміністратора, модератора, учасника конференції, секретаря, перекладача. Режими функціонування ККС включають:

1. підготовку конференції або голосування;
2. початкову реєстрацію учасників;
3. оперативну реєстрацію учасників;
4. проведення конференції (обговорення);
5. голосування;
6. оформлення підсумків;
7. збереження інформації.

До режиму підготовки входить формування початкового пакету документів, які необхідні для проведення конференції або голосування, та їх розповсюдження учасникам. Підготовку проводить секретар, а розповсюджує адміністратор чи модератор.

Режим початкової реєстрації учасників включає реєстрацію користувачів та слухачів в системі за допомогою ідентифікатора. При роботі з віддаленими користувачами необхідно проводити автентифікацію користувачів.

Під час сеансу зв'язку можливе підключення користувачів, що активує режим оперативної реєстрації учасника. При цьому вносяться зміни до реєстру учасників конференції або голосування.

Під час проведення конференції, або окремо, може бути ініційовано голосування. Управління конференцією або голосуванням проводиться модератором. Якщо режим голосування запущено без конференції, то всі учасники повинні пройти процес ідентифікації та автентифікації відповідно статусу голосування. При голосуванні використовуються декілька режимів за доступністю інформації про волевиявлення:

- поіменне голосування;
- тайна голосування;
- відкрите голосування.

За кількістю варіантів голосування буває одноваріантним та багатоваріантним. В свою чергу, багатоваріантне голосування може бути альтернативним, коли учасник голосує лише за одну відповідь, або рейтингове, коли кожній відповіді виставляється певна оцінка. Загальна таблиця сценаріїв голосувань наведена в таблиці 2.

Таблиця 2

Варіанти голосування

	Поіменне	Відкрите	Таємне
Кількісне	+	+	+
Альтернативне	x	X	+
Рейтингове	x	X	+

Після проведення голосування обов'язково виконується режим оформлення підсумків. Цей режим також виконується після завершення конференції, але може мати спрощену форму, оскільки рішення, прийняті в процесі спілкування, не завжди можливо та потрібно оформляти у формальному вигляді.

Режим збереження інформації виконується при закінченні будь-якого сеансу зв'язку та зберігає протокол проведення конференцій або голосування в базу даних. В режимах спілкування можливе виконання синхронного перекладу в реальному часі. При цьому потік голосових даних від співрозмовника направляється до перекладача, а переведений потік на іншій мові передається іншому співрозмовнику. В разі використання режиму конференції потік перенаправляється декільком користувачам.

Конфіденційність в ККС передбачає використання спеціальних засобів автентифікації, ідентифікації та обмеження доступу до інформації.

Для початкової автентифікації користувачів в конференц-системах може бути запропонований метод автентифікації на основі конфіденційних даних, які знаходяться в таблиці з ключами [5]. В цьому випадку автентифікація користувача проходить за допомогою симетричного алгоритму криптографічного перетворення та полягає в наступному:

1. користувач відправляє повідомлення з номером рядка в таблиці ключів та зашифрованими налаштуваннями сеансу зв'язку;
2. сервер, використовуючи ключ із вказаного рядка, проводить зворотні криптографічні перетворення. Якщо в разі зворотних перетворень правильно розпізнано формат налаштувань, то сервер відправляє клієнту підтвердження у вигляді повідомлення. Повідомлення складається з нового номера в таблиці ключів та зашифрованих налаштувань сеансу зв'язку за допомогою ключа з цього рядка;
3. якщо клієнт отримане від сервера повідомлення після зворотних криптографічних перетворень розпізнає, то він починає сеанс передачі голосових даних, зашифрованих за допомогою цього ключа.

Порівняно з протоколами IP-телефонії запропонований метод автентифікації використовує в 2,25 рази менше мережевих пакетів. Ключі не передаються мережею, а розповсюджуються за допомогою захищених каналів зв'язку, наприклад, спеціальними кур'єрськими службами.

Під час проведення сеансу зв'язку для повторної автентифікації необхідно використовувати додаткові заходи автентифікації. Для систем відео або голосового конференц-зв'язку найбільш прийнятними є засоби біометричної автентифікації. До переваг таких засобів належить відсутність відволікання учасника на автентифікацію, причому автентифікація за голосом або відео зображенням може відбуватися паралельно сеансу зв'язку, не порушуючи процес конференції. При необхідності процес біометричної автентифікації проводиться декілька разів для досягнення необхідної точності, оскільки

контрольний та еталонний шаблон повністю ніколи не збігаються. Для забезпечення конфіденційності мультимедіа даних, які циркулюють в конференц-системі, слід використовувати багатофакторну автентифікацію [6]. Таким чином, при цьому використовується двофакторна автентифікація користувача, яка є необхідною для підтримання належного рівня інформаційної безпеки в системах IP-телефонії. Автентифікація користувача під час сеансу зв'язку не є обов'язковою, оскільки таблиці ключів є секретними, а обмеження доступу до терміналу під час сеансу зв'язку може бути створено за рахунок виконання правил безпеки використання терміналів на робочих місцях.

Для ідентифікації слід використовувати двофакторну ідентифікацію – за фізичним секретом та біометричними властивостями учасника, наприклад, відбитку пальця. Ідентифікація пристрою проходить за схемою «списків довіри». Даний підхід використовується в брандмауерах. Існує три види списків: «білі» – списки з адресами, яким система довіряє; «сірі» – списки, в які вносяться адреси пристроїв, з яких вперше було встановлення з'єднання та які находяться в зоні «часткової довіри», та «чорні» – списки, в яких зберігаються адреси комп'ютерів, з яких було проведено атаки на систему конференц-зв'язку.

Конфіденційність підтримується за рахунок симетричних криптографічних перетворень. На відміну від стандартної схеми симетричної криптосистеми в методі запропоновано використовувати криптографічні перетворення зі своїм ключем для кожної сторони. Схема процесів криптографічного перетворення наведена на рис.1, де *Ксм[i][1]* – ключ сервера з *i*-того рядка; *Ксм[i][2]* – ключ клієнта з *i*-того рядка.

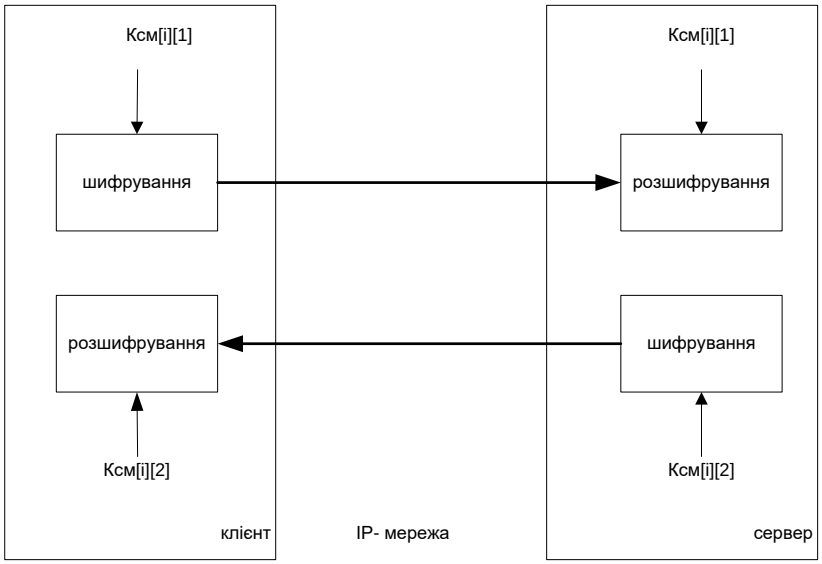

Рис.1. Схема процесів перетворення інформації під час передачі

Шифрування та розшифрування проходить за одним алгоритмом, але з різними ключами. Слід зазначити, що ключі *Ксм[i][1]* та *Ксм[i][2]* для різних клієнтів відрізняються, оскільки вони знаходяться в різних таблицях.

Ця схема використовується і для передачі результатів голосування. При проведенні таємного голосування після проведення зворотних криптографічних перетворень результати голосування накопичуються в буфері, а інформація, отримана при автентифікації, ігнорується та не зберігається. Буфер виконує роль урни з анонімними бюлетенями.

Узагальнена архітектура ККС

Виходячи з принципів побудови ККС, можуть бути визначені необхідні складові елементи системи, які визначають її архітектуру (рис.2):

1. АРМ користувача.
2. АРМ адміністратора.
3. АРМ модератора.
4. АРМ секретаріату.
5. АРМ перекладача.
6. Сервер ККС.

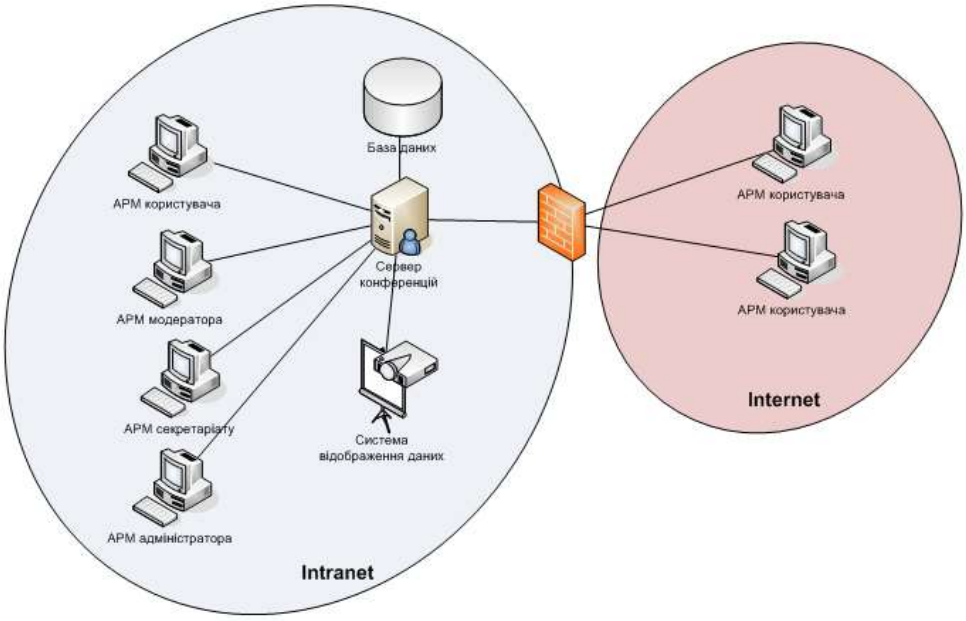

Рис.2. Компоненти ККС

На рис.3 наведено архітектуру АРМ користувача та сервера ККС. Архітектура АРМ адміністратора та модератора відрізняються від АРМ користувача можливостями модулів голосування, відображення результатів. Архітектура АРМ секретаріату та АРМ адміністратора наведена на рис.4.

Для підтримання конфіденційності даних необхідно використовувати криптографічні перетворення, попередньо розповсюдивши ключі [5]. Використання додаткових процесів перетворення інформації обумовлено використанням публічних IP-мереж, в яких шлях проходження конфіденційної інформації не відомий. Зловмисник може провести конфігурацію мережі з метою проходження всього трафіку через модифікований вузол та отримати конфіденційну інформацію [7].

Дослідження архітектури корпоративних конференц-систем

Використання в системі додаткових процесів обробки мультимедіа інформації впливає на часову затримку між відправленням та отриманням голосових даних. Для систем IP-телефонії відомим апаратом QoS(Quality of Service) визначена максимальна часова затримка в 300 мсек між відправленням та отриманням абонентом голосових даних. Для того, щоб визначити вплив додаткових процесів обробки інформації на якість зв'язку, запропонована імітаційна модель корпоративної конференц-системи на базі протоколу IP. Вона дає можливість спростити процес побудови систем цього класу. Модель побудована на базі розширених мереж Петрі [8].

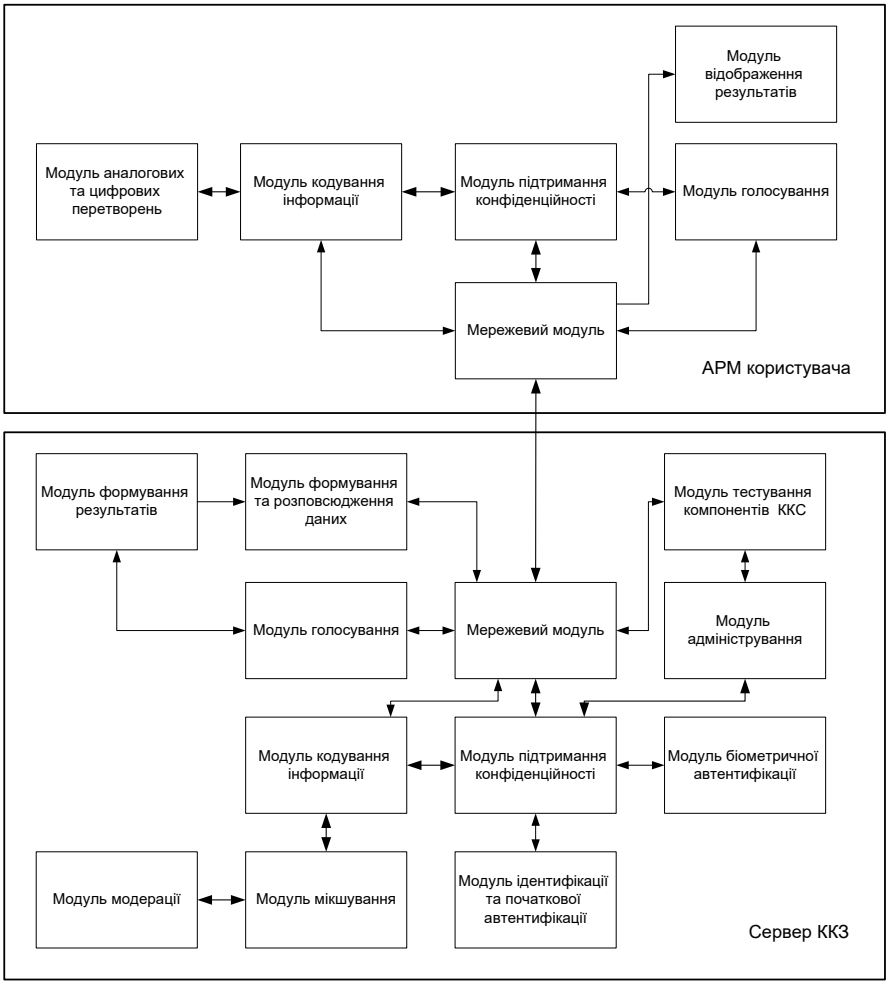

Рис.3. Архітектура сервера та користувача ККС

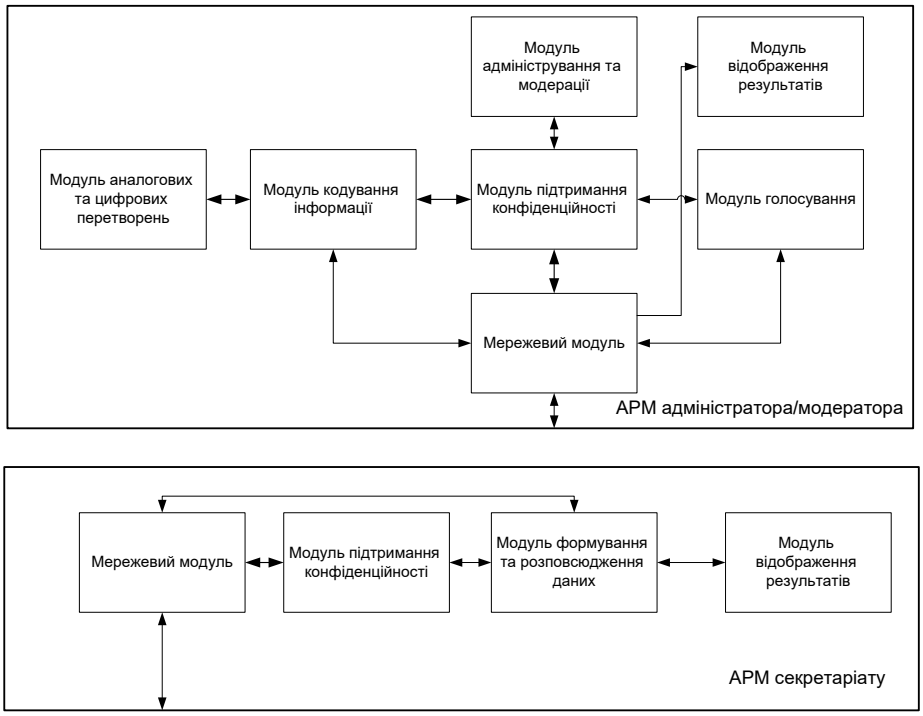

Рис.4. Архітектура АРМ секретаріату та АРМ адміністратора/модератора ККС

З використанням запропонованих моделей проведено дослідження та визначено середній час затримки в залежності від кількості підключених абонентів в ККС при передачі голосових повідомлень у відкритому (рис.5) та закритому (рис.6) режимах конференц-зв'язку.

Принципи побудови корпоративних конференц-систем були використані при модернізації відкритої конференц-системи DNCA. Отримані за допомогою моделювання результати порівняно з даними, які були отримані експериментально з використанням спеціального програмного забезпечення генерації дзвінків SIPRobots. Особливістю існуючої системи DNCA є те, що у відкритому режимі вона заздалегідь запрограмована на недосяжність максимальної кількості користувачів, тобто, для гарантування якості в системі встановлено максимум одночасних підключень. Тому на рис.5, графік 2, можливо було отримати значення затримки лише для 10000 користувачів. Аналогічно для закритого режиму роботи (рис.6) було встановлено обмеження в 200 користувачів.

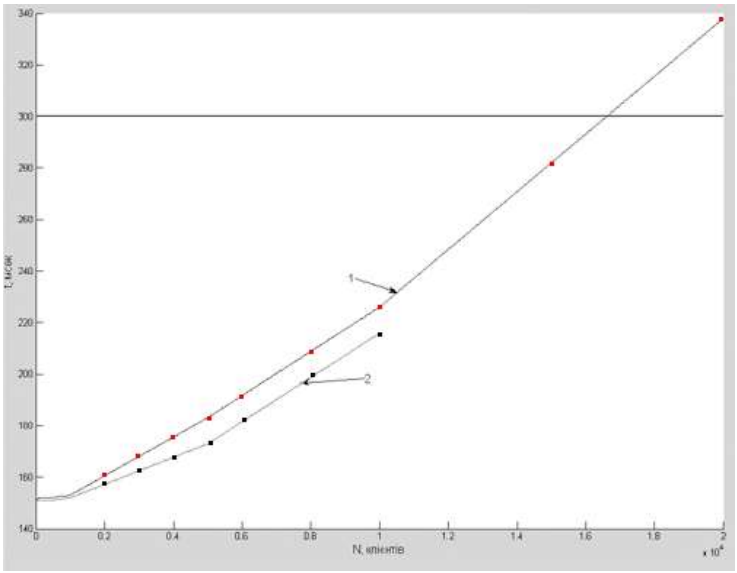

Рис.5. Графік залежності часової затримки від кількості клієнтів для публічного режиму роботи: 1 – дані імітаційного моделювання, 2 – експериментальні дані

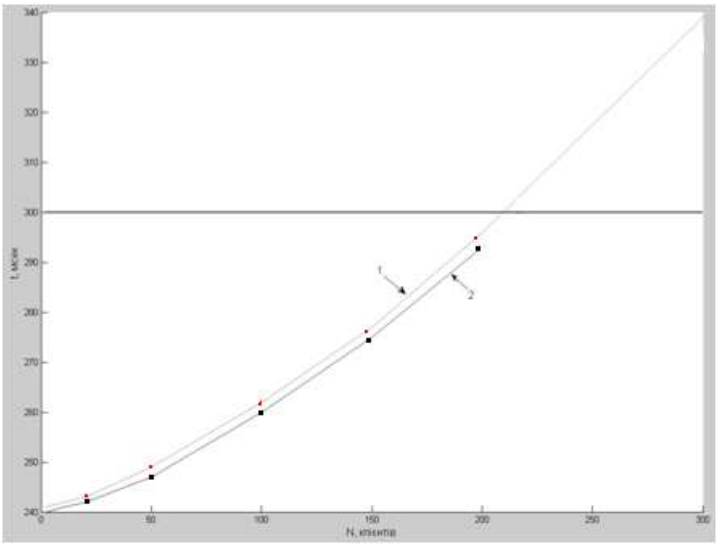

Рис.6. Графік залежності часової затримки від кількості клієнтів для конфіденційного режиму роботи: 1 – дані імітаційного моделювання, 2 – експериментальні дані

Висновки

В роботі проведено аналіз існуючих конференц-систем, який показав необхідність розширення функціональності та розроблення узагальненої архітектури ККС. Виділені основні компоненти системи та наведена архітектура компонентів. Для підтримання конфіденційності комерційної інформації запропоновано метод, в якому використовується, на відміну від існуючих систем, не тільки ідентифікація, а й багатофакторна автентифікація. Використання біометричної автентифікації під час сеансу зв'язку дозволяє не відволікати користувача від участі в конференції та, в той самий час, підтвердити його особу. Також для підтримання конфіденційності необхідним є використання криптографічних перетворень під час передачі даних. Порівняно з існуючими підходами автентифікації та встановлення зв'язку, які використовують для створення конференц-зв'язку в IP-мережах, запропонований метод використовує менше інформаційних повідомлень. Дослідження імітаційної моделі системи захищеного голосового конференц-зв'язку на базі протоколу IP дозволило дослідити ефективність запропонованого методу у критичних режимах роботи ККС, визначити максимально допустиме число користувачів без втрати якості.

Список літературних джерел

1. Конференц-система – Википедия. [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Конференц-система/

2. А.Зарубин, Е.Коптилина Системы конференц-связи для совместной работы // Connect! Мир связи, – 2008. – №11. – С. 25-27.

3. Bosch DCN NG - Оборудование для аудиоконференций. [Електронний ресурс]. – Режим доступу: www.confsystems.ru/aconf/catalog/1161765982

4. Digimic-Concept [Електронний ресурс]. – Режим доступу: http://www.braehler.su/en/konferenztechnik/digimic/index5a0a.html

5. Казимир В.В., Риндич Є.В., Кенийз Я.Я. Модуль комутації крипто-ключів для захищеної системи IP-телефонії // Науковий журнал «Вісник Національного авіаційного університету». – 2010. – №1. С.153-159.

6. Сіра Г.А., Риндич Є.В., Казимир В.В. Технології автентификації в web-системах та ір-телефонії // Науковий журнал «Вісник Хмельницького національного університету». – 2009. – №3. С. 147-154.

7. Риндич Є.В. IP-телефонія та найпоширеніші небезпеки в ній // Збірник наукових праць п'ятої міжвузівської науково-практичної конференції «Комплексна економічна безпека підприємництва: сучасні тенденції формування та перспективи розвитку, економіко-правові аспекти». – Чернігів. –2008. –С. 130-133.

8. Риндич Є.В., Казимир В.В. Імітаційна модель системи захищеного конференц-зв'язку на базі протоколу IP // Науковий журнал «Вісник Чернігівського державного технологічного університету» серія «Технічні науки». – 2010. – №42. С. 182-191