ПРОБЛЕМИ ЗАХИСТУ IP-ТЕЛЕФОНІЇ ВІД ПОСЯГАНЬ ЗЛОВМИСНИКІВ

Кузьменко І. С., курсант; Грицюк Ю. І., д.т.н., проф.
Львівський ДУ БЖД, м. Львів, Україна

Можливість передачі голосових повідомлень мережою Інтернет вперше була реалізована в 1993 році. Ця інформаційна технологія отримала назву *VoIP* (англ. *Voice over IP*; *IP*–телефонія) — система зв'язку, яка забезпечує передачу мовного сигналу мережею Інтернет або будь-якими іншими *IP*–мережами. Вхідний сигнал каналом зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискається) для того, щоб видалити надмірність коду. Одним з часткових застосувань такої технології є *IP*–телефонія, тобто система зв'язку, яка передбачає оцифровування голосу абонента і пересилання отриманих даних окремими пакетами мережею Інтернет [2].

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

Технологія *IP*–телефонії об'єднує мережі з комутацією каналів зв'язку (що передають голосову інформацію) і мережі з комутацією пакетів даних (дані, що передаються) в єдину комунікаційну мережу. Безперебійне розпізнавання голосу і його передача з однієї мережі в іншу вирішується за допомогою різних шлюзів [1].

Сучасна *IP*–телефонія дає змогу використовувати будь-яку *IP*–мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу на сьогодні *IP*–телефонія стала деяким стандартом у телефонних комунікаціях — забезпечує зручність, надійність та відносно невисоку вартість *IP*–телефонії порівняно з аналоговим зв'язком. Також вона підвищує ефективність роботи державних установ і дає змогу здійснювати такі раніше недоступні операції, як інтеграція з різними бізнес-додатками.

Проте, сучасна *IP*–телефонія схильна до різних атак: до черв'яків і вірусів, до *DoS*–атак, до несанкціонованого віддаленого доступу та ін. основним загрозам, яким піддається *IP*–телефонна мережа, притаманні [2]:

- реєстрація чужого терміналу, що дає змогу робити дзвінки за чужий рахунок;
- підміна абонента, що дає змогу зловмиснику перенаправляти дзвінки;
- внесення змін до голосового або сигнального трафіку;

- зниження якості голосового трафіку;
- перенаправлення та перехоплення голосового або сигнального трафіку;
- підроблення голосових повідомлень;
- відмова в обслуговуванні;
- віддалений несанкціонований доступ до інфраструктури IP-телефонії.

Це далеко не увесь перелік можливих проблем, пов'язаних з використанням *IP*–телефонії. 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. Думати про забезпечення інформаційної безпеки необхідно вже на етапі підготовки проекту *IP*–телефонії, позаяк саме на цьому етапі необхідно домовитися про те, які механізми захисту мережевої інфраструктури доцільніше використовувати у мережі.

Найбільш досконалий захист від прослуховування забезпечує 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. Але така функціональність збільшує тривалість проходження сигналу, що необхідно враховувати при побудові захищеної лінії зв'язку.

Для передачі мовних сигналів і даних з локальних віртуальних мереж 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.

Атаки типу «відмова в обслуговуванні» на застосування *IP*–телефонії (наприклад, на сервери оброблення дзвінків) і на середовище передачі даних є досить серйозною проблемою. Якщо йдеться про атаки на середовище передачі даних, то за нього у *IP*–телефонії відповідає протокол *RTP* (*Real-Time Protocol*). Для захисту мереж можна використовувати як вбудовані в мережеве устаткування механізми забезпечення інформаційної безпеки такі та інші додаткові рішення.

Сьогодні протокол *SIP* приходить на зміну протоколам *H*.323, проте він 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*.

Література

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

2. Комплексна система захисту інформації. [Електронний ресурс]. — Доступний з http://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.