

ЗАХИСТ ІНФОРМАЦІЇ У КАНАЛАХ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Цибуляк Б. З., к.ф.–м.н.

*Львівський державний університет безпеки життєдіяльності,
м. Львів, Україна*

У сучасному світі питання захисту інформації набувають все більшого значення, оскільки вони стосуються як підприємств, що володіють своїми корпоративними секретами, розробками та ін., так і кожної людини зокрема, яка має свою конфіденційну інформацію. Як відомо, інформація має свою ціну, тому поява значного числа конкуруючих між собою різних структур в умовах ринкової економіки природним чином створила певний простір для злочинної діяльності, спрямованої на протизаконне одержання інформації, закритої для доступу сторонніх осіб, з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам [1]. Тому одним з основних джерел загроз інформаційної безпеки є використання пристроїв технічної розвідки для добування важливої інформації.

Метою роботи було проаналізувати можливість витоку даних по технічних каналах та методи їх захисту. До таких каналів можна віднести існуючі лінії технічних засобів (ТЗ) передачі інформації та допоміжні технічні засоби і системи (мережа електроживлення, пожежна сигналізація, заземлення, металеві труби систем опалення, водопостачання й інші струмопровідні металоконструкції), що проходять через приміщення контрольованої зони і виходять за її межі, доступ до яких не складно отримати.

Конфіденційна інформація дуже часто передається по телефонних комунікаціях, що пов'язано з оперативністю і зручністю використання цього виду зв'язку. Не зважаючи на все ширше використання для передачі мовної інформації та даних засобів стільникового зв'язку, апарати дротового зв'язку наразі залишаються незмінними атрибутами офісних приміщень більшості установ. Слід відзначити, що якраз вони відносяться до розряду найменш захищених. І справа не лише в можливості несанкціонованого прослуховування телефонних розмов у режимі реального часу, їхнього запису чи ретрансляції, а й у використанні абонентської телефонної лінії для встановлення телефонних закладок, прослуховуванні приміщень у режимі покладеної телефонної трубки, а також використання для живлення засобів технічної розвідки чи передачі по них інформації за межі контрольованих приміщень [2].

Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних та технічних заходів, а також реєстрацією електронних пристроїв перехоплення інформації. Виявлення каналів витоку мовної інформації зводиться до реєстрації на об'єкті підслуховуючих пристроїв та систем [3].

Щоб запобігти несанкціонованому використанню телефонних ліній крім обмеження фізичного доступу до засобів телефонного зв'язку необхідно використовувати наступні ТЗ:

- застосування пасивних ТЗ захисту (обриву ліній, лічильників часу розмови, сигналізаторів підключення, у тому числі по міжміському зв'язку);
- застосування активних ТЗ захисту (пристрої кодування доступу до телефонних ліній, пристрої захисту від паралельного підключення, пристрої активного маскування інформації та ін.);
- обмеження небезпечних сигналів;
- фільтрування небезпечних сигналів;
- відключення джерел небезпечних сигналів.

Не завжди вирішення питань захисту інформації можна вирішити шляхом залучення спеціалізованих фірм, чи кваліфікованих спеціалістів. У результаті аналізу технічних вимог до системи захисту інформації слід обрати варіант комплексу пристроїв захисту мовної інформації з використанням засобів, які є в Україні сертифікованими чи мають узгоджені технічні умови [3]. До пристроїв захисту телефонних ліній можна віднести: аналізатори стану телефонних ліній «Скеля-1А», «Рікас-4»; фільтри телефонних ліній «Скеля-1Ф», «ФЗП-103-2»; «Рікас-1», «Рікас-2», «Базальт-3», призначені для захисту мовної інформації від витоку абонентськими телефонними лініями внаслідок акустоелектричного перетворення в телефонному апараті в режимі «очікування виклику»; «Скеля-1Г», «Кварц-2», «Гном-4» — генератори шумових сигналів у звуковому діапазоні частот; «Скеля-1К», «Р5055» фірми «Ренар», призначені для автоматичного включення або відключення кінцевих абонентських пристроїв від ліній аналогової телефонної мережі; а також пристрій комбінованої дії «Скеля-1А».

Література

1. Концепція технічного захисту інформації в Україні [Текст]: постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126 // Урядовий кур'єр. — 1997, 12 листопада. — С. 3. — Режим доступу до пост.: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1126-97-%EF>.
2. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев— М. : Гостехкомиссия РФ. — 1998. — 320 с.
3. Мелешко О. О. Проблеми, які виникають при захисті телефонних ліній / О. О. Мелешко, І. О. Лебединська, А. В. Палазюк, А. І. Ткачук [Електронний ресурс]. — Режим доступу: http://www.rusnauka.com/35_OINBG_2010/Informatica/76208.doc.htm