УДК 621.395

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Цибуляк Б. З., кандидат фізико-математичних наук
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

PROTECTION OF INFORMATION LEAKAGE BY CHANNELS TELEPHONE

Bohdan Tsybulyak, Philosophiae Doctor,
Lviv State University of Vital Activity Safety, Lviv, Ukraine

Вступ

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].

Одним з основних джерел загроз інформаційної безпеки є використання пристроїв технічної розвідки для добування важливої інформації. Тому питання аналізу джерел витоку інформації по технічних каналах та методи їх захисту є на сьогодні актуальною задачею. До таких каналів можна віднести існуючі лінії технічних засобів передачі інформації і допоміжні технічні засоби й 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 й доступ до яких не складно отримати. Метою роботи було провести аналіз загроз, пов'язаних з витоком даних через телефонні лінії (ТЛ) та запропонувати методи боротьби із несанкціонованого знімання із них інформації.

Загрози порушення конфіденційності у каналах зв'язку

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, комп'ютерних мереж, Інтернету, апарати дротового зв'язку наразі залишаються незмінними

атрибутами офісних приміщень більшості установ. Слід відзначити, що саме 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 (АТЛ) для встановлення телефонних закладок, прослухуванні приміщень у режимі покладеної телефонної трубки, а також використання мережі АТС для живлення засобів технічної розвідки чи передачі по них інформації за межі контрольованих приміщень. Проведені дослідження даної проблеми показали, що найвразливішою є ділянка АТЛ, оскільки розводка кожного абонента від телефонної розетки до розподільчої коробки чи шафи виконується двопровідним телефонним дротом марок ТРП або ТРВ, прокладеним, як правило, по відкритій ділянці приміщень. Доступ до магістральних телефонних кабелів є обмежений фізично (підземної прокладкою) і під'єднатися до відповідної пари багатопарного кабелю за умови мультиплексування сигналів є досить складно [2].

Тому методи запобігання та протидії поширенню конфіденційної інформації каналами телефонного зв'язку можна класифікувати наступним чином:

- обмеження фізичного доступу до каналів телефонного зв'язку;
- контроль та виявлення несанкціонованих під'єднань до АТЛ, яка перебуває у робочому стані;
- встановлення запобіжних засобів протидії витоку мовної інформації;
- усунення чи виведення з ладу встановлених телефонних закладок;
- впровадження криптографічних методів захисту конфіденційної інформації, що передається засобами телефонного зв'язку.

Методи протидії несанкціонованому доступу

Для перехоплення телефонних розмов чи прослуховування приміщень можуть бути використані як безпосередньо телефонні апарати, так і ТЛ за умови встановлення на них засобів технічної розвідки, так званих телефонних закладок. Тому обмеження фізичного доступу до АТЛ, яке досить просто організувати у контрольованих зонах і складно у об'єктах з вільним доступом, є одним із найпростіших запобіжних заходів. Суть методу в обох випадках зводиться до ретельного огляду телефонного апарата і мережі щодо підключення сторонніх пристроїв. Сучасні телефонні закладки мають дуже малі розміри, або можуть бути закамуфльовані під радіоелектронні елементи, які важко виявити, особливо, якщо вони встановлені, наприклад, у телефонному апараті чи розетці.

Проте навіть без проникнення у контрольоване приміщення наявний у ньому телефонний апарат можна використати як джерело прослуховування розмов у режимі реального часу при піднятій телефонній трубці та приміщ-

щення при покладеній трубці за умови доступу до ТЛ на відстані, що не перевищує кількох десятків метрів. І якщо у першому випадку сигнал у лінію подається з мікрофонного кола, то у другому використовується явище акустично-електричних перетворень у дзвінковому колі телефонного апарату, яке постійно залишається підключене до ТЛ, на відміну від мікрофонної і телефонної капсулі. Спеціальні високочутливі низькочастотні підсилювачі, гальванічно підключені до ТЛ, дозволяють перехопити інформаційний сигнал, наведений у лінії, амплітуда якого у залежності від телефонного апарату може сягати кількох мілівольт [3]. Збільшити дальність перехоплення інформації можна за рахунок використання методу високочастотного нав'язування. В залежності від методу гальванічного підключення такі закладки поділяються на контактні (послідовні чи паралельні) та безконтактні, а по живленню – ті що живляться від телефонної мережі та автономні [4].

Ще одним із видів телефонного шахрайства є несанкціоноване підключення до телефонної лінії і використання її для власних потреб. Це, як правило, призводить до фінансових втрат постраждалого через надходження рахунків за здійснення міжміських/закордонних дзвінків та позбавлення абонента можливості вчасно передати інформацію, оскільки його лінія на момент втручання буде насилати сигнал "зайнято".

За умови можливості доступу в контрольоване приміщення, у ньому можна встановити виносний мікрофон, що використовуватиме телефонну лінію як канал передачі сигналу або джерело живлення.

Запобігти витоку мовної інформації через канали зв'язку можна з допомогою пасивних та активних методів. До широко вживаних пасивних методів захисту відносяться: обмеження чи фільтрація небезпечних сигналів за допомогою пристроїв "Скеля-1Ф", "ФЗП-103-2"; захист мовної інформації від витоку абонентськими телефонними лініями внаслідок акустоелектричного перетворення в телефонному апараті у режимі "очікування виклику" – "Рікас-1", "Рікас-2", "Базальт-3"; відключення з використанням пристроїв "Скеля-1К", TS2, "Р5055" фірми "Ренар" джерел таких сигналів – телефонного апарату – за умови покладеної телефонної трубки. Визначити наявність несанкціонованого підключення до каналу зв'язку можна з використанням індикаторних пристроїв "Скеля-1А", "Рікас-4", що фіксують зміну параметрів телефонної лінії, порівняно з відповідними їх значеннями для "чистої" лінії (контроль сталої напруги живлення, струму короткого замикання, навантажувальної характеристики, зміни рівня сигналу на вході приймача контролю у момент підняття трубки, а також низькочастотних сигналів телефонних закладок та сигналів високочастотного нав'язування і накачки, сигналізатор обриву ТЛ тощо), а також періодичний контроль на наявність телефонних закладок у знеструмленому стані з використанням аналізаторів дротових ліній або пристроїв нелінійної локації типу "ULAN-

2" (вимірювання імпедансу АТЛ, асиметрії проводів АТЛ, знімання вольт-амперної, перехідної та лісажу-характеристик, визначення віддаленості до неоднорідностей лінії, спричинений контактними під'єднаннями) [5].

Активні методи захисту від просочування інформації по електроакустичному каналу за допомогою пристроїв "Скеля-1Г", "Кварц-2", "Гном-4" передбачають лінійне зашумлення телефонних ліній низькочастотним сигналом (300…3400 Гц) у режимі покладеної телефонної трубки і його припинення при знятті трубки телефонного апарату, що призводить придушення мікрофонних систем, які використовують телефонну лінію для передачі інформації на низькій частоті; або подачу широкосмугової високочастотної маскуючої перешкоди під час розмови в діапазоні вищих частот звукового діапазону (від 6…8 кГц до 16…20 кГц чи від 20…25 кГц до 50…100 кГц), що спричиняє активізацію підслуховуючих пристроїв і суттєве спотворення корисних сигналів (погіршення розбірливості мови) при перехопленні їх всіма типами підслуховуючих пристроїв. До активних методів протидії несанкціонованому доступу відносяться методи подачі у телефонну лінію синфазної низькочастотної маскуючої перешкоди; підвищення напруги в телефонній лінії під час розмови до 18…24 В; подачу під час розмови в лінію постійної напруги, відповідної напрузі в лінії при піднятій телефонній трубці, але зворотної полярності (метод "обнулення"). Перелічені заходи дозволяють порушити функціонування або відключити підслуховуючі пристрої, не залежно від способу їх під'єднання до лінії.

Виведення з ладу встановлених телефонних закладок, гальванічно під'єднаних до лінії, реалізується методом "випалювання" – подаванням у лінію при від'єднаному телефонному апараті високовольтних імпульсів напругою 1,5 кВ потужністю 15-50 ВА в режимах закороченої та розімкненої ТЛ, що призводить до знищення вхідних каскадів пристроїв перехоплення інформації чи їхніх блоків живлення. До пристроїв, які реалізують цей метод, належать "ПТЛ-1500", "КС-1300", "Кобра" [6].

Одними із найдосконаліших способів захисту даних, що передається каналами зв'язку, є використання криптографічних алгоритмів шифрування мовної інформації. Такий спосіб буде вимагати від абонентів, що спілкуються, наявності однакових пристроїв кодування-декодування сигналу – скремблерів. Вони забезпечують повну конфіденційність переговорів і можуть використовуватися у вигляді телефонної приставки типу Р6020, "Горіх-II"; телефонного апарату "Горіх-Т"; накладки на телефонну трубку ACS-2.

Висновки

Безперервне вдосконалення як технологій, так і засобів несанкціонованого знімання мовної інформації, вимагає серйозної уваги до методів та засобів захисту ТЛ. У роботі проведено класифікацію загроз порушення

конфіденційності у каналах телефонного зв'язку та запропоновано методологію усунення несанкціонованого зняття інформації.

Комплексне використання ряду перелічених технічних засобів дозволяє запобігти використанню каналів зв'язку для підслуховування телефонних розмов та прослуховування приміщень, через які вони проходять.

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/cgibin/laws/main.cgi?nreg=1126-97-%EF\.
2. Хома В.В. Методи і засоби технічного захисту інформації на абонентських телефонних лініях / Хома В.В. // Автоматика, вимірювання та керування. — Львів.: Видво Нац. ун-ту "Львів. політехніка". — 2009. — № 639. — С. 87—93. — Режим доступу до журн.: http://ena.lp.edu.ua:8080/handle/ntb/2342.
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
4. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / Хорев А.А. — М.: Гостехкомиссия РФ. — 1998. – 320 с.
5. Универсальный анализатор проводных коммуникаций ULAN-2. Техническое описание и инструкция по эксплуатации. — М. — 2004. — 88 с.
6. Лагутин В.С. Утечка и защита информации в телефонных каналах / В.С. Лагутин, А.В. Петраков. — М.: Энергоатомиздат. — 1996. — 304 с.

References

1. Kontseptsiia tekhnichnoho zakhystu informatsii v Ukraini [Tekst]: postanova Kabinetu Ministriv Ukrainy vid 8 zhovtnia 1997 roku № 1126 // Uriadovyi kurier. — 1997, 12 lystopada. — S. 3. — Rezhym dostupu do post.: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?nreg=1126-97-%EF\.
2. Khoma V.V. Metody I zasoby tekhnichnoho zakhystu informatsii na abonentskykh telefonnykh liniiakh / Khoma V.V. // Avtomatyka, vymiriuvannia ta keruvannia. — Lviv.: Vydvo Nats. Un-tu "Lvivska politekhnika". — 2009. — № 639. — S. 87—93. — Rezhym dostupu do zhurn.: http://ena.lp.edu.ua:8080/handle/ntb/2342.
3. Meleshko O.O. Problemy, yaki vynykaiyt pry zakhysti telefonnykh linii // O.O. Meleshko, I.O. Lebedynska, A.V. Palaziyk, A.I. Tkachuk [Elektronnyi resurs]. — Rezhym dostupu: http://www.rusnauka.com/35_OINBG_2010/Informatica/76208.doc.htm
4. Khoriev A.A. Zashchita informatsii ot utiechki po tekhnicheskim kanalam. Chast 1. Tekhnicheskie kanaly utiechki informatsii / Khoriev A.A. — M.: Gostekhkomissiia RF. — 1998. — 320 s.
5. Universalnyi analizator provodnykh kommunikatsii ULAN-2. Tekhnicheskoie opisaniie i instruktsiia po ekspluatatsii. — M. — 2004. — 88 s.
6. Lagutin V.S. Utiechka i zashchita informatsii v telefonnykh kanalakh / V.S. Lagutin, A.V. Petrakov. — M.: Energoatomizdat. — 1996. — 304 s.

Цибуляк Б. З. ***Захист інформації від витоку каналами телефонного зв'язку.*** *Розглянуто основні проблемні питання, пов'язані зі створенням комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Проведено огляд методів і засобів виявлення несанкціонованих під'єднань до абонентських телефонних ліній та запропоновано методи боротьби із витоком мовної інформації з використанням адекватних технічних пристроїв захисту.*

Ключові слова*: технічний захист інформації, інформаційна безпека, мовна інформація, комутована телефонна мережа, канали зв'язку.*

Цыбуляк Б. З. ***Защита информации от утечки каналами телефонной связи.*** *Рассмотрены основные проблемные вопросы, связанные с созданием комплексов технической защиты информации на объектах информационной деятельности. Проведен обзор методов и средств обнаружения несанкционированных подключений к абонентским телефонным линиям и предложены методы борьбы с утечкой речевой информации с использованием адекватных технических устройств защиты.*

Ключевые слова: *техническая защита информации, информационная безопасность, речевая информация, коммутированная телефонная сеть, каналы связи.*

Bohdan Tsybulyak ***Protection of information leakage by channels telephone.***

Introduction. The design rule requirements for abstracts and reports for participate in the International Scientific Technical Conference «Radio Engineering Field, Signals, Devices and Systems» or abbreviated REFSDS are presented at this paper.

Requirements for document. The requirements for execution of text, formulas, tables and figures with examples of implementation are expounded. The examples of bibliographic records execution and abstracts are presented.

Methods of counteraction to the unauthorized access. The characteristics of the known methods of detecting unauthorized connections to the subscriber telephone line, providing the confidentiality of telephone conversations, protecting from listening of apartments and prevention of the unauthorized use of telephone connection are given.

Conclusions. The classification of threats of confidentiality violation in telephone communication channels is conducted and methodology for eliminating of unauthorized interception of information is proposed. The complex use of a number of the listed technical equipments allows to prevent the use of communication channels for the wire tapping and listening of apartments, through which they pass.

Keywords*: technical defence of information, information security, language information, switched telephone networks, communication channels.*