ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Шевчук Руслан Петрович

УДК 004.934

БАГАТОКАНАЛЬНІ КОМП'ЮТЕРНІ ЗАСОБИ ПЕРЕТВОРЕННЯ ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ ФОРМАТІВ СТИСНЕНИХ МОВНИХ СИГНАЛІВ

05.13.05- комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2008

Дисертацією є рукопис.

Робота виконана в Тернопільському національному економічному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Мельник Анатолій Олексійович,
Національний університет "Львівська політехніка",
завідувач кафедри "Електронні обчислювальні машини"

Офіційні опоненти: доктор технічних наук, професор
Воробель Роман Антонович,
Фізико-механічний інститут ім. Г. В. Карпенка НАН України, завідувач відділу обчислювальних методів і систем перетворення інформації;

кандидат технічних наук
Бохан Костянтин Олександрович
Національний аерокосмічний університет ім. М.Є.Жуковського "Харківський авіаційний інститут", доцент кафедри комп'ютерних систем та мереж.

Захист відбудеться 11 вересня 2008 р. о 16.00 годині на засіданні спеціалізованої вченої ради К 58.082.02 у Тернопільському національному економічному університеті за адресою: 46009, м. Тернопіль, вул. Львівська 11, тел. (0352) 53-39-82.

З дисертацією можна ознайомитись у бібліотеці Тернопільського національного економічного університету за адресою: 46009, м. Тернопіль, вул. Львівська 11.

Автореферат розісланий "____" серпня 2008 р.

Вчений секретар
спеціалізованої вченої ради,
к.т.н, доцент Яцків В.В.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасний етап розвитку комп'ютерних систем та їх висока гетерогенність вимагають від мережного обладнання, що працює з різними форматами даних, чіткої взаємодії та можливості в реальному часі гарантувати захищену передачу даних з одного сегменту мережі в інший. Відомо, що сьогодні розроблено велику кількість протоколів, які регламентують передачу інформаційних сигналів різних форматів. Зокрема, тільки форматів стиснення мовних сигналів розроблено декілька десятків, і всі вони структурно та семантично різняться між собою. Тому часто виникають ситуації, при яких приймач даних не в змозі їх відтворити, оскільки не має належних засобів для цього. Часто, під час передачі комп'ютерними мережами, втрачається інформаційний зміст даних, оскільки процес передачі слабо захищений від можливих загроз щодо конфіденційності, цілісності та автентичності даних. Для запобігання та уникнення таких ситуацій в комп'ютерні системи вмонтовують засоби перетворення та криптографічного захисту форматів сигналів. Одним з найбільш перспективних на сьогоднішній час напрямів є розробка багатоканальних комп'ютерних засобів перетворення та криптографічного захисту форматів стиснених мовних сигналів, які вмонтовують у комп'ютерні системи IP-телефонії, комп'ютерної телефонії, мультимедіа-конференцій, стільникового зв'язку та спеціалізованих систем зв'язку.

Значний вклад у розвиток засобів перетворення форматів стиснених мовних сигналів внесли: Канг Х.Г, Беаджент К, Тадей Х, Кокс Р.В., Шу-Мін Тсай, Яр-Фер Янг, Бесціер Л. Багато наукових робіт присвячено пошуку нових шляхів стиснення мовних сигналів. Зокрема, необхідно відзначити значний внесок відомих вчених: Котельникова В.А, Шенона К, Рабінера Л.Р, Шафера Л.В, Макхоула Дж, Грея А., Семенова В. Ю, Ватоліна Д. та інші. Алгоритми мікшування мовних сигналів досліджувались у роботах: Ренжен П.В, Гарік М, Ременейшн В.С, Хусейн А.В, Раденковіч М, Хедл Р. Спеціальні питання розробки комп'ютерних засобів захисту інформації досліджувались у роботах Мельника А.О., Хорошко В.О., Задіраки В.К., Николайчука Я.М., Карпінського М.П., Дворянкіна С.В., Петракова А.В.

Проте дослідження у цьому напрямі не втрачають своєї актуальності, оскільки залишилось чимало невирішених проблем. Зокрема, відсутня класифікація існуючих алгоритмів стиснення та мікшування мовних сигналів, яка враховувала б особливості їх побудови та можливості використання у процесі перетворення з одного формату в інший. Існуючі багатоканальні комп'ютерні засоби перетворення форматів стиснених мовних сигналів базуються на класичному методі – тандем кодера-декодера, що призводить до значних часових затримок, високої складності оброблення потоків даних в реальному масштабі часу та втрати якості мови. Відомі структури багатоканальних комп'ютерних засобів перетворення форматів стиснених мовних сигналів не враховують особливості роботи алгоритмів стиснення та мікшування. При передачі стиснених мовних сигналів незахищеними комп'ютерними мережами не враховуються загрози щодо конфіденційності, цілісності та автентичності даних.

Таким чином, актуальною є задача розробки багатоканальних комп'ютерних засобів перетворення та криптографічного захисту форматів стиснених мовних

сигналів, що враховують основні закономірності і особливості функціонування комп'ютерних систем реального часу.

Зв'язок з науковими програмами, планами, темами. Напрямок виконаних дисертаційних досліджень безпосередньо пов'язаний з науково-дослідним напрямком кафедри "комп'ютерних наук" Тернопільського національного економічного університету. Результати, отримані в дисертаційній роботі, використано при виконанні держбюджетної науково-дослідної роботи на тему "Розробка теоретичних засад, алгоритмічного та програмного забезпечення моделювання технічних, екологічних та економічних систем на основі аналізу інтервальних даних" (номер державної реєстрації 0102U002565 (2002-2006 рр.) та у спільній україно-румунській науково-дослідній роботі на тему "Співпраця між Україною і Румунією в галузі розподілених систем" (номер державної реєстрації 0106U005307 (2006-2007 рр.), що виконувались в Тернопільському національному економічному університеті.

Мета і завдання дослідження. Метою досліджень є розробка методів та багатоканальних комп'ютерних засобів для підвищення продуктивності перетворення форматів і криптографічного захисту стиснених мовних сигналів в реальному масштабі часу.

Для досягнення поставленої мети необхідно ефективно розв'язати наступні взаємопов'язані завдання:

1) порівняльний аналіз алгоритмів, що використовуються у процесі перетворення форматів стиснених мовних сигналів з метою узагальнення їх структурних особливостей;
2) порівняльний аналіз комп'ютерних засобів перетворення форматів стиснених мовних сигналів та визначення областей їх доцільного використання;
3) дослідження методів перетворення та мікшування форматів стиснених мовних сигналів;
4) формалізація математичних моделей та створення структур багатоканальних комп'ютерних засобів перетворення форматів стиснених мовних сигналів;
5) удосконалення структур операційних пристроїв криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec, орієнтованих на захист мовних сигналів;
6) дослідження багатоканальних комп'ютерних засобів перетворення форматів стиснених мовних сигналів.

Об'єкт дослідження - перетворення форматів стиснених мовних сигналів у багатоканальних комп'ютерних системах реального часу.

Предмет дослідження - методи та комп'ютерні засоби перетворення форматів та криптографічного захисту стиснених мовних сигналів.

Методи дослідження: основні наукові результати і висновки, одержані на основі теорії інформації, теорії цифрових автоматів, теорії кодування, моделюванні алгоритмів і апаратних засобів комп'ютерів та експериментальних досліджень.

Наукова новизна отриманих результатів. Під час досліджень отримано наступні нові наукові результати:

- запропоновано метод перетворення форматів стиснених мовних сигналів між G.723.1 та G.729A, який на відміну від відомих дає можливість виконувати пряме перетворення ряду параметрів кадру одного формату у параметри кадру іншого та

передбачає виконання чотирьох етапів, зокрема, перетворення лінійних спектральних пар, перетворення висоти тону і пошук у адаптивній та фіксованій кодових книгах. Розроблений метод дозволяє зменшити часову затримку, апаратну складність декодера та покращити якість мовлення;

- запропоновано метод перетворення форматів стиснених мовних сигналів між GSM 06.20 та G.729A, який на відміну від відомих враховує структурну схожість модулів короткотермінової фільтрації, довготермінової фільтрації та випадкового збудження алгоритму лінійного прогнозування, що генерується векторною сумою, а також алгоритму лінійного прогнозування, що генерується алгебраїчним кодом спряженої структури. Це дало можливість провести пряме перетворення параметрів, згенерованих даними модулями. Розроблений метод передбачає виконання трьох етапів, зокрема, перетворення коефіцієнтів лінійного передбачення, перетворення висоти тону і швидкий пошук у фіксованій кодовій книзі та дозволяє зменшити часову затримку і апаратну складність;

- вперше запропоновано метод багатоступінчастого мікшування мовних сигналів на основі пам'яті з довільним доступом, відповідно до якого процес мікшування починається при надходженні хоча б двох блоків даних у цільову комірку пам'яті з довільним доступом, що дозволяє уникати черг у буфері блоку мікшування та зменшити затримки пов'язані з часом очікування блоків даних;

- удосконалено структури операційних пристроїв криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec для різних сервісів оброблення даних за різних технологічних характеристик компонентного базису, що забезпечило зменшення затрат обладнання на їх реалізацію.

Практичне значення одержаних результатів. Отримані результати дисертаційних досліджень використані у розробках КБ "Стріла". За результатами проведених досліджень впроваджено: метод перетворення стиснених мовних сигналів між форматами G.723.1 та G.729A для підвищення ефективності використання каналів зв'язку між територіально віддаленими джерелами формування сигналів багатоканальних комп'ютерних систем реального часу; метод багатоступінчастого мікшування на базі пам'яті з довільним доступом для мікшування мовних сигналів по мірі їх поступлення у багатоканальні засоби комп'ютерних систем; удосконалені структури операційних пристроїв криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec для забезпечення захисту сигналів, що передаються у системах зв'язку реального часу.

Теоретичні та експериментальні результати досліджень впроваджено у навчальний процес на кафедрі "комп'ютерних наук" Тернопільського національного економічного університету при читанні лекцій і проведені лабораторних занять з курсів "Програмне забезпечення мультимедіа", "Методи та засоби захисту програмного забезпечення" і "Методи та засоби вимірювання та цифрової обробки інформації". Результати впроваджень підтверджуються відповідними актами.

Особистий внесок здобувача. Дисертаційна робота є результатом самостійної роботи автора. У працях опублікованих у співавторстві, здобувачу особисто належать: [3] - виділено базові операції алгоритмів MD5 і SHA-1 та на їх основі побудовано структури операційних пристроїв хешування; виділено ряд граф-алгоритмічних операційних пристроїв та отримано аналітичні вирази, що описують

їх часові характеристики; [4,11] - запропоновано математичну модель визначення часових затримок на основних елементах рекурсивної архітектури, що дало змогу отримати аналітичні залежності часових затримок від кількості паралельних мультимедіа конференцій із змінною кількістю учасників. У роботі [5] запропоновано математичну модель операційного пристрою процесора підтримки протоколу IPSec, на основі якої розроблено програмне забезпечення для удосконалення структур операційних пристроїв криптографічного модуля процесора підтримки протоколу IPSec. У роботах: [6] - проведено класифікацію алгоритмів стиснення мовних сигналів, окреслено сучасний стан галузі стиснення мовних сигналів та виділено основні напрямки її розвитку; [7,13] - формалізовано математичну модель та створено структуру багатоканального транскодера стиснених мовних сигналів; [8,14] - запропоновано метод багатоступінчастого мікшування та створено структуру блоку мікшування для його реалізації; [9] - створено модель багатоканального транскодера між G.729A і G.723.1 на базі цифрового сигнального процесора типу TMS320C6201; [10] - проведено аналіз архітектур багатоабоненських мультимедіа-конференцій, на підставі якого запропоновано рекурсивну архітектуру; [12] - проведено порівняльний аналіз протоколів організації мультимедіа-конференцій. [15] - досліджено метод багатоступінчастого мікшування; [16] - запропоновано метод перетворення форматів стиснених мовних сигналів між G.729A і GSM 06.20.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи доповідались та обговорювались на 13-ти міжнародних і національних конференціях: “Проблеми інформатики і моделювання” Харків, 2003; “Сучасні проблеми радіоелектроніки, телекомунікацій та комп’ютерної інженерії” Львів-Славсько, 2004 та 2006; науковій конференції професорсько-викладацького складу, докторантів, аспірантів, здобувачів наукових ступенів “Економічні, правові, інформаційні та гуманітарні проблеми розвитку України в постстабілізаційний період”, Тернопіль 2004-2008; “Наукова конференція Тернопільського технічного університету” Тернопіль, 2004; “Досвід розробки та застосування САПР в мікроелектроніці” Львів-Поляна, 2005 та 2007; “Інтелектуальні засоби збору даних і сучасні обчислювальні системи: розробка і застосування” Софія (Болгарія), 2005 та Дортмунд (Німеччина), 2007.

Публікації. Результати, отримані за час досліджень, опубліковані в шістнадцяти наукових працях, з яких 8 статей у наукових фахових виданнях, одна з яких є одноосібною, 8 тез доповідей в матеріалах конференцій.

Структура дослідження. Дисертація складається з вступу, переліку умовних скорочень, п’яти розділів, висновків, переліку використаних джерел та додатків. Основний зміст роботи викладений на 179 сторінках тексту, 45 рисунків, 33 таблиці, бібліографія з 154 найменувань та додатків загальним обсягом 28 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі наведено загальну характеристику роботи, обґрунтовано її актуальність, сформульовано мету та основні завдання досліджень, визначено методи вирішення поставлених завдань, сформульовано наукову новизну роботи та практичну цінність одержаних результатів, викладено короткий зміст роботи.

Наведені дані про реалізацію та впровадження результатів роботи, її апробацію та публікації.

У першому розділі проведено аналіз особливостей побудови багатоканальних засобів перетворення форматів (транскодування) стиснених мовних сигналів (МС). Висвітлено принципи функціонування комп'ютерних засобів транскодування (транскодерів) стиснених МС у незахищених багатоканальних системах реального часу. Показано переваги та недоліки класичного методу транскодування (тандем) стиснених МС. Визначено умови, при яких доцільно виконувати транскодування та криптографічний захист стиснених МС. Проведено аналіз алгоритмів стиснення та мікшування МС, який дозволив їх класифікувати, виділити переваги і недоліки. Обґрунтовано переваги алгоритмів класу гібридного стиснення МС та багатоступінчастого множинного мікшування МС. Проведено порівняльний аналіз комп'ютерних засобів транскодування стиснених МС, визначено області їх доцільного використання. Доведено, що для комп'ютерних систем реального часу найбільш перспективними є апаратно реалізовані транскодери стиснених МС. Обґрунтовано актуальність завдання дослідження багатоканальних комп'ютерних засобів перетворення та криптографічного захисту форматів стиснених МС. Дослідження показали, що розв'язання цього завдання дозволить підвищити ефективність використання каналів зв'язку, зменшити результуючі затримки між територіально віддаленими джерелами та підвищити ефективність функціонування комп'ютерних систем зв'язку.

У другому розділі запропоновані методи транскодування стиснених МС на основі перспективних алгоритмів класу гібридного стиснення багатоканальних систем IP-телефонії, комп'ютерної телефонії та стільникового зв'язку.

У процесі транскодування стиснених МС блоки даних $L_{i,j}(c_x)$ одного формату перетворюються у блоки даних $L_{i,j}(c_x)$ іншого формату (де c_x – значення відліку стисненого МС, i – порядковий номер блоку; j – номер джерела від якого одержано i-тий блок $i=1,...,s$; $j=1,...,N$; x – порядковий номер відліку, s – кількість блоків створених j-им джерелом; N – кількість джерел, що передають кадри із стисненими МС).

Запропонований метод транскодування між форматами G.729A та G.723.1, що працює відповідно до алгоритмів лінійного прогнозування, що генерується алгебраїчним кодом спряженої структури (ЛПАКСС) та багатоімпульсного квантування з максимальною достовірністю (БКМД), який завдяки подібності структур кодеків алгоритмів дозволяє здійснювати пряме перетворення ряду параметрів кадру одного формату у параметри кадру іншого формату. Розроблений метод передбачає виконання чотирьох етапів: перетворення лінійних спектральних пар (ЛСП), перетворення висоти тону (ВТ), пошук у адаптивній кодовій книзі (АКК) та фіксованій кодовій книзі (ФКК).

Процес виконання першого етапу, методу транскодування з формату G.723.1 до формату G.729A здійснює перетворення вектору ЛСП формату G.723.1 у вектор ЛСП формату G.729A. Оскільки, довжина кадру формату G.723.1 втричі більша від довжини кадру формату G.729A, то в процесі перетворення вектору ЛСП використано метод лінійної інтерполяції. Вектори ЛСП, що містяться у другому та третьому підкадрах кадру формату G.723.1 перетворюються у ЛСП кадрів формату G.729A. Після виконання цього процесу для кожного підкадру формату G.729A

будується перцептуально ваговий синтезуючий фільтр, а вектори ЛСП квантуються та перетворюються до коефіцієнтів лінійного прогнозування (КЛП).

Для визначення ВТ у циклі без зворотного зв'язку формату G.729A використано метод згладжування, у якому враховується подібність та неперервність параметрів ВТ. Для виконання цієї процедури, значення ВТ у циклі із зворотним зв'язком формату G.723.1 порівнюється із значенням ВТ другого підкадру попереднього кадру формату G.729A. Якщо відстань між двома значеннями ВТ менша 10 відліків, то вони неперервні, і значення ВТ одного формату можна представити значенням ВТ іншого формату. У іншому випадку, якщо різниця між значеннями ВТ форматів G.723.1 та G.729A є більшою за 10 відліків, їх локальні затримки максимізуються, а пошук продовжується в діапазоні ±3 відліків навколо значення затримки ВТ у циклі з зворотним зв'язком для двох форматів згідно з виразом:

$$\begin{cases} R(k_1) = \sum_{x=0}^{79} sw(c_x) - sw(c_x - k_1),\ p_1 - 3 \le k_1 \le p_1 + 3 \\ R(k_2) = \sum_{x=0}^{239} sw(c_x) - sw(c_x - k_2),\ p_2 - 3 \le k_2 \le p_2 + 3 \end{cases}, \quad (1)$$

де $R(k_1)$, $R(k_2)$ – максимізовані локальні затримки алгоритмів ЛПАКСС та БКМД;
$sw(c_x)$ – зважений МС, визначений згідно з стандартами G.729A та G.723.1;
k_1,k_2 – шукані значення ВТ у циклі без зворотного зв'язку алгоритмів ЛПАКСС та БКМД;
p_1,p_2 – часова затримка ВТ у циклі із зворотним зв'язком алгоритму ЛПАКСС та БКМД.

Після визначення локальних затримок для форматів G.723.1 та G.729A, значення $R(k_1)$ та $R(k_2)$ нормалізуються через енергію локальних максимальних затримок $R`(t_1)$ та $R`(t_2)$:

$$\begin{cases} R`(t_1) = \dfrac{R(t_1)}{\sqrt{\sum_{x=0}^{79} sw^2(c_x - t_1)}} \\ R`(t_2) = \dfrac{R(t_2)}{\sqrt{\sum_{x=0}^{239} sw^2(c_x - t_2)}} \end{cases}, \quad (2)$$

де t_1, t_2 – час локальних затримок алгоритмів ЛПАКСС та БКМД.

Якщо в процесі порівняння локальний максимум алгоритму ЛПАКС більший, ніж 3/4 часу БКМД, то затримка ВТ у циклі без зворотного зв'язку алгоритму ЛПАКСС буде рівна локальній максимальній затримці алгоритму БКМД. В іншому випадку, значення затримки ВТ T_{op} визначається відповідно до виразу:

$$T_{opt} = \begin{cases} t_1, \text{ якщо } R'(t_2) \le 0{,}75 \cdot R(t_1) \\ t_2, \text{ якщо } R'(t_2) > 0{,}75 \cdot R(t_1) \end{cases}. \quad (3)$$

Третій та четвертий етапи запропонованого методу – пошук в АКК та ФКК. Процедури пошуку повністю ідентичні аналогічним процедурам алгоритму ЛПАКСС. При цьому шуканими параметрами АКК є затримка ВТ - Z_{pot} та

коефіцієнт підсилення ВТ - G_{pot}, а шуканими параметрами ФКК є індекс кодової книги - I_{cb} та коефіцієнт підсилення кодової книги - G_{cb}.

При транскодуванні з G.729A до G.723.1 виконуються однотипні етапи. Для перетворення вектора ЛСП формату G.729A до вектора ЛСП формату G.723.1 використано вектори ЛСП з трьох кадрів формату G.729A. Метод лінійної інтерполяції використовується тільки для знаходження вектора ЛСП четвертого підкадру G.723.1. Для визначення ВТ у циклі без зворотного зв'язку для кадру формату G.723.1 з цільового МС обчислюється перцептуально зважений МС. Також використовується функція зладжування ВТ. Процедури пошуку параметрів в АКК та ФКК ідентичні аналогічним процедурам алгоритму БКМД.

Проведений порівняльний аналіз часових характеристик запропонованого методу показав, що загальна затримка, як мінімум, на 5 мс. менша, ніж у класичному методі, що пояснюється відсутністю процесу аналізу КЛП.

Аналіз алгоритмів ЛПАКСС та лінійного передбачення, що генерується векторною сумою (ЛПГВС) показав, що вони відрізняються лише оптимізаційними процедурами визначення параметрів МС. Порівняння параметрів алгоритмів ЛПАКСС та ЛПГВС показало, що вони різні, а структури та принцип роботи короткотермінового, довготермінового синтезуючих фільтрів та модулів визначення випадкового збудження двох алгоритмів – однакові. На основі проведених досліджень запропоновано ефективний метод транскодування стиснених МС між GSM 06.20 та G.729A, який дає можливість виконувати пряме перетворення параметрів з одного формату в інший.

Модулі алгоритмів ЛПАКСС та ЛПГВС генерують КЛП, ВТ і параметри збудження.

Для здійснення прямого перетворення параметрів збудження, КЛП та ВТ враховано структуру та довжину кадрів форматів G.729A та GSM 06.20. Запропонований метод реалізується етапами: перетворення КЛП, перетворення ВТ та швидкий пошук в ФКК.

На першому етапі короткотерміновий синтезуючий фільтр $A_i(z)$ моделі спектрального перетворення МС має вигляд:

$$A_i(z) = \frac{1}{1 - \sum_{j=1}^{P} a_{ij} z^{-j}}, \quad 0 \le i \le 3, \tag{4}$$

де a_{ij} – КЛП;
P – порядок лінійного прогнозувальника (для алгоритмів ЛПАКСС та ЛПГВС $P=10$).

Інформація про КЛП кадру формату G.729A закодована у векторах ЛСП. Для обчислення значень ЛСП виконуються процедури декомпресії та інтерполяції КЛП кадрів формату G.729A. ЛСП перетворюються до КЛП a_{ij} через обчислення 11-ти відліків імпульсного відгуку аналізуючих фільтрів відповідно до математичної моделі:

$$A(z) = \frac{Q(z) + P(z)}{2}, \tag{5}$$

де *A(z)* – значення аналізуючого фільтру;
Q(z), P(z) – функції визначення коефіцієнтів ЛСП відповідно згідно з стандартом GSM 06.20.

Далі виконується пошук найкращих кодових слів коефіцієнтів відбиття відповідно до математичних моделей, визначених в стандарті GSM 06.20.

На другому етапі обчислюється оптимальне значення ВТ. Обидва кодеки використовують процедуру підвищення частоти дискретизації та дробові значення ВТ: 0,33 для G.729A; 0,33, 0,166 і 0,5 для GSM 06.20. ВТ першого підкадру стискається незалежно від ВТ інших підкадрів. Стиснення значень ВТ наступних підкадрів виконується з врахуванням різниці поточної та попередньої затримки.

Визначення ВТ починається з пошуку значення в розімкнутому циклі та продовжується у закритому циклі.

Дослідження показали, що ВТ у форматі G.729A значно більша, ніж у форматі GSM 06.20, особливо на діапазонах зміни фонем, що пояснюється різним розміром кадрів та діапазонами зміни ВТ обидвох кодеків. ВТ підкадру, одержаного з підкадру формату G.729A, визначається як фіксована ВТ, передана підкадру формату GSM 06.20. На основі використання процесу фіксації ВТ центрального підкадру виконується прямий та зворотний пошук значення ВТ з метою ідентифікації параметрів *LAG1-LAG4* та формування траєкторії ВТ в межах кадру. Для виконання алгоритму прямого пошуку діапазон значень ВТ наступного підкадру обмежується відрізком $[-2^{M-1}+C;\ 2^{M-1}-1-C]$ тонових рівнів (де *M*- визначає кількість біт для кодування значення ВТ, *C* – кількість тонових рівнів), що відповідають значенням ВТ поточного підкадру. Для реалізації алгоритму зворотнього пошуку діапазон значень ВТ обмежується відрізком $[-2^{M-1}+1+C;\ 2^{M-1}-C]$ тонових рівнів. Для обох алгоритмів пошуку, вибирається значення ВТ відповідно до якого значення нормалізованої кореляції в межах пошукового ряду є максимальним. Для кадру формату GSM 06.20 доцільно вибрати траєкторію ВТ з найменшою енергією помилки довготермінового прогнозувальника.

На третьому етапі запропонованого методу у модулях алгоритмів ЛПАКСС і ЛППГВС обчислюється випадкове збудження із залишку МС після оцінки ВТ. Значення випадкового збудження алгоритму ЛПАКСС визначається наступним чином:

$$e'_{random}[c_x] = e_{pitch}[c_x] + e_{random}[c_x] - e'_{pitch}[c_x], \qquad (6)$$

де $e_{pitch}[c_x]$ – функція випадкового збудження;
$e_{random}[c_x]$ – функція адаптивного збудження;
$e'_{pitch}[c_x]$ – функція збудження ВТ, що отримується після перетворення параметрів ВТ.

Транскодування з GSM 06.20 до формату G.729A доцільно реалізовувати за три етапи: перетворення КЛП, перетворення ВТ та швидкий пошук у ФКК.

Перетворення ЛСП залежить від довжини кадрів та виконується відповідно до методу лінійної інтерполяції. Для формування математичної моделі перетворення ЛСП присвоїмо номери підкадрам: *g1, g2, g3, g4* – кадру формату GSM 06.20; *b1, b2* – кадру формату G.729A; *c1, c2* – наступного кадру формату G.729A. Оскільки довжина одного кадру формату GSM 06.20 вдвічі більша за довжину кадру формату G.729A, то перетворення ЛСП відображає така математична модель:

$$LSP_{b2}^{G.729A}(i) = t \cdot LSP_{g1}^{GSM\ 06.20}(i) + y \cdot LSP_{g2}^{GSM\ 06.20}(i); \quad (7)$$

$$LSP_{c2}^{G.729A}(i) = t \cdot LSP_{g3}^{GSM\ 06.20}(i) + y \cdot LSP_{g4}^{GSM\ 06.20}(i), \quad (8)$$

де $1 \le i \le 10$;

t, y – вагові коефіцієнти;

$LSP_{b2}^{G.729A}(i)$, $LSP_{c2}^{G.729A}(i)$ – ЛСП підкадрів формату G.729A;

$LSP_{g1}^{GSM\ 06.20}(i)$ $LSP_{g2}^{GSM\ 06.20}(i)$ $LSP_{g3}^{GSM\ 06.20}(i)$ $LSP_{g4}^{GSM\ 06.20}(i)$ – ЛСП підкадрів формату GSM 06.20.

Для перетворення ЛСП підкадру *b1* використано метод лінійної інтерполяції:

$$LSP_{b1}^{G.729A}(i) = 0{,}5 \cdot LSP_{b2}^{G.729A}(i) + 0{,}5 \cdot LSP_{c2}^{G.729A}(i), \quad (9)$$

де $LSP_{b1}^{G.729A}(i)$ - ЛСП підкадру *b1* формату G.729A.

Доведено, що запропоновані математичні моделі (7-9) дозволяють скоротити часову затримку, яка виникає при аналізі КЛП, та зменшити обчислювальну складність у порівнянні з класичним методом, оскільки не виконуються процедури обчислення автокореляційних коефіцієнтів, рекурсії Дарбіна при визначення КЛП та перетворення КЛП в ЛСП.

Оскільки, стиснений МС формату GSM 06.20 описується в сегменті голосних та приголосних звуків, то визначення ВТ для підкадру формату G.729A відбувається окремо для кожного сегменту звуків. У випадку, коли МС належить сегменту голосних звуків, то ВТ у розімкнутому циклі алгоритму ЛПАКСС є цілочисельним значенням тонової затримки T одержаним з кадру формату GSM 06.20. Далі виконується процедура пошуку ВТ в замкнутому циклі для значень: T, $T+1/3$, $T+2/3$ і $T+1$. У випадку, коли МС належить сегменту приголосних звуків, тонову затримку визначити неможливо. Тому для оцінки тонової затримки використовується значення ВТ, отримане з попереднього підкадру формату G.729A.

Результатом виконання процедури пошуку в ФКК алгоритму ЛППГВС є значення функції вартості описаної в стандарті GSM 06.20, яка досягає максимуму.

У роботі запропоновано метод багатоступінчастого мікшування на базі пам'яті з довільним доступом (адресної пам'яті). Структурна схема блоку мікшування МС (рис.1) ілюструє реалізацію запропонованого методу.

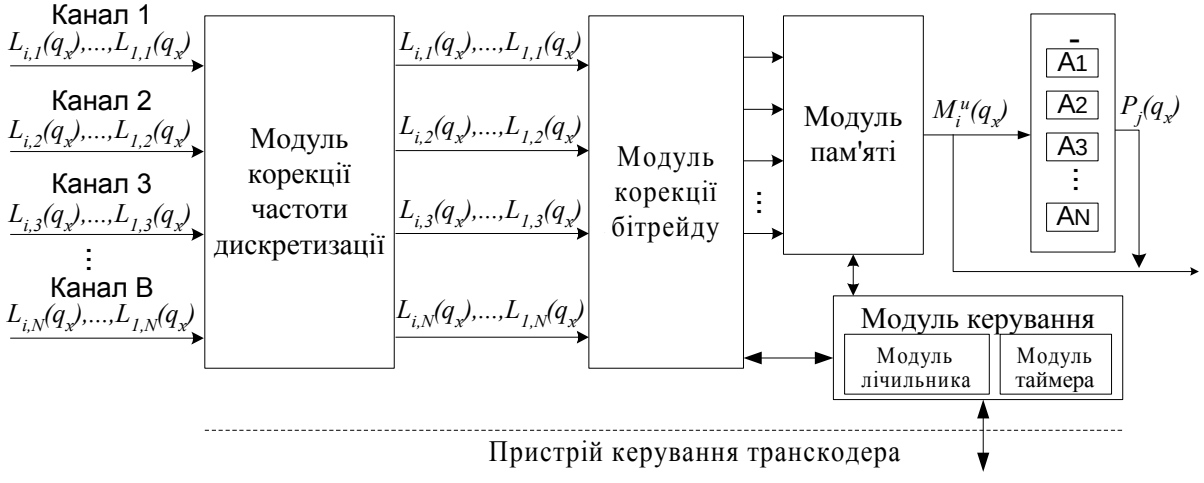


Рис. 1. Структура схема блоку багатоступінчастого мікшування

Як видно з рис. 1, значення відліків МС q_x через B вхідних каналів блоку мікшування (БМ) поступають у модуль корекції частоти дискретизації. Якщо частота дискретизації відліків q_x не рівна 8 КГц, то виконується алгоритм передискретизації. В іншому випадку дані передаються у модуль корекції бітрейду, де значення відліків q_x приводяться до 16-ти бітового формату та синхронізується розмір блоку даних. З модуля корекції бітрейду блоки даних $L_{i,j}(q_x)$ передаються у модулі пам'яті з довільним доступом, де для кожного i-го блоку виділяється комірка пам'яті обсягом $Lb(L_{i,j}(q_x))$ байт, якій присвоюється відповідна адреса. Процес мікшування виконується у комірках модуля пам'яті відповідно до принципу роботи методів багатоступінчастого мікшування. Тому значення відліків q_x з i-го блоку даних сумуються у комірках пам'яті по мірі їх надходження згідно виразу:

$$M_i^u(q_x) = \sum_{j=1}^{N} L_{i,j}(q_x), \qquad (11)$$

де $M_i^u(q_x)$ - функція мікшування.

Усі комірки модуля пам'яті адресуються відповідно до відмітки RTP-часу. Пристрій керування виконує процес заповнення комірок модуля пам'яті блоками даних $L_{i,j}(q_x)$. Модулі лічильника та таймера визначають момент часу в який необхідно передати значення $M_i^u(q_x)$ з комірки модуля пам'яті у модуль виключення власного блоку даних. Після отриманням даних $M_i^u(q_x)$ виконується процедура виключення власного блоку даних для кожного активного джерела згідно з виразом:

$$P_j(q_x) = M_i^u(q_x) - L_{i,j}(q_x), \qquad (12)$$

де $P_j(q_x)$ – функція виключення власного блоку даних j-го джерела сеансу зв'язку.

Запропонований метод мікшує значення відліків q_x по мірі надходження блоків даних $L_{i,j}(q_x)$, що дозволяє уникати черг та зменшити затримки. Результатом роботи БМ є значення $P_j(q_x)$ із RTP-заголовком для кожного даних j-го джерела сеансу зв'язку.

У процесі дослідження залежності швидкості виконання реалізованого методу від кількості wav-файлів та їх характеристик отримано експериментальні дані над випадковим чином вибраними файлами (табл.1).

Таблиця 1

Характеристики wav-файлів

№ п\п	Кількість відліків	Бітрейд	Частота дискретизації, КГц	Довжина блоку даних, біт	Довжина блоку даних, сек.	Кількість каналів	Опис
1	14592	8	8	240016	30	1	фрагмент мови, жіночий голос
2	240588	16	8	481176	30	1	жіночий спів
3	1323008	16	44,1	2646016	30	1	звук віаланчелі
4	1323008	16	44,1	5292032	30	2	музичний фрагмент
5	661520	16	22,05	2646080	30	2	стандартний звук Windows (Chimes)
6	330768	16	11,025	661536	30	1	звук, аплодисменти
7	240016	8	20,1	603250	30	1	МС, чоловічий голос

На рис. 2 показано зміну часу мікшування двох wav-файлів. Кількісні показники на рисунках отримані засобами профілювання розробленого алгоритму в середовищі Matlab 6.0 без використання підпрограм виведення графічної інформації на процесорі Celeron 666 МГц.

Результати досліджень показали, що на час мікшування значно впливають: частота дискретизації; кількість біт, якими кодується відлік; кількість каналів; розмір data-чанку.

У роботі доведено, що при частоті дискретизації 8 КГц, 16-ти бітному кодуванню відліку та стерео звучанню запропонований метод є найефективніший.

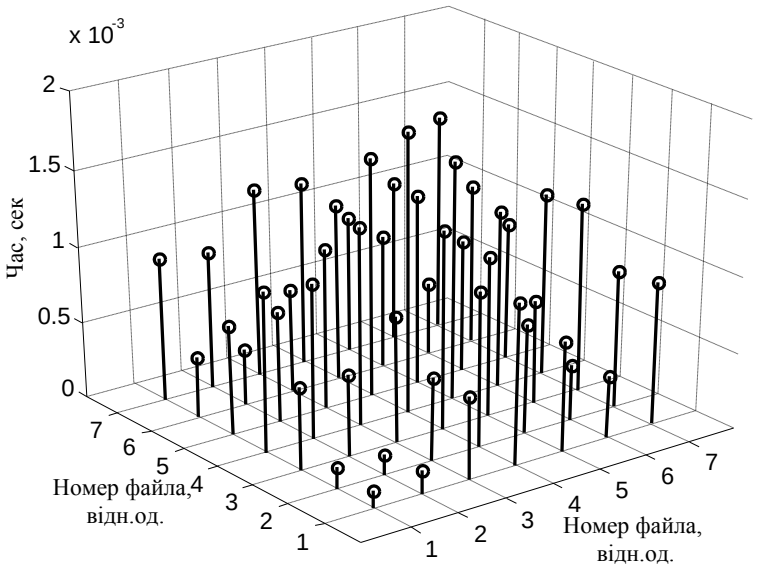


Рис. 2. Залежність часу мікшування двох wav-файлів від їх порядкових номерів

У третьому розділі сформовано принципи та запропоновано алгоритми оброблення кадрів із блоками даних $L_{i,j}(c_x)$ багатоканальним транскодером. На основі запропонованих у другому розділі методів удосконалено структури багатоканальних транскодерів стиснених МС.

Структурна організація багатоканального транскодера стиснених МС представляється у виді трьох складових: процедури декомпресії, мікшування та компресії (рис.4).

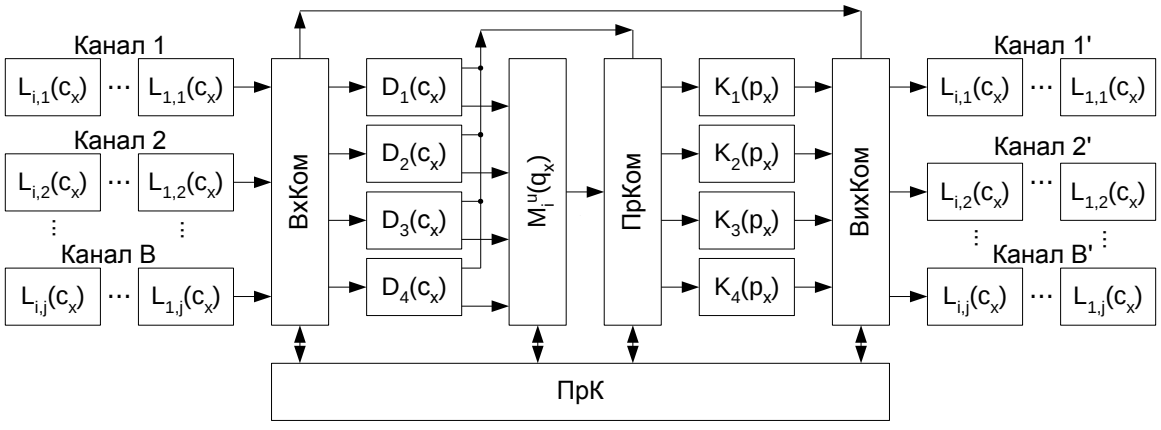


Рис.4. Структурна схема багатоканального транскодера

З рис. 4 витікає, що багатоканальний транскодер є лінійною конвеєрною схемою із послідовно з'єднаних вхідного комутатора (ВхКом), декомпресорів $(D_1(c_x)\text{-}D_4(c_x))$, БМ $(M_i^u(q_x))$, проміжного комутатора (ПрКом), модулів стиснення $(K_1(p_x)\text{-}K_4(p_x))$ та вихідного комутатора (ВихКом). Розглянемо детальніше процес проходження блоків даних у багатоканальному транскодері. Чергові блоки даних $L_{i,j}(c_x)$ з активних каналів передачі подаються у ВхКом, який паралельно отримує інформацію з ПрКом про початковий a $(a \in F)$ та кінцевий формат даних b $(b \in F)$, а також кількість учасників сеансу зв'язку N. Далі, відповідно до запропонованого алгоритму, виконується опрацювання вхідних блоків даних $L_{i,j}(c_x)$, які з вхідного комутатора відправляються у модулі транскодера для подальшого перетворення. Функціями проміжного комутатора є зберігання та відправлення блоків даних $L_{i,j}(p_x)$ у відповідні модулі стиснення. Функціями вихідного комутатора є зберігання та видача у канали зв'язку опрацьованих даних. Керування процесом транскодування виконується пристроєм керування, який відправляє у модулі транскодера інформацію про алгоритми стиснення та мікшування МС, а також інформацію про стан опрацювання блоків даних $L_{i,j}(c_x)$.

На основі запропонованих у другому розділі методів транскодування удосконалено структурні схеми транскодерів стиснених МС, які виконують пряме перетворення параметрів кадрів між форматами G.729A та G.723.1, а також між форматами G.729A та GSM 06.20. В якості прикладу на рис. 5 наведена структурна схема транскодера з GSM 06.20 до G.729A.

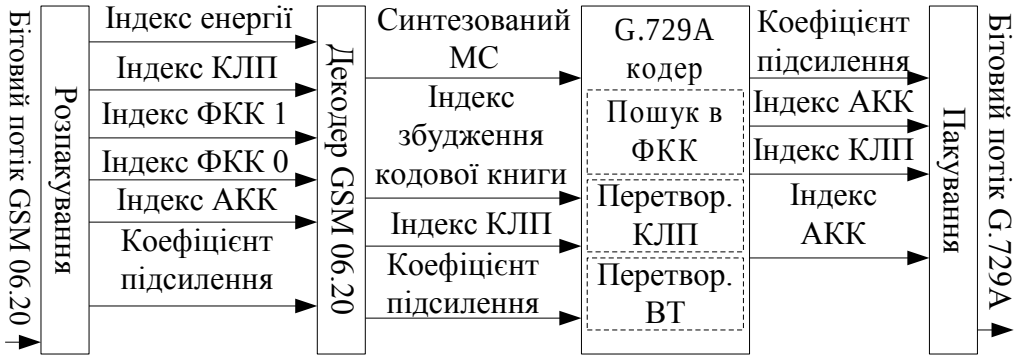


Рис. 5. Структурна схема транскодера з GSM 06.20 до G.729A.

Удосконалені структури орієнтовані на використання в мережевому обладнанні багатоабоненських конвергентних мереж та дають можливість обробляти формати стиснених МС регламентовані стандартом H.323v2. Дослідження показали, що використання удосконалених структур транскодерів дозволяє підвищити продуктивність оброблення блоків даних $L_{i,j}(c_x)$.

У четвертому розділі проведено дослідження базових структур операційних пристроїв (ОП) криптографічних алгоритмів для процесорів підтримки протоколу IPSec, що дозволило побудувати аналітичні вирази, які описують час оброблення кадрів із блоками даних $L_{i,j}(c_x)$, залежно від параметрів структури ОП.

На основі побудованих аналітичних виразів у роботі запропоновано математичну модель ОП процесора підтримки протоколу IPSec, параметром якої є значення відображення потокових графів базових криптографічних алгоритмів. Аргументами математичної моделі ОП є алгоритми оброблення кадрів із блоками

даних $L_{i,j}(c_x)$, технологічні характеристики компонентного базису реалізації та перелік сервісів протоколу IPSec.

Враховуючи сучасні тенденції розвитку комп'ютерних систем та їх компонентів, у яких довжина кадру пов'язана із швидкістю його поступлення, розроблено програмне забезпечення для пошуку оптимальних параметрів структур ОП криптографічних модулів процесорів підтримки протоколу IPSec.

У табл. 2 наведено перелік удосконалених характеристик структур ОП криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec для різних сервісів оброблення даних за різних технологічних характеристик компонентного базису.

Таблиця 2

Удосконалені характеристики структур ОП криптографічних модулів процесорів підтримки протоколу IPSec

Розмір кадру, біт	Швидкість поступлення кадрів, Кбіт/с	Сервіси протоколу IPSec				
		AH (MD5)	AH (SHA-1)	ESP (DES)	AH+ESP (MD5,DES)	AH+ESP (SHA-1,DES)
256	64	i(64;1)	i(80;1)	ik(2;8)	i(64;1),ik(8;2)	i(80;1), ik(8;2)
512	128	i(64;1)	i(80;1)	ik(8;8)	i(64;1),ik(8;2)	i(64;1), ik(8;2)
2048	512	i(64;1)	i(80;1)	ik(2;8)	i(64;1),ik(8;2)	i(64;1), ik(8;2)
6144	1576	i(64;1)	i(80;1)	ik(8;8)	i(64;1),ik(16;8)	i(64;1), ik(16;2)

Синтезовано ОП хешування та шифрування на програмовану логічну інтегральну схему типу ALTERA EPF10K50-3, що дозволило визначити технологічні характеристики для знаходження параметрів структур ОП криптографічних модулів процесора підтримки протоколу IPSec. Для ідентифікації структур ОП було використано наступне умовне позначення: $SN(Nksr, Npp)$, де SN – код назви структури ОП ("і" – ітераційний граф-алгоритмічний ОП, "к" – конвеєрний граф-алгоритмічний ОП, "ік" – ітераційно-конвеєрний граф-алгоритмічний ОП), $Nksr$, Npp – параметри структур ОП (кількість реалізованих комбінаційних схем і конвеєрних регістрів відповідно). У роботі доведено, що реалізація отриманих удосконалених структур ОП (табл.2) виконується із мінімальними затратами обладнання.

На рис. 6 подано графік залежності часу оброблення кадрів різного розміру від кількості операцій сервісів AH, ESP та AH+ESP протоколу IPSec.

Аналіз графіку дозволяє зробити висновок, що найменша тривалість часу оброблення кадрів спостерігається при використанні сервісу ESP відповідно до алгоритму DES. Із збільшенням розміру кадру значення часу його опрацювання зростає прямопропорційно. Найбільший час оброблення кадрів спостерігається при автентифікуванні, відповідно до алгоритму SHA-1 та суміщенні сервісів протоколу IPSec (AH+ESP).

Аналіз отриманих результатів дозволив встановити, що в більшості випадків найменший час оброблення кадрів спостерігається при ітераційній та ітераційно-конвеєрній реалізації криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec.

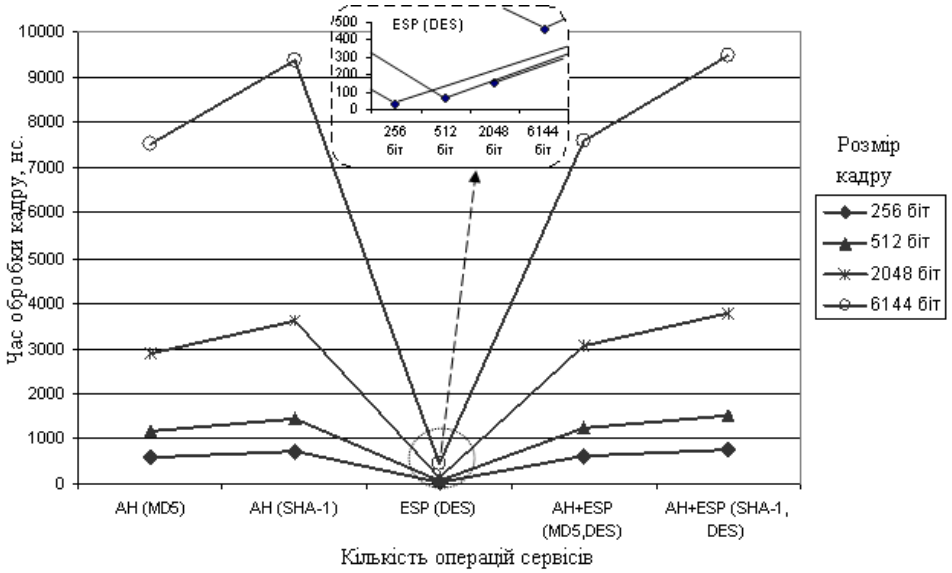


Рис. 6. Графік залежності часу оброблення кадрів різного розміру від кількості операцій сервісів протоколу IPSec

У п'ятому розділі на високорівневій мові програмування Visual C++ 6.0 з пакету Microsoft Visual Studio розроблено програмне забезпечення для транскодування стиснених звукових та мовних сигналів. Розроблений комп'ютерний засіб працює з такими кодеками: WMA Voice Encoder DMO, WM Speech Encoder DMO, WM Audio Encoder DMO, 3ivx D4 Audio Encoder, Indeo Audio Software, Pinnacle AC3 Encoder, Pinnacle AC3 Encoder, Pinnacle MP3 Encoder, Pinnacle MPEG Layer-2 Audio Encoder, Vorbis Encoder, IMC, IAC2, IMA ADPCM, PCM, Ogg Vorbis, Microsoft ADPCM, ACELP.net, DSP Group TrueSpeech, Windows Media Audio, GSM 06.10, G.723.1, CCITT A-Law, CCITT u-Law, AC-3 ACM Codec, MPEG Layer-3. Частоти дискретизації використаних кодеків змінюються від 8 до 96 КГц, швидкість від 0,1 до 768 Кб/с, кількість каналів від 1 до 5. Транскодування виконуються за допомогою функцій відображення бібліотеки Audio Compression Manager.

Розроблено програмне забезпечення виконання алгоритмів БКМД та ЛПАКСС для процесорів типу TMS320C6201. Програмні реалізації відповідають вимогами стандартів ITU-T G.723.1, ITU-T G.729A.

У роботі проведено дослідження апаратної складності реалізації кодеків розроблених алгоритмів. На рис.7 проілюстровано використання обчислювального ресурсу кодеками, що працюють відповідно до алгоритмів БКМД та ЛПАКС. На рис.8 проілюстровано використання пам'яті восьми канальним кодеком, що працюють відповідно до розроблених алгоритмів.

Реалізації кодеків дозволили розробити програмне забезпечення транскодування стиснених МС між форматами G.723.1 та G.729A на базі цифрового сигнального процесора типу TMS320C6201.

Для експериментальної оцінки реалізованого транскодера стиснених МС між G.729A та G.723.1 виконано тести оцінки якості мовлення PESQ та часової складності транскодування.

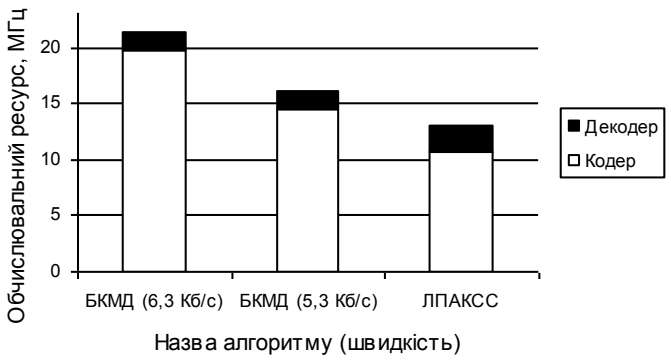


Рис. 7. Частота кодеків алгоритмів

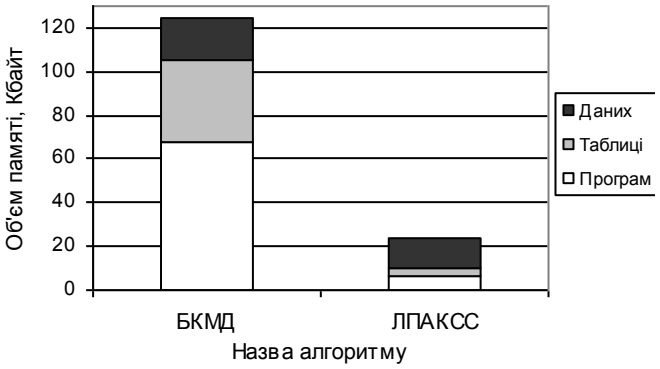
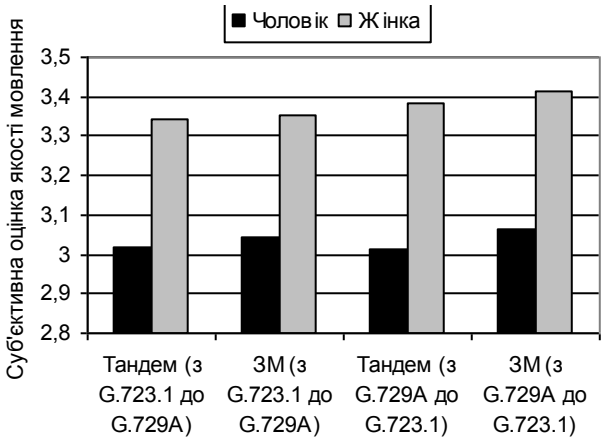
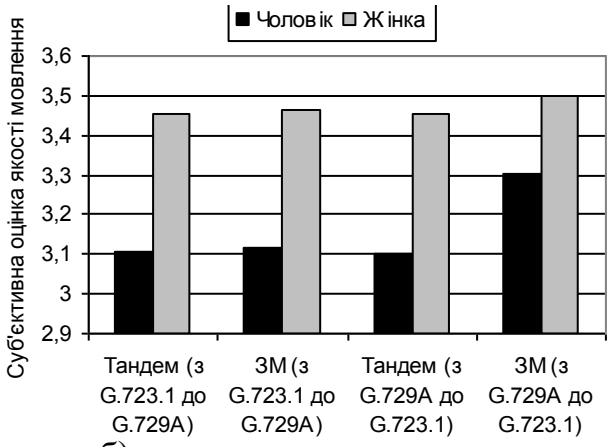


Рис. 8. Використання пам'яті

Для оцінки якості мови використані МС з бази фрагментів "ISABASE". Кожне речення мало довжину 8 секунд з частотою дискретизації 8 КГц. Дикторами було взято 4 чоловіки та 4 жінки і по 24 речення на кожного. На рис. 9 наведено результати оцінки якості мовлення відповідно до проведених тестів.



а)



б)

Рис. 9. Оцінка якості мовлення: а) формат G.723.1, 5.3 Кб/с; б) формат G.723.1, 6.3 Кб/с.

Для оцінки апаратної складності проведено серію обчислювальних експериментів з реалізованим транскодером на базі процесора типу TMS320C6201. У результаті порівняння одержаних результатів з даними реалізації класичного методу на цій же елементній базі встановлено, що апаратна складність стиснення МС змінюється, оскільки діапазон пошуку залежить від вхідного МС. Однак діапазон зміни апаратної складності в модулі декодування є незначним. Результати експериментів апаратної складності удосконаленого транскодера стиснених МС, наведені на рис. 10, показали, що запропонований метод забезпечує на 29,5-51,6% меншу апаратну складність у порівнянні з класичним методом.

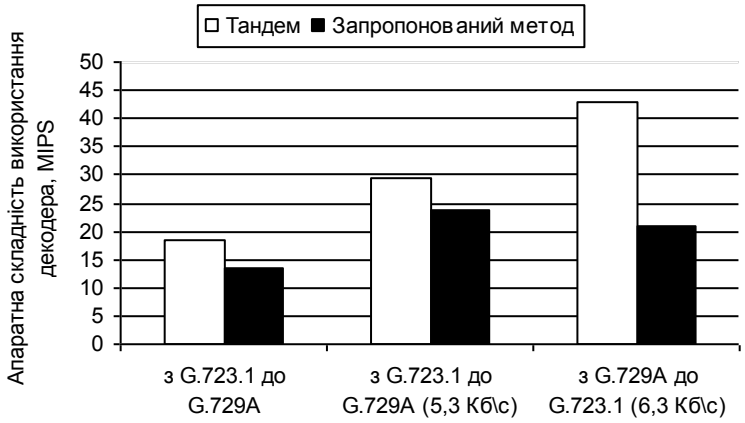


Рис. 10. Порівняння апаратної складності використання декодерів алгоритмів БКМД і ЛПАКСС під час транскодування

Отже, програмна реалізація удосконаленого транскодера на основі використання запропонованого методу транскодування між форматами G.729A та G.723.1 забезпечує кращу якість мовлення (0,3%-1,7% - під час транскодування з G.729A до G.723.1 5,3 Кб/с; 0,3%-6,4% - під час транскодування з G.729A до G.723.1 6,3 Кб/с) та меншу апаратну складність (25,9%-51,6%) у порівнянні з класичним методом.

У додатках подано документи, що підтверджують впровадження результатів наукових досліджень дисертації, наведено коди програм, а також блок-схеми розроблених алгоритмів.

ВИСНОВКИ

1. Проведено аналіз алгоритмів стиснення та мікшування МС, який дозволив їх класифікувати, виділити переваги і недоліки та окреслити перспективні напрями їх розвитку. Обґрунтовано, що найперспективнішими є алгоритми класу гібридного стиснення МС та багатоступінчастого множинного мікшування МС. Проведено порівняльний аналіз комп'ютерних засобів транскодування стиснених МС, визначено області їх доцільного використання. Показано, що для комп'ютерних систем реального часу найбільш перспективними є апаратно реалізовані транскодери стиснених МС.

2. Запропоновано метод перетворення форматів стиснених МС між GSM 06.20 та G.729A, що враховує структурну схожість модулів короткотермінової фільтрації, довготермінової фільтрації та випадкового збудження алгоритмів ЛППГВС та ЛПАКСС, яка дає можливість провести пряме перетворення параметрів, згенерованих даними модулями. Розроблений метод дозволяє зменшити часову затримку і апаратну складність у порівнянні з класичним методом.

3. Запропоновано метод перетворення форматів стиснених МС між G.723.1 та G.729A, який дає можливість виконувати пряме перетворення ряду параметрів кадру одного формату у параметри кадру іншого та передбачає виконання чотирьох етапів: перетворення ЛСП, перетворення ВТ, пошук у АКК та ФКК. Розроблений метод дозволяє зменшити часову затримку, апаратну складність використання декодера та покращити якість мовлення.

4. Вперше запропоновано метод багатоступінчастого мікшування МС на основі пам'яті з довільним доступом, який дає можливість опрацьовувати значення відліків з блоків даних, що були одержані шляхом декомпресії стиснених МС різних форматів. Процес мікшування починається при надходженні хоча б двох блоків даних у цільову комірку пам'яті з довільним доступом, що дозволяє уникати черг у буфері БМ та зменшити затримки пов'язані з часом очікування блоків даних.

5. Запропоновано алгоритми оброблення блоків даних $L_{i,j}(c_x)$ і удосконалено структури багатоканальних транскодерів стиснених МС орієнтовані на використання в мережевому обладнанні багатоабоненських конвергентних мереж. Дослідження показали, що використання удосконалених структур транскодерів дозволяє підвищити продуктивність оброблення блоків даних $L_{i,j}(c_x)$.

6. Запропоновано принципи побудови ОП криптографічних модулів процесорів підтримки протоколу IPSec. Дані принципи дозволили удосконалити характеристики структур криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec для різних сервісів оброблення даних за різних технологічних характеристик компонентного базису, що забезпечило зменшення затрат обладнання на їх реалізацію.

7. Створено реалізації багатоканальних комп'ютерних засобів транскодування стиснених МС. Результати комп'ютерного моделювання показали, що реалізація удосконаленого транскодера на основі використання запропонованого методу транскодування між G.729A та G.723.1, забезпечує кращу якість мови (до 6,4%) та використовує до 51,6% менше апаратних ресурсів у порівнянні з класичним методом.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Шевчук Р.П. Транскодування стиснених мовних сигналів між GSM 06.20 та G.729 / Р.П. Шевчук // Міжнародний науково-технічний журнал "Інформаційні технології та комп'ютерна інженерія" – 2007. – № 3. – С. 172–179.
2. Shevchuk R. Method of converting speech codec formats between G.723.1 and G.729A / R. Shevchuk // Proc. of the Intern. Conf. "Experience of Designing and Application of CAD Systems in Microelectronics" (CADSM'2007). – Lviv-Polyana, 2007. – P. 483–486.
3. Коркішко Т. Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSec / Т. Коркішко, Л. Коркішко, Р. Шевчук // Комп'ютинг. – 2003. – Т. 2, № 1. – С. 41–47.
4. Коркішко Т. Часові характеристики паралельних багатоабонентських мультимедіа конференцій рекурсивної архітектури / Т. Коркішко, Р. Шевчук // Вісник Тернопільського державного технічного університету. – 2004. – № 2. – С. 109 –116.
5. Коркішко Т. Синтез структур операційних пристроїв виконання криптографічних алгоритмів IPSEC оптимізованих для обробки медіа пакетів / Т. Коркішко, Р. Шевчук // Комп'ютинг. – 2004. – Т. 3, № 3. – С. 100–109.
6. Мельник А. Порівняльний аналіз алгоритмів стиснення мовних сигналів / А. Мельник, Р. Шевчук // Вісник національного університету "Львівська політехніка" Комп'ютерні системи і мережі. – 2004. № 523. – С. 109–117.

7. Мельник А. Особливості багатоканального транскодування форматів стиснених мовних сигналів / А. Мельник, Р.Шевчук // Вісник Тернопільського державного технічного університету. – 2005. – № 2. – С. 122–128.

8. Мельник А.О. Мікшування мовних сигналів у мультимедійних системах реального часу / А.О. Мельник, Р.П. Шевчук, Т.А. Коркішко // Комп'ютинг. – 2006. – Т.5, № 1. – С. 57–65.

9. Шевчук Р.П. Проектування багатоканального транскодера між G.723.1 та G.729A / Р.П. Шевчук, Л.І. Гончар // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2007. – № 2. – С.124–129.

10. Коркішко Т. Аналіз архітектур багатоабонентських мультимедіа-конференцій / Т. Коркішко, Р. Шевчук // Матеріали третьої міжнародної науково-технічної конференції "Проблеми інформатики і моделювання". – Харків. – 2003. – С. 6.

11. Korkishko T. Investigation of the characteristics of recursive architecture for multipoint parallel multimedia conferences / T. Korkishko, R. Shevchuk // Proc. of the Intern. Conf. "Modern Problems of Radio Engineering, Telecommunications, and Computer Science" (TCSET'2004). – Lviv-Slavsko, 2004. – P. 388–390.

12. Шевчук Р. Особливості організації мультимедіа конференцій / Р. Шевчук, А. Чвиль // Матеріали VIII наукової конференції ТДТУ імені Івана Пулюя. – Тернопіль. – 2004. – С. 88.

13. Melnik A. Transcoding of Formats of Compressed Speech Signals / A. Melnik, R. Shevchuk // Proc. of the 8-th Intern. Conf. Proc. of the Intern. Conf. "Experience of Designing and Application of CAD Systems in Microelectronics" (CADSM'2005). – Lviv-Polyana, 2005. – P. 151–153.

14. Melnik A. Method of multistage mixing speech signals for the real-time multimedia systems / A. Melnik, T. Korkishko, R. Shevchuk // Proc. of the Intern. Workshop "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications". – Sofia, Bulgaria, 2005. – P. 653–656.

15. Melnik A. Multichannel mixing of speech signals accordant with the method of multistage mixing / A. Melnik, R. Shevchuk, H. Sapozhnyk // Proc. of the Intern. Conf. "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET'2006). – Lviv-Slavsko, 2006. – P. 169–172.

16. Shevchuk R.P. Method of converting speech codec formats between GSM 06.20 and G.729 / R. Shevchuk, L. Honchar, P. Bykovyy // Proc. of the 4-th IEEE Workshop "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications". – Dortmund, Germany, 2007. – P. 686–689.

АНОТАЦІЯ

Шевчук Р.П. Багатоканальні комп'ютерні засоби перетворення та криптографічного захисту форматів стиснених мовних сигналів. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Тернопільський національний економічний університет, Тернопіль, 2008.

Дисертація присвячена удосконаленню багатоканальних комп'ютерних засобів перетворення та криптографічного захисту форматів стиснених мовних сигналів.

Запропоновано класифікацію алгоритмів стиснення та мікшування мовних сигналів, що враховує особливості їх побудови та можливості використання у процесі перетворення стиснених МС. Запропоновано методи перетворення між форматами GSM 06.20, G.729A, G.723.1, які дають можливість проводити пряме перетворення параметрів кадру одного формату в інший. Запропоновані методи покращують якість мови, зменшують часову затримку та апаратну складність у порівнянні з класичним методом перетворення, що підтверджують результати експериментів з їх реалізацією. Запропоновано метод багатоступінчастого мікшування мовних сигналів на основі пам'яті з довільним доступом, що дозволяє ефективно опрацьовувати значення відліків з блоків даних, що були одержані шляхом декомпресії стиснених мовних сигналів різних форматів. Процес мікшування починається при надходженні хоча б двох блоків даних у цільову комірку пам'яті з довільним доступом, що дозволяє уникати черг у буфері блоку мікшування та зменшити затримки пов'язані з часом очікування блоків даних. Удосконалено структури ОП криптографічних модулів апаратно-орієнтованих процесорів підтримки протоколу IPSec для різних сервісів оброблення даних за різних технологічних характеристик компонентного базису, що забезпечило зменшення затрат обладнання на їх реалізацію.

Ключові слова: багатоканальні комп'ютерні засоби, перетворення форматів, мікшування, транскодування, стиснення мовних сигналів, структури операційних пристроїв, IPSec.

АННОТАЦИЯ

Шевчук Р.П. Многоканальные компьютерные устройства преобразования и криптографической защиты форматов сжатых речевых сигналов. - Рукопись.

Диссертация на соискание учёной степени кандидата технических наук по специальности 05.13.05 - компьютерные системы и компоненты. - Тернопольский национальный экономический университет, Тернополь, 2008.

Диссертация посвящена усовершенствованию многоканальных компьютерных устройств преобразования и криптографической защиты форматов сжатых речевых сигналов (РС).

В работе проанализировано существующие алгоритмы сжатия и микширования РС, выделено их преимущества и недостатки, показано перспективные направления их развития. Проанализировано компьютерные устройства транскодирования сжатых РС и определены области их целесообразного использования. Доказано, что для компьютерных систем реального времени наиболее перспективными являются аппаратные транскодеры сжатых РЧ.

Предложены методы преобразования между форматами GSM 06.20, G.729A, G.723.1, которые дают возможность напрямую проводить преобразования параметров кадра одного формата в другой. Разработанные методы улучшают качество РС, уменьшают часовую задержку и аппаратную сложность в сравнении с известными методами.

Предложен метод многоступенчатого микширования РС на базе памяти с произвольным доступом, в соответствии с которым процесс микширования начинается при поступлении хотя бы двух блоков данных в целевую ячейку памяти

с произвольным доступом, что позволяет избегать очередей в буфере блока микширования и уменьшить задержки связанные с временем ожидания блоков данных.

Предложены алгоритмы обработки блоков данных с сжатыми РС и усовершенствованы структуры многоканальных транскодеров сжатых РС ориентированные на использование в сетевом оборудовании многоабонентских конвергентных сетей.

Предложены принципы построения операционных устройств криптографических модулей процессоров поддержки протокола IPSec. Усовершенствованы структуры операционных устройств криптографических модулей аппаратно-ориентированных процессоров поддержки протокола IPSec для разных сервисов обработки данных при разных технологических характеристиках компонентного базиса, что обеспечило уменьшение затрат оборудования на их реализацию.

Созданы реализации многоканальных компьютерных устройств транскодирования сжатых РС. Результаты компьютерного моделирования показали, что реализация усовершенствованного транскодера на основе использования предложенного метода транскодирования между G.729A и G.723.1, обеспечивает лучшее качество речи (до 6,4%) и использует на 19,5%-51,6% меньше аппаратных ресурсов в сравнении с классическим методом.

Ключевые слова: многоканальные компьютерные устройства, преобразование форматов, микширование, транскодирования, сжатие речевых сигналов, структуры операционных устройств, IPSec.

ABSTRACT

Shevchuk R.P. Multichannel computer facilities of converting and cryptographic defence formats of compression speech signals. - Manuscript.

The work for competition for a candidate degree of technical sciences by specialty 05.13.05 – Computer systems and components. it is the Ternopil National Economical University, Ternopil, 2008.

The dissertation work is devoted of improvement of multichannel computer facilities of converting and cryptographic defence formats of compression speech signals. The developed methods of converting compression of speech signal between formats GSM 06.20, G.729A, G.723.1, which enable to conduct the direct converting of parameters from one format into other. The developed method of multi-stage mixing speech signals on the basis of memory with arbitrary access, that to avoid turns in the mixer buffer and shorted processing delay. The improved structures operating device cryptographic modules of the processors IPSec for different services of data processing at different technological descriptions of component base, that provided reduce complexity.

Keywords: multichannel computer facilities, converting formats, mixing, transcoding, speech signals, structure of operating device, IPSec.