ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМИ SKYPE У ПОЖЕЖНО-РЯТУВАЛЬНИХ ПІДРОЗДІЛАХ

Лозинський О. І.; Грицюк Ю. І., д.т.н., проф.
Львівський ДУ БЖД, м. Львів, Україна

Програма *Skype* допомагає користувачам мережі Інтернет спілкуватися один з одним так, як вони це роблять звичайним телефоном. Її популярність є такою, що багато користувачів встановлюють її не тільки вдома, але й на роботі не звертаючи увагу на заборону системних адміністраторів. Кількість активних користувачів *Skype* з роками стрімко зростає [1].

Хоча програма *Skype* зручна для відеоспілкування, але чи безпечне її використання, наприклад, у структурних підрозділах Державної служби України з надзвичайних ситуацій (ДСНС України), де часто циркулює конфіденційна інформація? На перший погляд видається так, що проблеми тут ніякої немає. Програма *Skype* не вимагає повноважень адміністратора, не «з'їдає» багато трафіку, стає корисною в різних ситуаціях — як приватних, так і під час ведення ділових перегорів.

Водночас, безконтрольне використання програми *Skype* і інших *VoIP*–додатків у інтрамережах часто призводить до появи значного витоку конфіденційної інформації за рахунок нових комунікаційних каналів. Проте *VoIP*–програми в цьому не винні, оскільки саме інсайдери за допомогою них відправляють важливі відомості назовні. Отже, керівництво структурних підрозділів ДСНС України має або використовувати спеціальні засоби для захисту інтрамережі, що унеможливить витік інформації, або відмовитися від *VoIP*–програм, позаяк на їхню думку це призупинить крадіжку конфіденційної інформації. Насправді, це не вада інформаційної технології як такої, а результат людського чинника — саме працівники установи є джерелом витоку інформації (44,6 %) при використанні *Skype* [2].

Використання *VoIP*–програм у структурних підрозділах ДСНС України може супроводжується цілим комплексом загроз ІБ, при цьому проблема полягає в тому, що *VoIP*–програми взагалі дуже зручні для внутрішніх порушників ІБ. Проте загрози хакерської атаки (29,0 %) і проникнення в інтрамережу шкідливих програм (31,7 %) через використання *Skype* істотно перебільшені. Своє значення тут мають традиційні побоювання системних адміністраторів щодо зламування і зомбування комп'ютерів. Реально ж проблема хакерів не настільки актуальна, як черв'яки і троянські програми, які використовують програми для голосових конференцій. Ахіллесова п'ята всіх засобів комунікації полягає також в тому, що вони створюють додаткові канали витоку конфіденційної інформації, які варто брати під особливий контроль службі ІБ, або блокувати повністю.

Багато системних адміністраторів вважає, що за допомогою *Skype* інсайдери зможуть значно легше викрадати конфіденційну інформацію. По-

перше, голосовий трафік так само, як за допомогою мобільного телефону, можна подзвонити і по *Skype*, і зачитати конфіденційну інформацію охочому до неї. По-друге, пересилання файлів, яке є аналогічним відсиланню файлів по *FTP, e-mail* або по *ICQ*. По-третє, копіювання конфіденційних даних у буфер обміну, а потім вставка в чат, який підтримується програмою *Skype*, що є аналогом *ICQ* або чату в мережі Інтернет. Проте, зі всіх цих каналів витоку інформації відносно небезпечним є тільки голосовий трафік. Всі останні можливості легко контролюються тими ж самими засобами, які застосовуються для захисту інформації від її витоків через електронну пошту чи мережу Інтернет. Що ж до *VoIP*–трафіка, то його навряд чи можна вважати небезпечним каналом витоку інформації. Якщо конфіденційна інформація захищена від витоку, то за допомогою *Skype* її вкрасти не вдасться, а якщо ні, то її можна викрасти і без жодного *Skype*.

Таким чином, самі по собі *VoIP*–програми навряд чи є основним джерелом ризиків ІБ пожежно-рятувальних підрозділів. Майже половина випадків — провина самих працівників державної установи, які не вміють належно користуватися програмою *Skype* або мають прихований намір вкрасти інформацію. Відмовлятися від використання *Skype* — все одно що забороняти користуватися мережею Інтернет або електронною поштою. *VoIP*–програми корисні та зручні в експлуатації, проте аби усунути можливість витоку конфіденційної інформації, службі ІБ потрібно постійно та ретельно контролювати її трафік.

Виходячи з того, що програма *Skype* є приватною власністю та не є open source, рівень безпеки системи не може бути перевірений незалежними експертами. Отже, користувачі-експерти та не експерти — при використанні *Skype* можуть довіряти йому так само, як виробнику програмного забезпечення, а саме: весь трафік програми *Skype* кодується за замовчанням і користувач не може його вимкнути чи втрутитись в його роботу; розробники програми *Skype* повідомляють, що вони використовують тільки відкрито доступні та криптографічно стійкі алгоритми кодування інформації; користувач програми *Skype* не залучається до процесу кодування і тому не має справи з результатами інфраструктури *Public key*.

Отож, у структурі ДСНС України не варто обмежувати використання програми *Skype*, оскільки переваги цієї інформаційної технології очевидні, а недоліки є швидше наслідком неправильного її використання.

Література

1. Доля А. / Безопасность Skype в корпоративной среде / А. Доля // Безопасность. [Электронный ресурс]. — Доступный с http://citcity.ru/15563

2. 50 million concurrent users online! // Skype Numerology. [Electronic resource]. — Mode of access http://skypenumerology.blogspot.com/2013/01/50-million-concurrent-users-online.html