УДК 004.056:061.68

ВИКОРИСТАННЯ IP-ТЕЛЕФОНІЇ В ІНФРАСТРУКТУРІ МЕРЕЖІ ТА ОСОБЛИВОСТІ ЇЇ ЗАХИСТУ ВІД ПОСЯГАНЬ ЗЛОВМИСНИКІВ

Кузьменко І. С., Грицюк Ю. І., д.т.н., професор
Львівський державний університет безпеки життєдіяльності, Львів, Україна

USING IP-TELEPHONY IN NETWORK INFRASTRUCTURE AND PECULIARITIES OF ITS PROTECTION FROM INTRUDERS

Kuzmenko I. S., Grycyuk Yu. I., Doctor of Science (Technics), Professor
Lviv State University of Life Safety, Lviv, Ukraine

Вступ. Можливість передачі голосових повідомлень мережою Інтернет вперше була реалізована в 1993 році. Ця інформаційна технологія отримала назву *VoIP*[5], одним з часткових застосувань якої була *IP*–телефонія — послуга з передачі телефонних розмов абонентів за протоколом *IP* [4]. Отож *IP*-телефонія — це система зв'язку, яка передбачає оцифровування голосу абонента і пересилання отриманих даних окремими пакетами мережею Інтернет (або іншими *IP*–мережами) [6]. Строго кажучи, IP-телефонія є додатком більш загальної технології *VoIP* для організації двостороннього спілкування. На сьогодні технологія *VoIP* передбачає всі варіанти передачі голосу за протоколом *IP*, в т.ч. й варіанти, які не мають ніякого відношення до телефонії та спілкування людей [5]. Наприклад, передача звуку в системах IP відеоспостереження, в системах сповіщення, при трансляції вебінарів, при перегляді фільмів у режимі *on-line* і т.п.

Не дивлячись на чималий вік технології *VoIP*, в т.ч. і *IP*–телефонії зокрема, а також їх широке розповсюдження в корпоративному і державному секторах [3], використання цієї інформаційної технології викликає ряд серйозних застережень, пов'язаних з безпекою інфраструктури мережі [1, 2]: відносно нескладно встановити прослуховування *VoIP*-дзвінків і змінити їх зміст, відносна схильність системи *VoIP* до *DoS*-атак і т.д. Спробуємо коротко розглянути кожне з цих застережень, що і становить основну мету цієї роботи.

***IP*-телефонія — нова інформаційна технологія цифрового зв'язку.** Стосовно організації системи зв'язку [4], то під *IP*–телефонією розумію технологію голосового спілкування та обмін факс-повідомленнями через мережу, що використовує протокол ІшР в режимі реального часу. Цей прото-

[5] *VoIP* (англ. *Voice over IP*; *IP*-телефонія) – система зв'язку, яка забезпечує передачу мовного сигналу мережею Інтернет або будь-якими іншими *IP*-мережами. Сигнал каналом зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискається) для того, щоб видалити надмірність коду.

кол може використовуватися як у мережі Інтернет, так і в локальних мережах будь-яких навчальних закладів, державних і комерційних організаціях, сучасних бізнес-структурах. Багато користувачів мережі Інтернет вважає рівноцінним поняття «Інтернет-телефонії» і «*IP*–телефонії», хоча насправді це не зовсім так. *IP*–телефонія для передачі голосу передбачає використання виділеного каналу зв'язку, тоді як Інтернет-телефонія допускає використання загальних каналів зв'язку мережі Інтернет. Завдяки цьому саме *IP*–телефонії властиві [2]:

- висока якість послуг зв'язку при значній економії засобів передачі даних;
- підвищена безпека і конфіденційність переданої інформації;
- використання в технічних рішеннях різних засобів зв'язку (див. рис.).

Технологія *IP*-телефонії об'єднує мережі з комутацією каналів зв'язку (що передають голосову інформацію) і мережі з комутацією пакетів даних (даних, що передаються) в єдину комунікаційну мережу. Безперебійне розпізнавання голосу і його передача з однієї мережі в іншу вирішується за допомогою різних шлюзів [5]. Шлюз — це пристрій, в якому з одного боку під'єднуються телефонні лінії, а з іншого боку — *IP*–мережа. Голос, як аналогові коливання в системі *IP*–телефонії, існує тільки в телефонній трубці, або в тому пристрої, який перетворює його у цифрову інформацію.

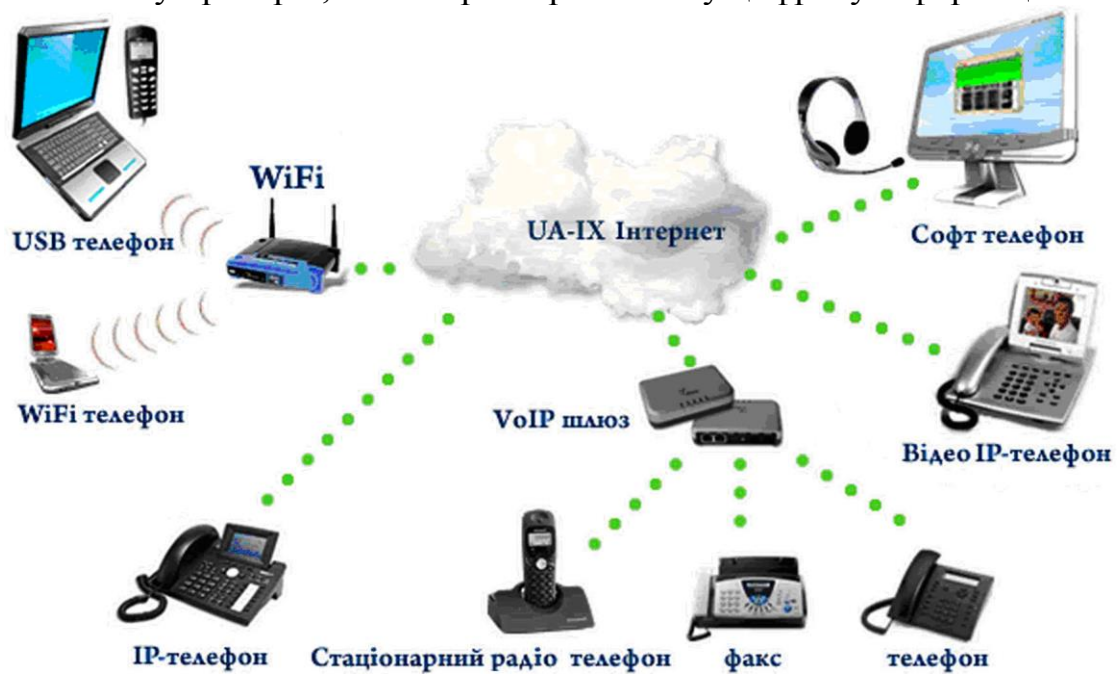

Рис. Схема організації IP-телефонії

На інших ділянках каналу передачі даних від одного абонента до іншого мова оцифровується і передається у вигляді *IP*–пакетів. Пакети мають порядковий номер, адреси точок призначення (прийому і передачі) та інформацію для завадостійкого коректування помилок, які можуть траплятися внаслідок перешкод у каналах зв'язку. Для того, щоб пакети були направлені потрібному адресату, використовується *IP*–адреса, згідно з якою здійснюється їх маршрутизація [5]. Вузли *IP*–телефонії направляють ці па-

кети усією мережею до завершення маршруту прибуття. Оскільки пакети через затримку у каналах зв'язку можуть доставлятися не в тій послідовності, в якій були відправлені, то спочатку відбувається їх накопичення, а потім впорядкування до необхідної послідовності. Для відновлення початкового обсягу впорядкованих даних використовуються порядкові номери пакетів. Для повідомлень, де не важливий порядок і інтервал надходження пакетів даних, таких як *E-mail*, тривалість затримок між окремими пакетами не має вирішального значення.

Таким чином, сучасна *IP*–телефонія — це інформаційна технологія, яка дає змогу використовувати будь-яку *IP*–мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу. Сьогодні вже можна говорити про те, що *IP*–телефонія стала деяким стандартом у телефонних комунікаціях. Це пояснює зручність, надійність та відносно невисоку вартість *IP*–телефонії порівняно з аналоговим зв'язком. Також *IP*–телефонія підвищує ефективність ведення бізнесу і дає змогу здійснювати такі раніше недоступні операції, як інтеграція з різними бізнес-додатками.

Недоліки та вразливості *IP*-телефонії. Сучасна *IP*-телефонія схильна до різних атак, до черв'яків і вірусів, до *DoS*-атак [1], до несанкціонованого віддаленого доступу та ін. Сьогодні велику кількість компаній інтегрують *IP*–телефонію з іншими додатками, наприклад, з електронною поштою. З одного боку — з'являються додаткові зручності, а з іншого боку — і нові вразливості. Окрім цього, для функціонування мережі *IP*–телефонії потрібна велика кількість інфраструктурних компонентів, зокрема сервери підтримки, комутатори, маршрутизатори, міжмережеві екрани, *IP*–телефони і т.д. При цьому для підтримки функціонування *IP*–мережі часто використовуються не спеціалізовані операційні системи. Водночас для універсальної операційної системи або стека протоколів можна використовувати давно відомі засоби захисту — антивіруси, персональні міжмережеві екрани, системи запобігання атакам і т.п. Відсутність досконалості таких засобів для роботи із додатками *IP*–телефонії може негативно позначитися на рівні захищеності інфраструктури мережі.

До основних загроз, яким піддається *IP*–телефонна мережа, належать [2]:

- реєстрація чужого терміналу, що дає змогу робити дзвінки за чужий рахунок;
- підміна абонента, що дає змогу зловмиснику перенаправити дзвінки;
- внесення змін до голосового або сигнального трафіку;
- зниження якості голосового трафіку;
- перенаправлення та перехоплення голосового або сигнального трафіку;
- підроблення голосових повідомлень;
- завершення сеансу зв'язку;
- відмова в обслуговуванні;
- віддалений несанкціонований доступ до інфраструктури *IP*-телефонії;

- несанкціоноване оновлення ПЗ на *IP*–телефоні, наприклад, з метою впровадження троянської або шпигунської програми;
- зламування білінгової системи (для операторської телефонії).

Це далеко не весь перелік можливих проблем, пов'язаних з використанням *IP*–телефонії [4, 5]. Альянс щодо безпеки *VoIP* розробив документ, який детально описує широкий спектр загроз *IP*–телефонії, який, окрім технічних загроз, містить обман користувачів, непроханий спам і т.д. Чим надійніше захищена *IP*–телефонна мережа, тим менша ймовірність зламування та зловживання зловмисників у такій мережі. Думати про забезпечення інформаційної безпеки необхідно вже на етапі підготовки проекту *IP*–телефонії, позаяк саме на цьому етапі потрібно домовитися про те, які механізми захисту інфраструктури доцільніше використовувати у мережі.

Щодо керованості та продуктивності *IP*–телефонії, найбільш доцільною є така її архітектура, де всі компоненти захисту вбудовані в елементи самої мережі. Якщо розглядати *IP*–телефонну мережу без використання додаткових засобів захисту, то, застосовуючи вбудовані мережеві комутатори і захисні механізми, можна домогтися побудови відносно стійкого захисту від атак на периметрі. Вбудований функціонал дає змогу забезпечити [2]:

- можливість створення віртуальних локальних мереж *VLAN* (*Virtual Local Area Network*) з використанням вбудованих можливостей комутаторів;
- використання вбудованих механізмів фільтрації та контролю доступу;
- обмеження та представлення гарантованої пропускної смуги, яка дає змогу ефективно пригнічувати *DoS*–атаки;
- обмеження кількості пристроїв з різними *MAC*–адресами, під'єднаними до одного порту;
- запобігання атакам на витрачання пулу адрес *DHCP*–сервісу;
- запобігання засміченню таблиць *ARP* і «крадіжці» адрес;
- запобігання атакам з анонімних адрес;
- використання списків контролю доступу, що обмежують адреси вузлів, які можуть передавати дані *IP*–телефонам.

Вважається, що вбудована в архітектуру *IP*–мережі система управління викликами, яка може під'єднуватися до спеціально виділеної локальної інформаційної мережі інфраструктури, ізольованої від робочої мережі організації, є додатковим «рубежем» в її захисті [1]. До недоліків належить також те, що вбудовані в мережеве устаткування захисні функції не завжди забезпечують належний рівень безпеки і для його покращення можуть знадобитися додаткові вкладення в модернізацію устаткування.

Використання спеціалізованих міжмережевих екранів значно підвищує безпеку *IP*–телефонної мережі. Наприклад, фільтрація трафіка з врахуванням стану з'єднання (*stateful inspection*) дає змогу пропускати тільки необхідний трафік і з'єднання, встановлені в певному напрямі — від сервера до клієнта або навпаки. Окрім цього, міжмережевий екран дає змогу здійснювати [2]:

- фільтрацію трафіку управління установкою *IP*–телефонних з'єднань;
- передачу трафіку управління через *NAT* і мережеві тунелі;
- *TCP*–перехоплення, яке забезпечує перевірку закриття *TCP*–сесій, що дає змогу захищатися від ряду атак типу відмови в обслуговуванні (*DOS*).

Захист *IP*–телефонії від прослуховування. Локальні внутрішні мережі (ЛВМ) знижують до певної міри ризик прослухування телефонних розмов, проте в разі перехоплення аналізатором мовних пакетів для фахівця не виникає проблеми відновити запис будь-якої розмови [4]. Зловмисник, що знаходиться всередині периметра мережі, може під'єднати комп'ютер прямо до роз'єму настінної розетки, конфігурувати його як елемент віртуальної ЛВМ системи *IP*–телефонії та розпочати атаку.

Найбільш досконалий спосіб протидії подібним маніпуляціям — використання *IP*–телефонів із вбудованими засобами шифрування інформації. Окрім цього, додатковий захист забезпечує шифрування трафіку між телефонами і шлюзами, що є найбільш логічним вирішенням проблеми захисту розмов від прослухування [1]. Якщо така функціональність має деякі труднощі, які необхідно враховувати при побудові захищеної лінії зв'язку. В основному може бути затримка, пов'язана з процесом шифрування та розшифрування трафіку. Варіантом вирішення проблеми можуть слугувати швидші алгоритми або під'єднання механізмів *QOS* у модуль шифрування.

Механізм *QOS* (*Quality of Service – якість обслуговування*). Прийнято вважати, що основне призначення механізмів *QOS* — забезпечення належної якості зв'язку, проте вони мають велике значення і при вирішенні завдань інформаційної безпеки [5]. Для передачі мовних сигналів і даних з логічно окремих віртуальних ЛВМ використовується загальна фізична пропускна смуга. При зараженні вузла вірусом або черв'яком може статися переповнювання мережі трафіком. Проте, якщо вдатися до відповідно налагоджених механізмів *QOS*, трафік *IP*–телефонії буде, як і раніше, мати пріоритет при проходженні через загальні фізичні канали, і *DoS*–атака виявиться безуспішною.

Захист *IP*-телефонії від *DoS*-атак. Атаки типу «відмова в обслуговуванні» на застосування *IP*–телефонії (наприклад, на сервери оброблення дзвінків) і на середовище передачі даних є досить серйозною проблемою [6]. Якщо йдеться про атаки на середовище передачі даних, то за нього у *IP*-телефонії відповідає протокол *RTP* (*Real-Time Protocol*). Він уразливий для будь-якої атаки, яка перевантажує мережу пакетами або призводить до уповільнення процесу їх оброблення кінцевим пристроєм (телефоном або шлюзом). Отже, зловмисникові достатньо «забити» мережу великою кількістю *RTP*–пакетів або пакетами даних з високим пріоритетом обслуговування, які конкуруватимуть з легітивними *RTP*–пакетами. В такому разі для захисту мережі можна використовувати як вбудовані в мережеве

устаткування механізми забезпечення інформаційної безпеки, так і запровадити такі додаткові рішення [2]:

- розділення корпоративної мережі на сегменти передачі голосу і даних, які не перетинаються між собою, що запобігає появі в «голосовій» ділянці поширених атак, у т.ч. і *DOS*–атак;
- спеціальні правила контролю доступу на маршрутизаторах і міжмережевих екранах, які захищають периметр корпоративної мережі та окремі її сегменти;
- систему запобігання атакам на сервері управління дзвінками і комп'ютером з голосовими додатками;
- спеціалізовані системи захисту від *DOS*– і *DDoS*–атак;
- спеціальні налаштування на мережевому устаткуванні, які запобігають підміну адреси і обмежують пропускну смугу, а також не дають змоги вивести з ладу ресурси, що атакуються, великим потоком не потрібного трафіку.

Стандарти в *IP*–телефонії. Сьогодні протокол *SIP* приходить на зміну протоколам H.323 [4], при цьому багато розробників пристроїв, що підтримують *IP*–телефонію, фокусують свої сили на збільшенні кількості функцій, а не на безпеці. Протокол *SIP* практично позбавлений будь-яких серйозних захисних функцій. Це змушує потенційних користувачів сумніватися в безхмарному майбутньому *IP*–телефонії, яку багато експертів пов'язують саме з протоколом *SIP*. Певні надії свого часу було покладено на альянс щодо безпеки *IP*–телефонії, мета яких полягала у дослідженні щодо підвищення обізнаності, вивчення та розроблення безкоштовних методик та інструментів для проведення тестів у області захищеності *IP*–телефонії.

Висновки. З'ясовано, що *IP*–телефонія — це додаток, який працює в *IP*–мережі, і адекватні заходи щодо її захисту загалом позбавляють зловмисника додаткових можливостей з організації прослухування, реалізації *DoS*–атак і використання ресурсів мережі як лазівок у *IP*—телефонну мережу.

Виявлено, що першочерговою вимогою до забезпечення безпеки *IP*–телефонної мережі належить потреба розділення мовних і звичайних даних. Тобто *IP*–телефонія має бути відокремлена від мережі, де передаються інші дані за допомогою *VLAN*. Така сегментація дає змогу створити додатковий рубіж, який запобігає появі атак і зловживань, у т.ч. й ті, джерело яких знаходиться у внутрішній мережі. Водночас, при проектуванні *IP*–телефонної мережі важливо забезпечити відповідну смугу пропускання та не забувати про використання механізмів *QOS* для пріоритетності *IP*–телефонного трафіку.

Встановлено, що використання засобів захисту інформації, орієнтованих на особливості роботи *IP*–телефонії, допомагає уникнути додаткових фінансових витрат на модернізацію наявного устаткування або придбання нових захисних пристроїв.

Література

1. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новіков. — К. : Вид. група BHV, 2009. — 608 с.

2. Дербенцева К. Защищенная IP-телефония / К. Дербенцева [Электронный ресурс]. — Режим доступа: http://citcity.ru/15561

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р., № 80/94, редакція від 30.04.2009 р. [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-вр

4. IP-телефония. Обзор технологии. [Электронный ресурс]. — Режим доступа: http://www.price.od.ua/articles.phtml?id=71

5. Платов М. Что важно знать об IP-телефонии? [Электронный ресурс]. — Режим доступа: http://www.opennet.ru/docs/RUS/voip_asterisk/1.html

6. Что такое IP-телефония и как это работает. [Электронный ресурс]. — Режим доступа: http://itel.com.ua/publications/item=14-chto-takoe-ip-telefoniya-i-kak-eto-rabotaet

References

1. Haivoronskyi M. V., Novikov O. M. (2009) Bezpeka informatsiino-komunikatsiinykh system [Security Information and Communication Systems]. Kyiv, BHV Publ., 608 p.

2. Derbentseva K. Secure IP-telephony. Available at: http://citcity.ru/15561(Accessed 01 Dec 2013)

3. Zakon Ukrainy “Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh” [The Law of Ukraine “Data Protection in the information and telecommunication systems”]. Available at: http://zakon4.rada.gov.ua/laws/show/80/94-вр (Accessed 01 Dec 2013)

4. IP-telephony. Technology review. Available at: http://www.price.od.ua/articles.phtml?id=71 (Accessed 01 Dec 2013)

5. Platov M. What preferably to know about IP-telephony? Available at: http://www.opennet.ru/docs/RUS/voip_asterisk/1.html (Accessed 01 Dec 2013)

6. What is IP-telephony and how it works. Available at: http://itel.com.ua/publications/item=14-chto-takoe-ip-telefoniya-i-kak-eto-rabotaet (Accessed 01 Dec 2013)

Кузьменко І. С., Грицюк Ю. І. ***Використання IP-телефонії в інфраструктурі мережі та особливості її захисту від посягань зловмисників.*** *Розглянуто переваги і недоліки використання IP-телефонії в інфраструктурі мережі та особливості її захисту від посягань зловмисників, які стосуються її інформаційної безпеки: встановлення прослуховування IP-дзвінків і зміни їх змісту, схильності системи VoIP до DoS-атак і т.д. Встановлено, що використання засобів захисту інформаційної мережі, орієнтованих на особливості роботи IP-телефонії, допомагає уникнути додаткових фінансових витрат на модернізацію наявного устаткування або придбання нових захисних пристроїв.*

Ключові слова: *IP-телефонія, інфраструктура мережі, засоби захисту інформації, інформаційні атаки, інформаційна загроза.*

Кузьменко И. С., Грыцюк Ю. И. ***Использование IP-телефонии в инфраструктуре сети и особенности ее защиты от посягательств злоумышленников.*** *Рассмотрены преимущества и недостатки использования IP-телефонии в инфраструктуре сети и особенности ее защиты от посягательств злоумышленников, которые касаются ее информационной безопасности: установка прослушивания IP-звонков и изменения их содержания, склонности системы VoIP к DoS-атакам и т.д. Установлено, что использование средств защиты информационной сети, ориентированных на особенности*

работы IP-телефонии, помогает избежать дополнительных финансовых расходов на модернизацию имеющегося оборудования или приобретение новых защитных устройств.

Ключевые слова: *IP-телефония, инфраструктура сети, средства защиты информации, информационные атаки, информационные угрозы.*

Kuz'menko I. S., Grycyuk Yu. I. ***Using IP-telephony in network infrastructure and peculiarities of its protection from intruders.*** *The article highlights advantages and drawbacks of using IP-telephony in network infrastructure and peculiarities of its protection from intruders concerning its information safety: setting interception of IP-calls and change of their content, disposition of the VoIP system to DoS-attacks etc. It has been determined that using of means of information network protection oriented on the features of IP-telephony work enables to avoid additional financial expenses on modernization of available equipment or acquisition of new protective devices.*

Keywords: *IP-telephony, network infrastructure, means of information network protection, information attacks, information threats.*