УДК 004.7; 004.056/057

[1]**В.В. Казимир**, д.т.н., проф.
[2]**Є.В. Риндич**, асп.
[3]**Я.Я. Кенійз**, магістр

МОДУЛЬ КОМУТАЦІЇ КРИПТОКЛЮЧІВ ДЛЯ ЗАХИЩЕНОЇ СИСТЕМИ IP-ТЕЛЕФОНІЇ

[1,2]Інститут проблем математичних машин та систем НАН України
[1]E-mail: vvkazymyr@gmail.com
[2]E-mail: zkaster@rambler.ru
[3]Національний авіаційний університет
[3]E-mail: slavik_ks@mail.ru

Описано програмний модуль комутації криптоключів для захищеної системи IP-телефонії. В основу запропонованої реалізації покладено комплекс стандартних протоколів та методів криптування, які забезпечують користувачів захищеним від прослуховування даних каналом зв'язку, зокрема під час проведення конференцій.

захист інформації, IP-телефонія, криптографія, модуль комутації криптоключів

Вступ

Інформація − це документовані або публічно оголошені відомості про події та явища, що відбувалися або відбуваються у суспільстві, державі та навколишньому середовищі. Те, що інформація має цінність, люди усвідомили дуже давно, – недаремно листування всього світу завжди було об'єктом пильної уваги.

Сучасне суспільство дедалі більше стає інформаційним, а успіх будь-якого виду діяльності надто залежить від володіння певними відомостями та інформацією, а також від їх відсутності в конкурентів. І чим сильніше виявляється вказаний ефект, тим більшими є потенційні збитки від зловживань в інформаційній сфері, і тим більша потреба в захисті інформації.

Один з перспективних видів зв'язку за допомогою локальних та глобальних мереж є IP-телефонія. Вона дозволяє скоротити витрати на міжміські та міжнародні переговори, що є одним з найбільш поширених варіантів її використання. Вартість голосового зв'язку через IP-мережу виходить дешевшою завдяки тому, що в IP-телефонії використовують поширені протоколи комутації пакетів, на відміну від значно дорожчих мереж з комутацією каналів, які застосовуються в традиційній телефонії.

Крім того, завдяки використанню голосових кодеків досягається істотне стискування мовної інформації. Так, для передачі голосового потоку в системах цифрової телефонії потрібен канал 64 кбіт/с (ISDN мережі), а в системах IP-телефонії, з використанням найбільш популярних натепер кодеків (G.711, G.723, G.729, G.729a) потрібна набагато менша пропускна здатність (6−13 кбіт/с) [1].

Тож переваги IP-мереж дозволяють їм стати базовою транспортною інфраструктурою, що дозволяє задовольнити вимоги кінцевих користувачів як до набору надаваних телекомунікаційних послуг, так і до їх вартості, гнучкості, розширюваності і надійності [2].

Аналіз досліджень і публікацій

Виникнення індустрії обробки інформації зумовило виникнення індустрії засобів захисту інформації. Серед всього спектра методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. На відміну від інших методів вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв особливостей вузлів її обробки, передачі і зберігання. Криптографічні методи створюють бар'єр між інформацією, що захищається, і реальним або потенційним зловмисником із самої інформації [3].

Проведені дослідження рівня захисту інформації в існуючих системах IP-телефонії [4] показали, що наявні системи IP-телефонії реалізують недостатньо високий рівень захисту інформації та використовують відносно нестійкі криптографічні алгоритми, або алгоритми, надійність і якість яких не доведено. А використання асиметричних криптографічних схем для генерації ключів збільшує рівень інформаційної небезпеки.

Постановка завдання

Актуальним питанням є розроблення саме модуля комутації ключів, який працює за принципами, відмінними від відомих систем. При цьому ключі, які використовуються в криптографічних перетвореннях не повинні передаватися по тій самій мережі, що й дані. За допомогою такої передачі виключається можливість викрадення ключів або несанкціонованих змін даних і програм, при цьому стійкість системи визначається винятково криптографічними якостями алгоритмів криптографічних перетворень, які використовуються. Як відомо для несанкціонованого доступу до даних, зашифрованих сучасними симетричними алгоритмами криптографічного перетворення, зловмисник повинен мати значні обчислювальні ресурси і високу кваліфікацію як криптоаналітик. Використання сеансових ключів дозволяє звести спроби криптоаналізу майже до нуля. Прикладом стійкого алгоритму є стандарт, який забезпечує високу криптографічну стійкість, і більшість з відомих атак не є для нього небезпечними [5].

Архітектура захищеної системи IP-телефонії

Криптографічний захист інформації – це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних для приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Якщо користувач суворо дотримується норм секретності (зберігання секретних ключів) і тим самим запобігає викраденню ключів або несанкціонованим змінам даних і програм, то стійкість системи визначається винятково криптографічними якостями.

Для того щоб клієнт міг передати голосовий сигнал за допомогою IP-мережі, ця інформація має бути:

− оброблена аналого-цифровим перетворювачем;

− стиснута за допомогою кодексів;

− оброблена одним зі стійких та швидких алгоритмів криптографічного перетворення;

− поміщена в мережевий пакет та відправлена за допомогою транспорту мережі.

Аналого-цифровий перетворювач (analog-to-digital converter) − пристрій, що перетворює вхідний аналоговий сигнал в дискретний код (цифровий сигнал). Обернене перетворення здійснюється за допомогою (цифроаналогового перетворювача. Цифроаналогове перетворення необхідне для відновлення голосового сигналу.

Для стискання голосового потоку використовуються кодеки. Це набір стандартів з кодування−декодування звуку, які на рівні приладів реалізує шлюз в IP-телефонії. Наприклад, рекомендація G.711 описує кодек, що використовує перетворення аналогового сигналу з точністю 8 біт, тактовою частотою 8 кГц і простою компресією амплітуди сигналу. Швидкість потоку даних на виході перетворювача становить 64 кбіт/с (8 біт×8 кГц). Для зниження шуму квантування і поліпшення перетворення сигналів з невеликою амплітудою при кодуванні використовується нелінійне квантування за рівнем згідно зі спеціальним псевдологарифмічним законом. Кодек G.728 використовує оригінальну технологію з малою затримкою LD-CELP (low delay code excited linear prediction) і гарантує оцінювання MOS (Mean Opinion Score), аналогічне G.726 за швидкості передавання 16 кбіт/с. Цей кодек призначено для використання, переважно в системах відеоконференцій. У пристроях IP-телефонії цей кодек застосовують досить рідко. Якість голосу в IP-телефонії оцінюється за п'ятибальною шкалою одиницями суб'єктивної оцінки експертами MOS. Оцінки 3,5 бала і вище відповідають стандартній і високій якості, 3,0−3,5 − прийнятній, 2,5−3,0 − якості синтезованого звуку. Для передачі мови з хорошою якістю доцільно орієнтуватися на MOS не нижче 3,5 бала (див. таблицю).

Значення MOS для різних кодеків

Кодек	Швидкість передачі, кбіт/с	MOS
G.711	64	4,3
G.726	16−40	2,0−4,3
G.723	5,3−6,3	3,7−3,8
G.728	16	4,1
G.729	8	4,0
G.729a	8	3,4

У блоці шифрування голосова інформація зашифровується за допомогою алгоритму шифрування, наприклад стандарта. Потім вона упаковується. На іншому кінці мережі для прийняття інформації виконують ті самі дії тільки в зворотному порядку, тобто відбувається дешифрування, а потім декодування.

ГОСТ 28147−89 — вітчизняний стандарт симетричного шифрування, введений в 1990 р. ГОСТ 28147−89 — блоковий шифр з 256-бітовим ключем і 32 циклами перетворення, що оперує 64-бітовими блоками. Основа алгоритму шифру − мережа Фейстеля. Базовим режимом шифрування за ГОСТ 28147−89 є режим простої заміни (визначені також складніші режими гамування, гамування зі зворотним зв'язком і режим імітовставки). Для зашифрування в цьому режимі відкритий текст спочатку розбивається на дві половини. Для генерації підключів вихідний 256-бітовий ключ розбивається на вісім 32-бітових блоків [6]. Розшифрування виконується так само, як і зашифрування, але інвертується порядок підключів.

Перевагами ГОСТ 2814−89 є безперспективність силової атаки (XSL-атаки не враховуються, оскільки їх ефективність дотепер повністю не доведено), ефективність реалізації і відповідно висока швидкодія сучасних комп'ютерів; наявність захисту від нав'язування помилкових даних (вироблення імітовставки).

Система, що пропонується, складається з комп'ютерів клієнтів та сервера, на якому розміщено модуль комутації криптоключів (МКК). Загальну архітектуру захищеної системи IP–телефонії, що пропонується, показано на рис. 1.

У ролі клієнта можна використовувати, як персональний комп'ютер, так і спеціальний пристрій – IP-телефон.

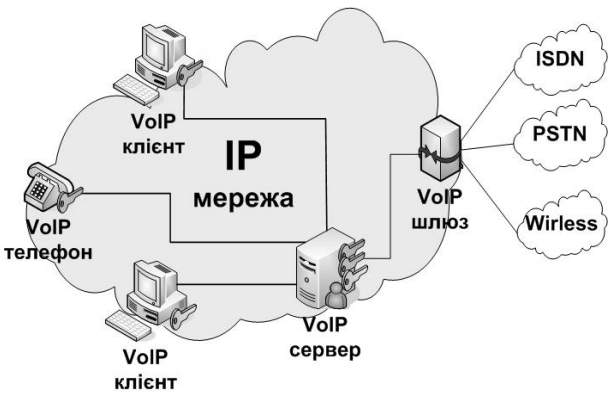

Рис. 1. Архітектура захищеної системи IP-телефонії

Робота модуля комутації криптоключів

Пропонується алгоритм обміну ключами, що використовує асиметрично-симетричну криптосистему, а шифрування пакетів даних виконується за алгоритмом стандарта.

Спочатку сервер згідно з асиметричною схемою криптографічних перетворень випадковим чином вибирає будь-який публічний ключ із заздалегідь побудованої ключової матриці і відсилає його клієнту.

Клієнт за допомогою отриманого публічного ключа зашифровує такі дані (рис.2):

− номер ключа, яким будуть потім зашифровуватись повідомлення за алгоритмом стандарта;

– IP-адреси клієнтів, яким потрібно відіслати пакети голосової інформації.

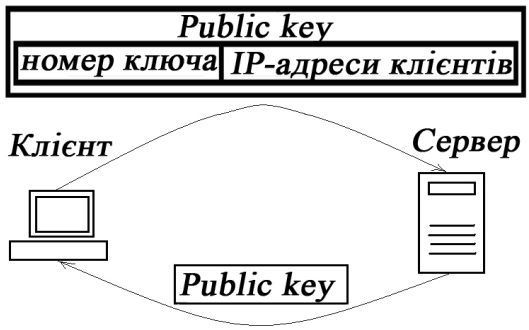

Рис. 2. Асиметричний обмін ключами

Використання асиметричної схеми на цьому етапі гарантує ідентифікацію клієнтів та підвищує рівень захисту від несанкціонованого втручання в роботу системи.

Сервер за допомогою блока МКК, який містить як публічні, так і приватні ключі всіх клієнтів мережі, розшифровує повідомлення, яке надійшло від клієнта за допомогою приватного ключа (рис. 3). Після того як сервер розшифрує повідомлення, яке надійшло від клієнта, він отримує номер ключа, за яким надалі буде зашифровуватися та розшифровуватись голосова інформація вже за симетричною схемою, та адреси абонентів, кому адресована дана інформація. Дані про ключ сесії, за яким буде вестись обмін голосовою інформацією, МКК сповістить клієнтам на іншому боці, передавши їм тільки номер цього ключа.

Обмін повідомленнями між клієнтом та сервером за допомогою МКК показано на рис. 4.

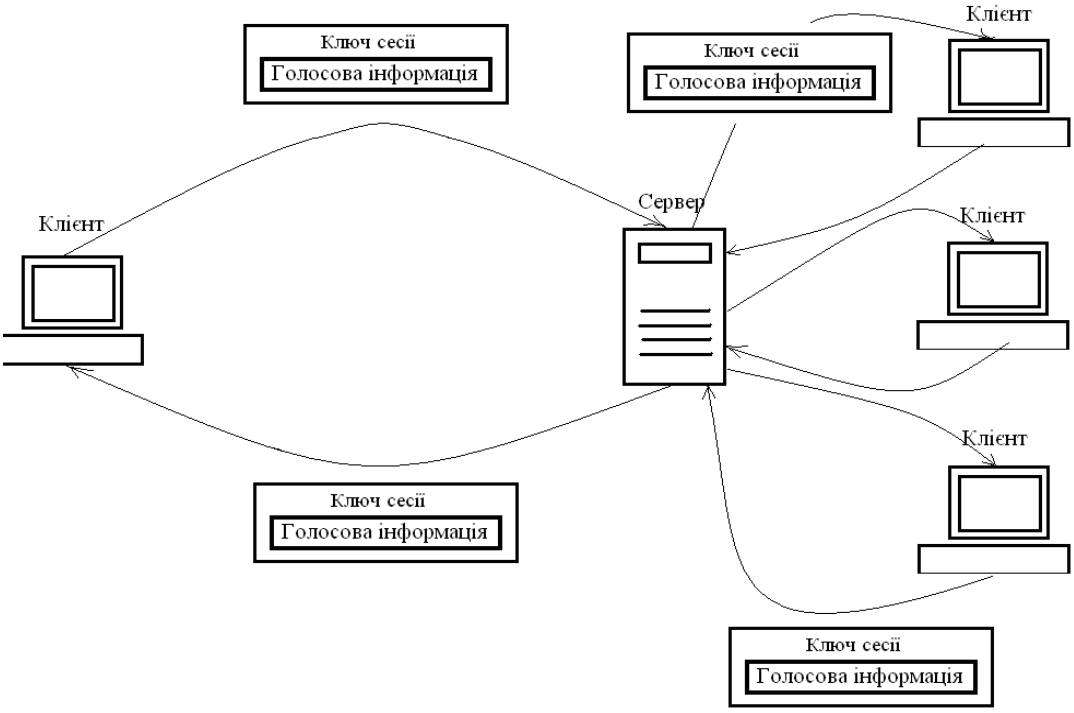

Рис. 3. Обмін інформацію між сервером та клієнтами за симетричною схемою

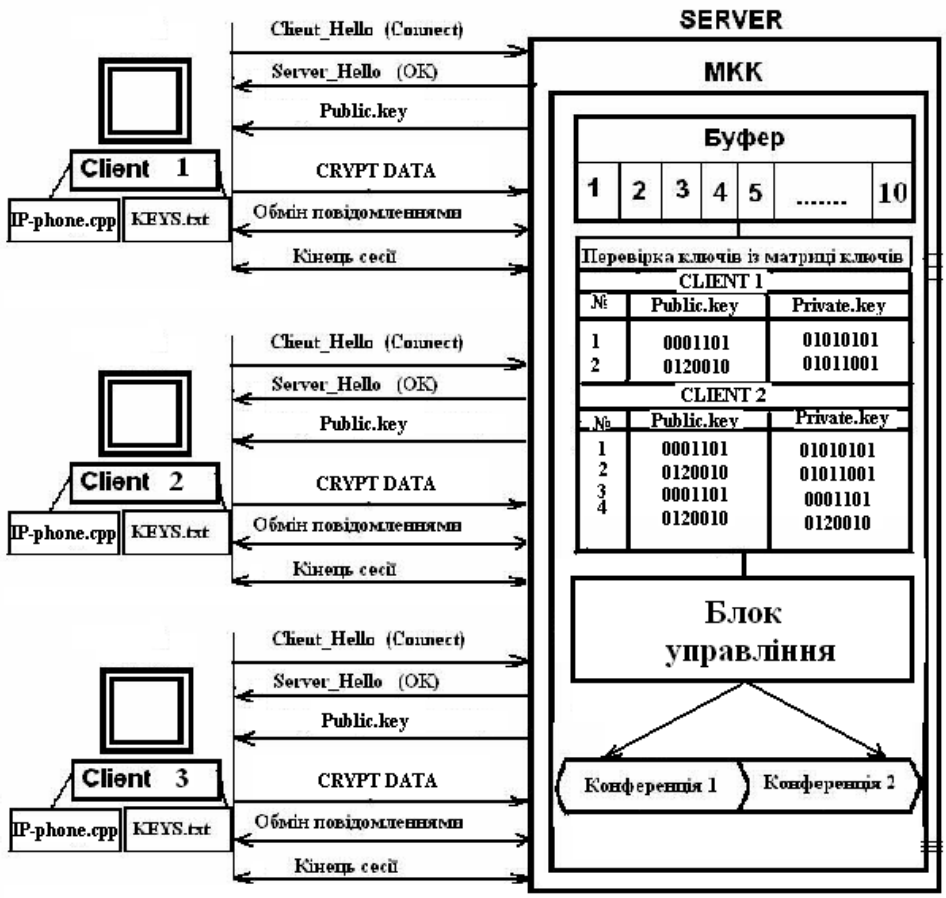

Рис. 4. Послідовність обміну повідомленнями між клієнтом та сервером

Алгоритм взаємодії клієнта та сервера складається з таких кроків.

1. Client відсилає повідомлення Client_Hello.

2. Server розміщує клієнтів по черзі в буфер. Треба враховувати, що дуже малий буфер призводитиме до постійних втрат пакетів, що «запізнилися», а дуже довгий − до неприйнятно тривалої додаткової затримки. Зазвичай передбачається динамічне підстроювання довжини буфера протягом усього часу існування з'єднання. Довжина буфера залежить від завантаженості мережі та обсягу медіатрафіку, який генерують клієнти.

3. Server відсилає відповідь клієнту Server_Hello– відгукується йому.

4. Server відсилає публічний ключ Public.key.

5. Client зашифровує номер ключа та IP-адреси клієнтів конференції отриманим публічним ключем.

6. На сервері в МКК за допомогою приватного ключа розшифровуються та вилучаються дані про IP-адреси клієнтів та призначається номер конференції.

7. За заданими клієнтом IP-адресами МКК зашифровує номер ключа сесії за допомогою публічного ключа та відправляє їх клієнтам, які зможуть розшифрувати ці дані за допомогою приватного ключа.

8. Надалі повідомлення, які містять медіадані, шифруються за алгоритмом ГОСТ 28147-89. Оскільки алгоритм ГОСТ 28147-89 використовує симетричний метод шифрування інформації, то саме тут буде використовуватись ключ, номер якого передав клієнт із самого початку для шифрування та розшифрування голосової інформації . Сервер ці повідомлення вже не розшифровує, а тільки передає їх потрібним клієнтам, які, знаючи номер ключа, можуть розшифровувати їх за тим самим алгоритмом ГОСТ 28147-89.

Для кожного клієнта МКК містить ключі, що зберігаються у ключовій матриці, умовний вигляд якої показано на рис. 5.

Насправді ключі значно довші, ніж показані на рис. 3.

Так, для алгоритму ГОСТ 28147-89 розмір ключа становить 256 біт.

CLIENT 1		
№	Public.key	Private.key
1	0001101	01010101
2	0120010	01011001
CLIENT 2		
№	Public.key	Private.key
1	0001101	01010101
2	0120010	01011001
3	0001101	0001101
4	0120010	0120010

Рис. 5. Умовне зображення матриці ключів

Щоб відповісти, клієнт використовує аналогічні дії, які були описані для клієнта, який відправляє пакети даних на сервер, але тепер його будуть чути й інші клієнти конференції. Після того як клієнт отримав повідомлення від клієнта, який передав повідомлення, він розшифровує повідомлення за допомогою ключа за алгоритмом ГОСТ 28147-89 та виконує обернені операції з вилучення звуку з пакетів інформації. Таким чином, відбувається захищена конференція.

Якщо користувач хоче створити конференцію, для цього йому потрібно встановити зв'язок із сервером. На сервері МКК поміщує клієнта в буфер, перевіряє ключі та через блок керування призначає номер конференції. Тільки користувачі однієї конференції чують один одного.

Висновки

Запропоновано архітектуру комп’ютерної системи зв’язку з використанням сервера, обладнаного модулем комутації криптоключів, який забезпечує проведення захищених голосових переговорів як в режимі «точка-точка», так і під час організації конференцій. Застосування комбінованої асиметрично-симетричної схеми побудови криптосистеми значно підвищує надійність захищеного зв’язку. Насамперед це пов’язано з тим, що секретні ключі не передаються, але за їх допомогою створюється шифрований канал. Запропонована архітектура виключає можливість несанкціонованого втручання в спілкування. Отже, модуль комутації криптоключів дає змогу забезпечити шифрований надійний канал обміну голосовою інформацією засобами IP-телефонії.

Література

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение/ Бернард Скляр. − 2-е изд. / пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

2. *Гольдштейн Б.С.* IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. – М.: Радио и связь, 2001 – 336 с.

3. *Коблиц Н.* Курс теории чисел и криптографии / Н Коблиц. − М.: ТВП, 2001. – 270 с.

4. *Литвинов В.В.* Сучасний стан захисту інформації в IP-телефонії / В.В. Литвинов, В.В. Казимир, Є.В. Риндич // Математичні машини і системи. – 2009. – №2. – С. 76−84.

5. *Баричев С.Г.* Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. − М.: Горячая линия – Телеком, 2001. – 144 с.

6. *Сравнение* стандарта шифрования РФ и нового стандарта шифрования США. [Електронный ресурс] / А. Винокуров , Э. Применко. –Електронный ресурс: http://www.enlight.ru/crypto/index.htm

Стаття надійшла до редакції 12.11.09.

[1]**В.В. Казимир,** [2]**Е.В. Рындич,** [3]**Я.Я. Кенийз**

МОДУЛЬ КОММУТАЦИИ КРИПТОКЛЮЧЕЙ ДЛЯ ЗАЩИЩЕННОЙ СИСТЕМЫ IP-ТЕЛЕФОНИИ

[1,2]Институт проблем математических машин и систем НАН Украины
[3]Национальный авиационный университет

защита информации, криптография, IP-телефония, модуль коммутации криптоключом

Описан программный модуль коммутации криптоключей для защищенной системы IP-телефонии. За основу предложенной реализации взят комплекс стандартных протоколов и методов криптографических преобразований, который обеспечивают пользователей защищенным от прослушивания данных каналом связи, в том числе при проведении конференций.

[1]**Volodymyr V. Kazymyr,** [2]**Yevhen V. Ryndych,** [3]**Yaroslav Y. Kenyz**

CRYPTOKEY COMMUTATION MODULE FOR SECURED IP-TELEPHONY SYSTEM

[1,2]Institute of the Problems of the Mathematical Machines and Systems of the National Academy of Sciences of Ukraine
[3]National Aviation University

cryptography, cryptokey switch module, information security, IP – telephony

In the article described programmatic cryptokey switch module for the protected IP – telephony system. Analyzed IP-telephony system's architecture and determinated the modules place in it. Algorithm of cryptokey switching based on using asymmetric cryptographic transformations for client's authorization and definition of a secret key for transferring of voice data. Such module's structure provides secured data transferring channel for users including conferencing.