УДК 004.7;004.942

Є.В. Риндич, канд. техн. наук
Чернігівський державний технологічний університет, м. Чернігів, Україна

АРХІТЕКТУРА ЗАХИЩЕНОЇ СИСТЕМИ ГОЛОСОВОГО КОНФЕРЕНЦ-ЗВ'ЯЗКУ В IP-МЕРЕЖАХ

Е.В. Рындич, канд. техн. наук
Черниговский государственній технологический університет, г. Чернигов, Украина

АРХИТЕКТУРА ЗАЩИЩЕННОЙ СИСТЕМЫ ГОЛОСОВОЙ КОНФЕРЕНЦ-СВЯЗИ В IP-СЕТЯХ

Y.V. Ryndych, Candidate of Technical Sciences
Chernihiv State Technological University, Chernihiv, Ukraine

ARCHITECTURE OF SECURED VOICE CONFERENCE SYSTEMS IN IP-NETWORKS

Досліджено існуючі системи конференц-зв'язку. Визначено загальні риси захищених конференц-систем та їх функціональність. Запропоновано загальну архітектуру захищеної системи голосового конференц-зв'язку в IP-мережах. Визначено певні особливості побудови систем голосового конференц-зв'язку, пов'язані з обробленням інформації на стороні сервера.

***Ключові слова**: клієнт-серверна архітектура, інформаційна система, конференц-зв'язок, конфіденційність, мікшування голосових даних.*

Исследовано существующие системы конференц-связи. Определено общие черты защищенных конференц-систем и их функциональность. Предложена общая архитектура защищенной системы конференц-связи в IP-сетях. Определены некоторые особенности построения систем голосовой конференц-связи, связанные с обработкой информации на стороне сервера.

***Ключевые слова**: клиент-серверная архитектура, информационная система, конференц-связь, конфиденциальность, микширование голосовых данных.*

Studied existing conference. Defined similarities and functionality of protected conference systems. The general architecture of a secure conferencing systems in IP-networks proposed. Identified several design features of voice conferencing related to information processing on the server side.

***Key words**: client-server architecture, informative system, conferencing, confidentiality, mixing voice.*

Постановка проблеми. Сучасний етап розвитку конференц-систем та їх висока гетерогенність вимагають від мережевого обладнання чіткої взаємодії та 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 розроблення захищених корпоративних конференц-систем на базі протоколу IP, які дозволяють створювати голосові конференції з дотриманням вимог конфіденційності інформації, що передається.

Проте питання побудови захищених систем голосового конференц-зв'язку в IP-мережах, розрахованих на значну кількість учасників переговорів, та підтримки всіх притаманних їм властивостей освітлені недостатньо і потребують подальшого дослідження. Під час передачі стиснених мовних сигналів IP-мережами повною мірою не відпрацьовуються ефективні механізми забезпечення обмеженого доступу. Досі не визначені загальні принципи архітектурної побудови та підходи до моделювання корпоративних конференц-систем на базі протоколу IP, які б дозволяли створювати нові системи й аналізувати використання в існуючих системах додаткових елементів забезпечення конфіденційності комерційної інформації, що циркулює в системі.

Таким чином, актуальною є науково-прикладна задача розроблення архітектури систем голосового конференц-зв'язку в IP-мережах.

Аналіз останніх досліджень і публікацій. Сучасні тенденції розвитку інформаційних систем характеризується переходом до інтегрованої передачі даних і мовлення. Це забезпечується за допомогою систем конференц-зв'язку, які дозволяють у 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 у процесі свого функціонування проводити онлайн-презентації, спільно працювати з документами і додатками, синхронно переглядати сайти, відеофайли 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 у таких системах не виконуються умови конфіденційності режиму спілкування та передачі даних, які характерні для корпоративних систем. Тому актуальною є задача щодо розроблення конференц-системи, орієнтованої на корпоративне використання.

Конференц-системи 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 конференц-системи, як правило, не задовольняють ці вимоги повною мірою.

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

1. Автоматичне керування ходом конференції в обраному режимі роботи.
2. Можливість вимикати активні мікрофони.
3. Реєстрація учасників за допомогою карток ідентифікації.
4. Голосування.
5. Синхронний переклад виступаючого.
6. Автоматичне наведення відеокамер на того, хто виступає.

Напрямком розвитку цієї системи є автоматизація проведення локальної конференції, а саме включення до цієї системи функцій керування побутовими пристроями та освітленням [3]. Використання цієї системи як розподіленої або територіально рознесеної системи не можливе. 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 зі 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. Однак виробник не пропонує жодних варіантів створення розподіленої ККС, в якій буде циркулювати комерційна інформація. Така система розгортається в межах одного підприємства [4].

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

Загальна порівняльна характеристика розглянутих вище конференц-систем наведена в табл.

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

Мета статті. Провести аналіз та виділити особливості побудови захищеної системи голосового конференц-зв'язку в IP-мережах. Запропонувати узагальнену архітектуру цього класу систем з урахуванням їх особливостей.

Таблиця

Загальна порівняльна характеристика конференц-систем

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	+	+	+	+	+	-	-	-	+	+

Основна частина. Для створення конференц-зв'язку на основі протоколу IP можна використовувати «клієнт-серверну» архітектуру або архітектуру «кожний з кожним» [5-8]. При цьому найбільш важливими є необхідність проведення мікшування голосових потоків, отриманих від декількох клієнтів, та отримання інформації про кількість інформаційних потоків, які створюються між клієнтами й передаються мережею. Залежність кількості інформаційних потоків для архітектури «клієнт–сервер» виражена формулою (1), а залежність для архітектури «кожний з кожним» – формулою (2), де n – це кількість абонентів у конференції.

$$k = 2 * n, \tag{1}$$

$$k = 2 * n * (n - 1). \tag{2}$$

Існуючі протоколи конференц-зв'язку, хоча і підтримують створення конференцій, але розраховані на передачу голосових або відеоданих між двома абонентами. Прикладом такого протоколу є протокол SIP. Саме тому доцільно використовувати архітектуру «клієнт-сервер» (рис. 1).

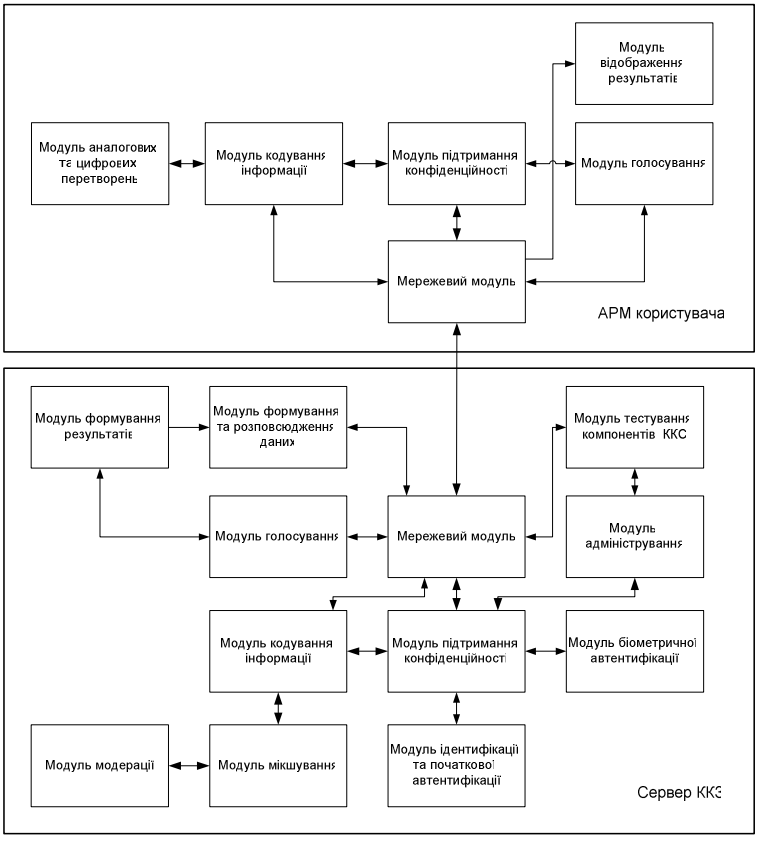

Рис. 1. Архітектура сервера та клієнта захищеної системи голосовогои конференц-зв'язку

Під час реалізації модуля мікшування були виявлені такі особливості: програмне збільшення гучності на стороні клієнта, вплив зовнішніх завад, реалізація зведення декількох голосових потоків.

Зведення виконується на стороні сервера за допомогою мікшера. Його структура зображена на рис. 2.

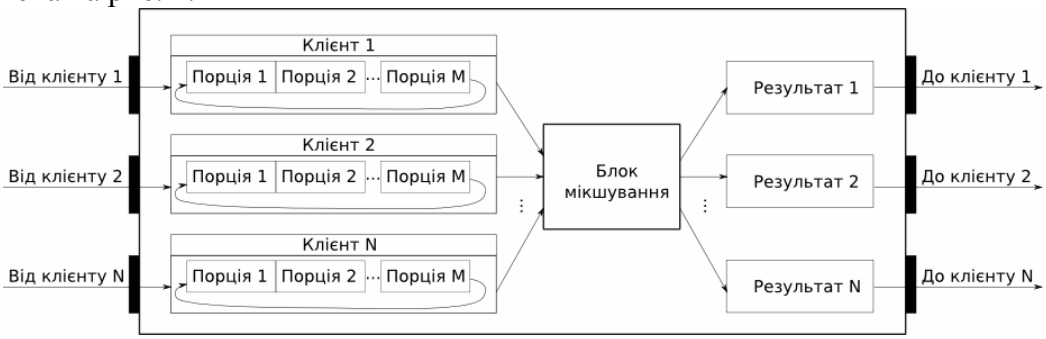

Рис. 2. Структурна схема мікшера

Для кожного клієнта мікшер містить індивідуальний кільцевий буфер, до якого надходять дані з попереднього елемента. Розмір кожного буфера фіксований і має однакове значення для всіх клієнтів. Під час записування даних у буфер, дані, що знаходяться в кінці буфера, перезаписуються. Оскільки використовується кільцевий буфер, то здається, що дані безрезультатно втрачаються, але це не відповідає дійсності. Цьому є логічне пояснення, а саме: оскільки система працює в режимі реального часу, то актуальні дані, тобто ті, що надійшли найпізніше, мають найвищий пріоритет. Через це система має право на перезапис даних, які втратили свою актуальність.

Під час зведення з кожного буфера виймається одна порція даних. Якщо буфер порожній, то вважається, що була отримана порція з порожніми даними.

Власне зведення відбувається у блоці мікшування.

Зведення відбувається через рівні проміжки часу. Для усунення ефекту акустичного еха початкові дані, отримані з кільцевого буфера, не беруть участі у зведенні, результат якого буде відправлено до цього ж самого клієнта. Структурна схема зведення партії порцій даних представлена нижче на рис. 3.

Рис. 3. Структурна схема алгоритму мікшування для одного клієнта

Рисунок 3 відображає тільки частину алгоритму, а саме для клієнта 1. Для усіх інших клієнтів схема така сама і має тільки одне вищеназване зауваження: у формуванні результату зведення для клієнта дані від самого клієнта не враховуються.

Як власне алгоритм була використана адаптована версія [9] алгоритму Віктора Тота, який він описує у своїй статті [10]. Використаний алгоритм дозволяє уникнути виникнення дисторшну – звукового ефекту, що виникає при жорсткому обмеженні амплітуд. Така ситуація виникає під час зведення звукових рівнів, коли як алгоритм зведення використовується арифметична операція додавання, а отримуваний результат має більше значення, ніж максимально можливе (рис. 4). При цьому результату надається це саме найбільш можливе значення (рис. 5).

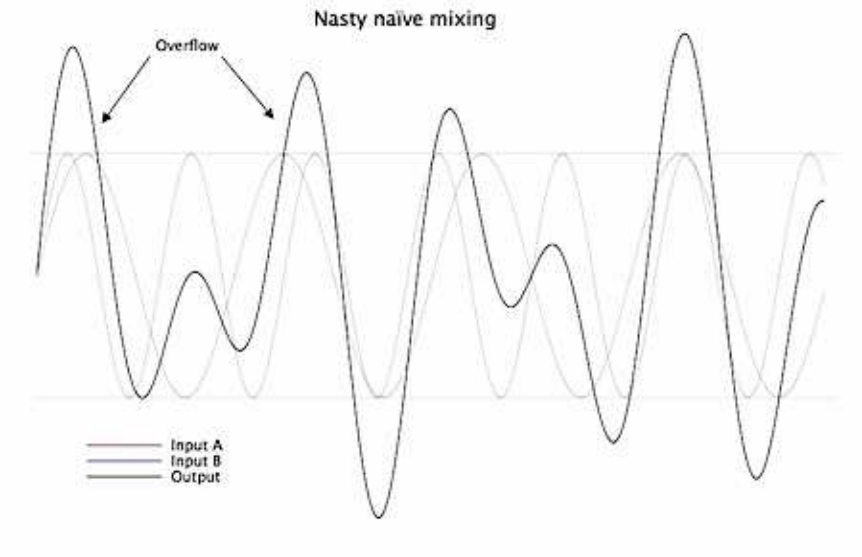

Рис. 4. Ілюстрація переповнення (overflow) результату зведення

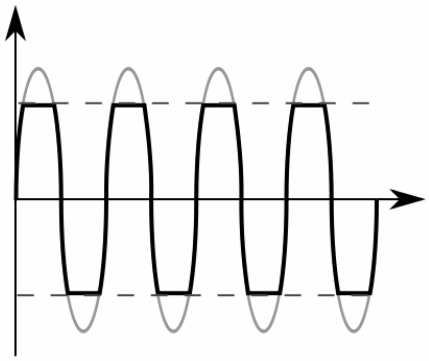

Рис. 5. Звуковий ефект "дисторшн", а саме його частковий випадок – "кліппінг"

Для усунення дисторшн ефекту замість звичайного арифметичного додавання використовується параметризоване арифметичне додавання.

Висновки. У роботі проведено аналіз існуючих конференц-систем, який показав необхідність розширення функціональності та розроблення узагальненої архітектури ККС. Виділені основні компоненти системи та наведена архітектура компонентів.

Як видно з опису мікшера, вузьким місцем усієї системи є алгоритм підготовки даних для зведення. Проблема полягає в тому, що мікшер виконує зведення через рівні проміжки часу. При цьому дані, які повинні брати участь у процесі зведення, можуть потрапляти через мережу на сервер у довільні моменти часу. Складність усієї задачі полягає в необхідності гарантування потрапляння порцій даних, які виникли в один момент часу, до мікшера з мінімальною різницею у часі, для того, щоб вони мали змогу взяти участь в одному і тому ж циклі зведення. Вирішення цієї складної проблеми надасть поштовх для значного прискорення розвитку всієї системи.

Список використаних джерел

1. *Конференц-система* [Электронный ресурс]. – Режим доступа : http://ru.wikipedia.org/wiki/.

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

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

4. *Digimic-Concept* [Electronic resource]. – Access mode : http://www.braehler.su/en/konferenztechnik/digimic/index5a0a.html.

5. *Хелд Г.* Сокращение задержки голоса по IP [Электронный ресурс] / Г. Хелд // LAN. – 2000. – № 7. – Режим доступа : http://www.osp.ru.

6. *Измерение* джиттера в цифровых системах [Электронный ресурс]. – Режим доступа : http://citforum.ru/nets/hard/jitter/.

7. *Данн Дж.* Джиттер. Теория. Ч. 3 [Электронный ресурс] / Дж. Данн. – Режим доступа : http://www.ixbt.com/proaudio/jitter-theory-part3.shtml.

8. *Ethereal* [Electronic resource]. – Access mode : http://ethereal.com.

9. *A quick-and-dirty* audio sample mixing technique to avoid clipping [Electronic resource]. – Access mode : atastypixel.com/blog/how-to-mix-audio-samples-properly-on-ios.

10. *Mixing* digital audio [Electronic resource]. – Access mode : www.vttoth.com/CMS/index.php/technical-notes/68.

УДК 681.5(042.3)

В.В. Семко, канд. техн. наук
Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ, Україна

ЛОГІКО-МАТЕМАТИЧНА МОДЕЛЬ ОПИСУ ПРОСТОРУ РІШЕНЬ

В.В. Семко, канд. техн. наук
Институт телекоммуникаций и глобального информационного пространства НАН Украины, г. Киев, Украина

ЛОГИКО-МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПИСАНИЯ ПРОСТРАНСТВА РЕШЕНИЙ

V.V. Semko, Candidate of Technical Sciences
Institute of Telecommunications and Global Information Space in the system of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

LOGICAL-MATHEMATICAL MODEL OF THE DESCRIPTION OF DECISIONS SPACE

Розглянуто питання розрахунку підпростору рішень простору спостережень при синтезі гарантованих управлінь у топологічному просторі пошуку. Запропоновано логіко-математичну модель опису підпростору рішень для пошукової системи.

***Ключові слова**: простір спостережень, простір рішень, пошукова система, об'єкт пошуку, топологічний простір.*

Рассмотрены вопросы расчета подпространства решений пространства наблюдений при синтезе гарантированных управлений в топологическом пространстве поиска. Предложена логико-математическая модель описания пространства решений для поисковой системы.

***Ключевые слова:** пространство наблюдений, пространство решений, объект поиска, топологическое пространство.*

The paper presents questions of calculation of decision of space of supervisions subspace are in-process considered at the synthesis of the assured managements in topological space of search. The logical-mathematical model of the description of decision space is offered for the searching system.

***Key words:** space of supervision, space of decisions, object of search, topological space.*

Постановка проблеми. Принциповою відмінністю задач пошуку є те, що при їх вирішенні використовується поточна інформація. Якщо така інформація надходить у дискретні моменти часу з великими інтервалами, синтез алгоритмів пошуку та переслідування зазвичай здійснюється з використанням методів теорії пошуку.

У разі використання методів теорії пошуку традиційно застосовуються ігрові методи. Використання теоретико-автоматних методів під час створення систем синтезу та прийняття рішень дозволяє створити новітні алгоритми пошуку та переслідування.

При цьому великий інтерес є під час застосування теоретико-автоматних методів у разі створення систем синтезу та прийняття рішень.

Під час створення сучасних автоматизованих засобів і систем управління виходять з положень теорії перетворення інформації (загальної теорії алгоритмів, абстрактної теорії автоматів) та теорії побудови різного роду перетворювачів інформації (елементи математичної логіки, абстрактна та структурна теорія автоматів).