УДК 004.7; 004.056/057

В.В. ЛИТВИНОВ, В.В. КАЗИМИР, Є.В. РИНДИЧ

СУЧАСНИЙ СТАН ЗАХИСТУ ІНФОРМАЦІЇ В IP-ТЕЛЕФОНІЇ

Abstract: *The information security analysis of modern IP-telephony systems was presented. Cryptosystem building schemes, common connection types of subscribers and most widespread cryptoalgorithms and VoIP protocols were analysed. Based on prepared analysis requirements to the complex protected VOIP-protocol were formulated.*
Key words: *IP-telephony, information security, cryptosystem, cryptoalgorithm, VoIP-protocol.*

Анотація: *Представлено аналіз стану захисту інформації в сучасних системах IP-телефонії. Проаналізовано основні схеми побудови криптосистем, види з'єднання абонентів, найпоширеніші алгоритми шифрування та протоколи VoIP. Виходячи з проведеного аналізу, сформульовано вимоги до комплексного захищеного VoIP- протоколу.*
Ключові слова: *IP-телефонія, захист інформації, криптосистема, алгоритм шифрування, VoIP-протокол.*

Аннотация: *Представлен анализ состояния защиты информации в современных системах IP-телефонии. Проанализированы основные схемы построения криптосистем, виды соединения абонентов, наиболее распространенные алгоритмы шифрования и протоколы VoIP. Исходя из проведенного анализа, сформулированы требования к комплексному защищенному VoIP- протоколу.*
Ключевые слова: *IP-телефония, защита информации, криптосистема, алгоритм шифрования, VoIP-протокол.*

1. Вступ

IP-телефонія є одним із приоритетних напрямків розвитку телефонного зв'язку. З кожним роком кількість абонентів, які використовують IP-телефонію (VoIP – Voice Internet Protocal) для проведення голосових переговорів, збільшується. Це пов'язано, насамперед, з меншою вартістю передачі даних за допомогою мережі Інтернет. Вже не тільки окремі користувачі, але й цілі підприємства намагаються використовувати Інтернет як основний засіб міжміського зв'язку. Оскільки комерційна інформація звичайно є конфіденційною, питання безпеки такого зв'язку є все більш актуальним.

Людством накопичено достатньо великий досвід щодо забезпечення таємності телефонних переговорів. Але IP-телефонія має ряд значних відмінностей від телефонної мережі загального користування, які роблять її особливо вразливою до зовнішнього втручання і утруднюють застосування існуючих підходів до захисту голосової інформації в мережі Інтернет.

На відміну від класичної телефонії, де використовується комутація каналів, IP-телефонія базується на мережевих протоколах з комутацією пакетів [1]. У процесі передачі даних по IP-мережі вони проходять через певну кількість недостатньо захищених серверів, до того ж з'єднаних між собою незахищеними каналами. Одночасно IP-телефонія певним чином відрізняється і від звичайної передачі даних IP-мережами. Це пов'язано з необхідністю виконання аналого-цифрових перетворень даних в реальному часі [2, 3]. Зважаючи на необхідність дотримання вимог щодо якості зв'язку, такі перетворення, включаючи стискання, шифрування та інш., повинні відбуватися за мінімально короткий час. Від того, наскільки існуючі системи відповідають усім цим вимогам, залежать, значною мірою, перспективи подальшого розвитку IP-телефонії.

Метою даної статті є детальне дослідження рівня захисту інформації в існуючих системах IP-телефонії, а саме аналіз структури протоколів передачі даних, що в них застосовуються, на предмет встановлення їх відповідності потребам збереження конфіденційності телефонних переговорів та формування вимог щодо комплексного захищеного протоколу обміну голосовими повідомленнями абонентів високої стійкості.

2. Існуючі підходи до захисту інформації в IP – телефонії

Захист інформації полягає в підтримці інформаційної безпеки, тобто стану захищеності інформаційного середовища, яке досягається шляхом дотримання конфіденційності, цілісності та доступності інформації [4]. Згідно з [5], дотримання вказаних вимог у випадку IP-телефонії можливо лише при умові використання криптографічних перетворень інформації, тобто шифрування.

2.1. Схеми побудови криптосистем

Конфіденційність зв'язку забезпечується шляхом реалізації криптосистем, які відрізняються схемами розповсюдження ключів. Звичайно розрізняють симетричні та асиметричні криптосистеми.

Асиметрична криптосистема, схема якої приведена на рис. 1, враховує те, що кожний користувач генерує два ключі, зв'язані деяким співвідношенням. Один ключ функціонує відкрито, інший є таємним. Повідомлення шифрується відкритим ключем, який розповсюджується всім адресатам, а процес дешифрування здійснюється за допомогою таємного ключа, який зберігається лише у його власника. Даний тип систем використовують як самостійний засіб захисту, так і при розподілі ключів, а також як засіб аутентифікації – можливості встановлення автора інформації. Тобто, асиметрична криптографія дозволяє не тільки зашифрувати інформацію, але й підтвердити, що повідомлення передане власником конкретного ключа і ніким іншим.

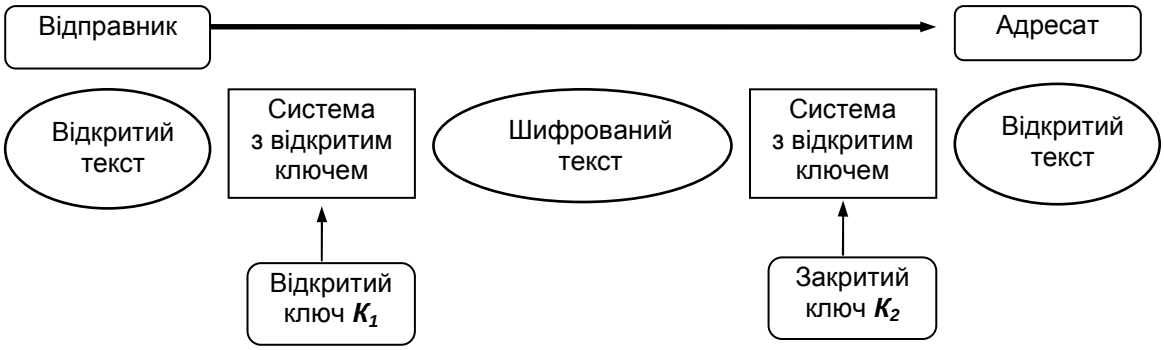

Рис. 1. Схема асиметричної криптосистеми

В асиметричних криптографічних системах надійність захисту інформації забезпечується не таємністю алгоритмів, а насамперед математичними фактами [6, 7].

Криптосистеми з відкритим ключем досить трудомісткі і при шифруванні мультимедіа даних не можуть використовуватися – швидкість роботи таких алгоритмів значно менша, ніж симетричних криптосистем [8].

Симетрична криптосистема, схема якої приведена на рис. 2, базується на процесі шифрування та дешифрування за допомогою одного секретного ключа, відомого обом сторонам. У цьому випадку надійність базується на секретності ключа.

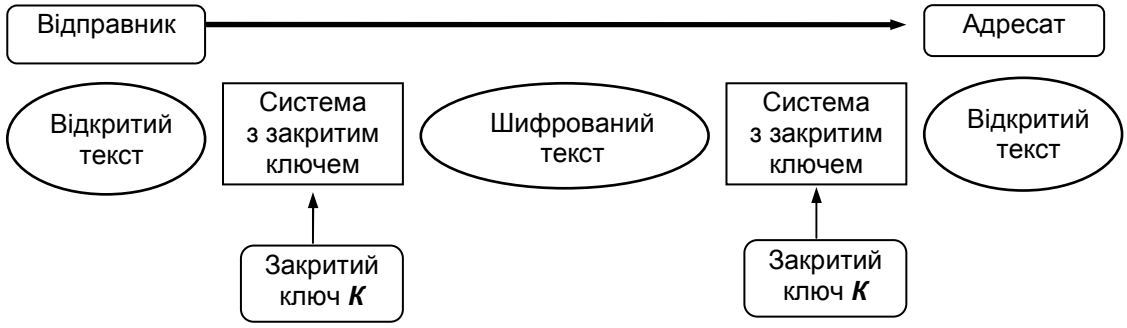

Рис. 2. Схема симетричної криптосистеми

Існує пропозиція У. Діффі та М. Хелмана ідентифікації користувачів за допомогою створення цифрового підпису на базі симетричних криптосистем, яка не поширилася в сучасних комп'ютерних системах та мережах [8, 9].

2.2. Протоколи захисту інформації в IP – телефонії

Захист інформації в IP-телефонії базується на використанні спеціальних протоколів захисту інформації (TLS – Transport Layer Security, VPN – Virual Private Network) або додаткових протоколів в межах існуючих протоколів IP – телефонії (SIP – Session Initiation Protocol, специфікація H.323, Skype).

2.2.1. Спеціальні протоколи

Протокол захисту інформації TLS є наступним поколінням поширеного криптографічного протоколу SSL (Secure Sockets Layer), який базується на асиметричній криптографії. Прикладом використання SSL є протокол HTTPS (Hypertext Transfer Protocol Secured),

Протокол захисту інформації TLS включає в себе три фази [6]:

1) діалог між двома сторонами для вибору алгоритму шифрування;

2) обмін ключами за допомогою криптосистем з відкритим ключем або аутентифікація за допомогою сертифікатів;

3) передача даних, які шифруються за допомогою симетричних алгоритмів шифрування.

Для обміну ключами використовують комбінації алгоритмів RSA (алгоритм розроблений в 80-х роках Р. Райвестом, А. Шаміром та Л. Адлеманом), алгоритм Діффі-Хелмана та DSA (Digital Signature Algorithm). Для симетричного шифрування використовують алгоритми RC2 (Ron's Code 2), RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standart), Triple DES або AES (Advanced Encryption Standard). Як відомо [9, 10], ці алгоритми мають свої вразливі місця, які дозволяють застосувати лінійний та диференційний методи криптоаналізу для зменшення кількості операцій порівняно з повним пошуком.

Використання VPN дозволяє створити тунель між ініціатором та термінатором. Ініціатор тунелю інкапсулює мережеві пакети в новий пакет. Конфіденційність та цілісність даних досягається за допомогою не тільки шифрування початкових даних, але й усього IP-пакета. Протокол VPN реалізується не тільки програмно, але й апаратно в маршрутизаторах. Робота VPN пов'язана з використанням відкритих ключів [11].

VPN з'єднання має ряд обмежень, до яких відносяться:

1) взаємодія програмного забезпечення (ПЗ) VPN та брандмауерів може значно погіршити продуктивність системи загалом, оскільки шифрується цілком IP-пакет;

2) VPN на базі маршрутизатора може негативно вплинути на інший трафік, який отримано від систем, які не використовують VPN-з'єднання;

3) для адміністрування ПЗ на базі VPN необхідні додаткові ресурси: засоби адміністрування, каталоги та інше;

4) складність в реалізації мобільності терміналів та безпосередньо абонентів при використанні стаціонарних терміналів;

5) проблеми використання при організації конференцій у зв'язку з виникненням часових затримок, які можуть досягати 300 мс.

2.2.2. Додаткові протоколи

Всі додаткові протоколи захисту інформації в IP-телефонії можна поділити на два види: відкриті, до яких можна віднести відомі міжнародні специфікації та стандарти, та закриті – протоколи з закритими стандартами. Так, закритим протоколом можна вважати будь-який протокол IP-телефонії, інформація щодо структури повідомлень якого є закритою.

2.2.2.1. Відкриті протоколи

Серед відкритих протоколів слід виділити такі:

• родину протоколів SIP (Session Initiation Protocol), розроблених IETF (The Internet Engineering Task Force);

• специфікацію протоколів H.323, розроблену ITU (International Telecommunication Union) для IP-телефонії .

SIP-протокол RFC (Request for Comments*)* 3261 [12] розроблено на основі протоколу HTTP. Він належить до сьомого рівня моделі OSI. Протокол SIP розроблено спеціально для використання в IP-мережах. Для з'єднання IP-мережі з мережею стільникового зв'язку існує модифікація протоколу SIP – протокол SIP-T, який визначає пряме та зворотне перетворення повідомлень SIP і ТМзК (телефонних мереж загального користування). В даному протоколі передбачена аутентифікація користувачів.

Безпосередньо для захисту інформації на базі протоколу SIP розроблено протокол SIPS (Session Initiation Protocol Secured), який поєднує в собі аутентифікацію та збереження конфіденційності зв'язку за допомогою протоколу TLS. Він може використовуватися лише в TCP-з'єднанні. При цьому виникає необхідність створення сесії та обміну ключами на кожній ділянці мережі, тобто між кожною парою серверів або SIP-шлюзів. При використанні протоколу SIPS у глобальній мережі часові затрати на шифрування стають головною складовою затримки в передачі голосових даних. Протокол SIPS поширюється лише на IP-мережу і не підтримує з'єднання з ТМзК.

Захист інформації в родині протоколів SIP реалізовано за допомогою п'яти механізмів [13]:

1. Аутентифікація за допомогою дайджеста повідомлення RFC 2617. Використовується алгоритм MD5 для отримання хеш-значення від імені, паролю та URL. Для конфіденційності медіа

даних використовують протокол SRTP (Secure Real-time Transport Protocol), а для обміну ключами використовують протокол SDP (Session Description Protocol) RFC 2327.

2. Забезпечення криптографічної безпеки електронної пошти на основі стандарту S/MIME (Secure/Multipurpose Internet Mail Extensions).

3. Використання протоколу TLS як для аутентифікації, так і для шифрування даних.

4. Використання протоколу IPSec (протокол для забезпечення захисту даних, що передаються по міжмережевому IP-протоколу); це дозволяє здійснювати підтвердження достовірності і шифрування IP-пакетів та розподілення ключів за допомогою протоколу IKE (Internet Key Exchange).

5. Використання протоколу IPSec та ручне розподілення ключів.

Використовуються протоколи SIP в мережі PSipTN (мережа IP-телефонії, що побудована на базі протоколу SIP) декількома операторами IP-телефонії, в тому числі TelTel, а також у глобальній мережі Internet у вигляді різноманітних софтфонів – програмного забезпечення персональних комп'ютерів. Крім того, ці протоколи підтримуються великою кількістю обладнання для створення корпоративних мереж IP-телефонії, наприклад, Avaya та Nokia.

Специфікація протоколів H.323 орієнтована на інтеграцію з ТМзК і на відміну від SIP складається з великої кількості інших протоколів. На рис. 3 зображено структуру H.323.

<table>
<tr><td colspan="2">Гарантована доставка інформації за протоколом TCP</td><td colspan="3">Негарантована доставка інформації за протоколом UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.225</td><td colspan="2">Потоки мови та відеоінформації</td></tr>
<tr><td>Управління з'єднанням(Q.931)</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="2">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Канальний рівень</td></tr>
<tr><td colspan="5">Фізичний рівень</td></tr>
</table>

Рис. 3. Структура протоколу H.323

Для захисту інформації в специфікації H.323 використовують протокол H.235, в якому передбачена аутентифікація за допомогою сертифікатів або сигнальних повідомлень.

Існує 9 рекомендацій інформаційної безпеки протоколу H.235, згідно з якими можна використовувати базові засоби протоколу H.235 або інші протоколи. В залежності від обраної рекомендації H.235 дозволяє проводити аутентифікацію, захист частини службових даних (H.225) чи медіа даних (RTP).

Аутентифікація в специфікації H.323 базується на алгоритмах HMAC-SHA1-96, цифрових сертифікатах, створених за допомогою алгоритмів SHA1 та MD5. Конфіденційність медіа трафіка забезпечується завдяки симетричним алгоритмам шифрування DES, 3DES та AES [14].

У той же час використання H.235 має ряд обмежень:

• складність у реалізації для глобальних мереж та недосить широке поширення в обладнанні;

• не всі шлюзи підтримують цей протокол, оскільки використання його рекомендацій не обов'язкове [15].

На рис. 4 та рис. 5 наведено дві рекомендації протоколу H.235, а саме профайли D та E.

Тип захисту інформації	RAS	H.225		H.245	RTP
Аутентифікація	HMAC-SHA1-96	HMAC-SHA1-96		HMAC-SHA1-96	
Цілісність	HMAC-SHA1-96	HMAC-SHA1-96		HMAC-SHA1-96	
Конфіденційність					DES/3DES
Розподілення ключів	Призначений пароль	Призначений пароль	Генерація та обмін за схемою Діффі-Хелмана	Вбудовані в H.235 сесійні ключи	

Рис. 4. Можливості захисту інформації в специфікації H.323 – профайл D

Тип захисту інформації	RAS	H.225	H.245	RTP
Аутентифікація	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	
Цілісність	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	
Конфіденційність				
Розподілення ключів	Призначений сертифікат	Призначений сертифікат		

Рис. 5. Можливості захисту інформації в специфікації H.323 – профайл E

Для захисту інформації в специфікації H.323 також використовують протокол IPSec в рамках VPN-з'єднання. При цьому шифруються всі дані, але тунель (захищене з'єднання між клієнтом та сервером) створюється тільки між двома кінцевими користувачами або серверами [16, 17].

H.323, як і SIP, використовують у глобальній мережі Internet у вигляді різноманітних софтфонів (наприклад, програмний комплекс Yate [18]) та в великій кількості обладнання Cisco, і не тільки для створення корпоративних мереж IP-телефонії.

2.2.2.2. Закриті протоколи

До закритих протоколів можна насамперед віднести протокол Skype, оскільки він є найпоширенішим представником цього виду протоколів (мережа IP-телефонії Skype вже налічує більше мільярда користувачів).

Протокол Skype не відомий широкій громадськості, тобто точно не відомо, за яким алгоритмом іде вибір портів для встановлення сесій і який формат мають службові та інформаційні

повідомлення, що, у свою чергу, вважається негативним фактором щодо безпеки інформації. Але аналіз повідомлень протоколу Skype, проведений у [19, 20], показав, що Skype використовує TCP та UDP-протоколи для установлення сесій.

Недоліком протоколу Skype є необхідність підключення користувачів до мережі Internet для проведення аутентифікації (дані також передаються за допомогою мережі Інтернет, навіть, якщо комп'ютери абонентів знаходяться в одній локальній мережі). Це пов'язано зі схемою системи Skype, коли вузли з більшою пропускною здатністю стають «мостами» (supernode), тобто виконують функцію маршрутизації передачі даних інших користувачів цього програмного засобу. Провівши реверс-інжинірінг клієнтського програмного забезпечення, можливо створити вузол, який зможе за допомогою модифікованого супер-вузла виконувати, крім стандартних, ще й додаткові функції [21]:

• перенаправляти запити користувачів на підконтрольний сервер та блокувати деяким користувачам доступ до системи (атака на відмову в обслуговуванні);

• перехоплювати логіни та паролі користувачів;

• записати всю розмову або деяку її частину.

Крім того, може бути застосована атака «людина посередині», коли для користувача А супер-вузол видає себе за користувача Б, а для користувача Б – за користувача А, підставляючи свої ключі (рис. 6).

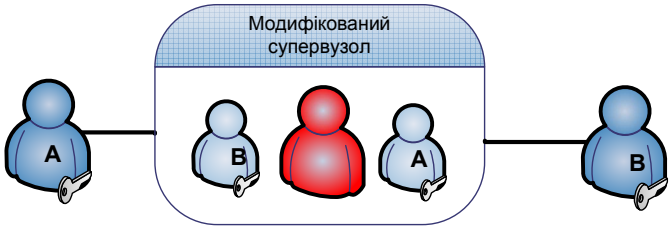

Рис. 6. Атака «людина посередині»

Що стосується безпосередньо захисту інформації, в Skype використовуються RSA-ключі та шифрування, подібне AES, але офіційних даних щодо алгоритмів шифрування розробник не надає. Відомо тільки, що захист інформації відбувається лише до з'єднання з ТМзК [21].

Таким чином, розподілена структура мережі Skype вносить досить суттєвий ризик в безпеку переговорів і є одним із дуже впливових факторів, чому Skype не може використовуватися як захищений зв'язок, незважаючи навіть на використання сучасних криптографічних алгоритмів [17, 18]. Аналогічні випадки відомі в історії розробки програмного забезпечення з закритим кодом, коли програмне забезпечення мало велику кількість прогалин у системі безпеки [22].

3. Висновки

Розглянувши основні схеми побудови криптосистем, види алгоритмів, специфікації та протоколи IP-телефонії, можна зробити висновок, що існуючі системи IP-телефонії реалізують недостатньо високий рівень захисту інформації та використовують відносно нестійкі криптографічні алгоритми або алгоритми, надійність і якість яких не доведена [10]. Використання асиметричних криптографічних схем для генерації ключів збільшує рівень інформаційної небезпеки. Для аутентифікації та хеш-функцій, які використовуються при цьому, слід використовувати більш стійкі

алгоритми, наприклад, ГОСТ Р 34.10-2001 та ГОСТ 34.11-94, або систему аутентифікації, побудовану на стійких симетричних алгоритмах шифрування, наприклад, ГОСТ 28147-89 [23].

Важливим питанням залишається розповсюдження ключів. Але на даному етапі, при відсутності нормативно закріпленої структури обміну відкритих ключів, найліпший рівень конфіденційності можливий при умові безпечного постачання ключів обом сторонам при використанні симетричного алгоритму шифрування [24].

Таким чином, захист інформації в VoIP потребує проведення подальших досліджень, у тому числі удосконалення вже існуючих систем шляхом використання додаткових засобів захисту, які б дозволили підвищити надійність існуючих методів шифрування, або розроблення нових методів та схем захисту з урахуванням потреб сьогодення. Враховуючи вже накопичений досвід, це може бути досягнуто, наприклад, шляхом розробки комплексного захищеного VoIP-протоколу, який би мав такі властивості:

1) використовувався не тільки в комп'ютерних мережах, але й у мережах GSM-операторів, щоб захистити весь шлях розповсюдження інформації;

2) базувався на клієнт-серверній архітектурі (особливо це важливо в разі організації голосових конференцій;

3) використовував тільки високонадійні алгоритми шифрування інформації;

4) забезпечував узгоджене функціонування засобів шифрування та вокодера для зменшення затримок у часі при передачі даних.

Слід зазначити, що створення комплексного протоколу IP-телефонії, який би підтримував також стільниковий зв'язок, вимагає проведення додаткового дослідження, оскільки мобільні телефони не підтримують передачу даних у форматах, які використовуються в IP-мережах.

СПИСОК ЛІТЕРАТУРИ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом «Вильямс», 2003. – 1104 с.
2. Гольдштейн Б.С. и др. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. – М.: Радио и связь, 2001 – 336 с.
3. Бабкин В.В. и др. Оптимизационная задача выбора речевого и канального кодирования / В.В. Бабкин, А.А. Ланнэ, В.С. Шаптала // Труды 7-ой международной конференции и выставки ЦОС и ее применения DSPA. – 2005. – С. 28 – 32.
4. Информационная безопасность – Википедия // Википедия – свободная библиотека [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Информационная_безопасность.
5. White paper. VoIP security and Privacy. Making PC Platforms and Networks Higly Secure.Printed in USA/1105/PMS/LKY/PP/150 Intel, 2006 – 8 p.
6. TLS – Википедия // Википедия – свободная библиотека [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/TLS.
7. Ботюк А.О. и др. Переваги асиметричної криптографії / А.О. Ботюк, М.П. Карпінський, Я.І. Кінах // Збірник доповідей Другої наук.-техн. конф. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – Київ: НТУУ "КПІ", 2000. – С. 242 – 244.
8. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001 – 270 с.
9. Баричев С.Г. и др. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2001. – 144 с.
10. Сравнение стандарта шифрования РФ и нового стандарта шифрования США [Електронний ресурс] / А. Винокуров, Э. Применко. – Режим доступу: http://www.enlight.ru/crypto/index.htm.
11. Росляков А.В. и др. IP-телефония / А.В. Росляков, М.Ю. Самсонова, И.В. Шибаева. – М.: Эко-Трендз, 2003. – 252 с.
12. Network Working Group Request for Comments: 3261 [Електронний ресурс]. – Режим доступу: http://www.ietf.org/rfc/rfc3261.txt.

13. Kuhn Richard D. Security Considerations for Voice Over IP Systems. Recommendations of the national Institute of Standards and Technology / Richard Kuhn D., Walsh Thomas J., Fries Steffen. – NIST Special Publication 800-58, 2005. – 100 p.
14. SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS. Infrastructure of audiovisual services – Systems aspects Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals. ITU-T Recommendation H.235, 2001 – 85 p. [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/T-REC-h.
15. Thermos P., Takanen A. Securing VoIP networks: threats, vulnerabilities, countermeasures. – Addison-Wesley Professional, 2007 – 384 p.
16. Браун С. Виртуальные частные сети VPN. – М.: Лори, 2001. – 504 с.
17. Практические аспекты защиты корпоративных сетей IP-телефонии [Електронний ресурс] / А. Лукацкий. – Режим доступу: http://www.pabx.ru/publications/more.html?id=723.
18. Main Page [Електронний ресурс]. – Режим доступу: http://yate.null.ro/pmwiki/.
19. Безопасность Skype в корпоративной среде [Електронний ресурс] / А. Доля. – Режим доступу: http://www.citcity.ru/security/articles/.
20. Уязвимости Skype [Електронний ресурс]. – Режим доступу: www.pgpru.com.
21. Porter T. Practical VoIP security / Porter Thomas, Jan Kanclirz Jr., Rockland MA.: SyngressPublishing Inc., 2006. – 592 p.
22. Симсон Л. Гарфинкель Передача голоса по IP-протоколу и безопасность программы Skype [Електронний ресурс]. – Режим доступу: http://www.skype.co.ua/content/view/90/16/.
23. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи x9.62-1998 и распределения ключей x9.63-199x на эллиптических кривых [Електронний ресурс] / М.Ф. Бондаренко, И.Д. Горбенко, Е.Г. Качко, А.В. Свинарев, Т.А. Гриненко. – Режим доступу: http://kiev-security.org.ua/box/19/84.shtml/.
24. Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий / М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных и др. // Радиотехника. – 2002. – № 126. – С. 5 – 17.

Стаття надійшла до редакції 14.10.2008