УДК 621.395

В. М. Іванюк[1], В. В. Хома[1,2]
[1]Національний університет "Львівська політехніка",
кафедра захисту інформації,
[2]Політехніка Опольська, інститут автоматики та інформатики

АНАЛІЗ ПЕРСПЕКТИВНИХ НАПРЯМІВ УДОСКОНАЛЕННЯ ЗАСОБІВ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ У ТЕЛЕФОННИХ ЛІНІЯХ

Описано способи під'єднання та принципи роботи телефонних закладок, проаналізовано переваги та недоліки методів і засобів виявлення несанкціонованих під'єднань до телефонної лінії. Показано актуальність пошуку нових підходів щодо побудови сторожових засобів виявлення несанкціонованих під'єднань.

The paper describes ways of connecting and operation principles of telephone bugs, analyzes the advantages and disadvantages of methods and tools for detection of unauthorized connections to the subscriber's telephone line. Topicality of searching for new approaches to the design of watchdog devices for detecting unauthorized connection is demonstrated.

Вступ

Сьогодні накопичено величезний досвід застосування методів і засобів ведення технічної розвідки. З переходом України до ринкової економіки протидія технічним розвідкам стала актуальною не лише для державних органів та військових структур, але і для захисту комерційної інформації приватних підприємств.

Зазвичай розвідувальні дії передбачають несанкціонований доступ до каналів передавання даних конкуруючої сторони, зокрема до її ліній телефонного зв'язку [1,2]. Телефонними каналами, окрім сигналів мовлення, передаються факсимільні повідомлення та, за участі модемів, комп'ютерні дані. Несанкціоноване отримання інформації може не лише завдати матеріальних збитків власнику, але і негативно позначатися на його репутації.

З погляду інформаційної безпеки найуразливішим компонентом у структурі телефонного зв'язку є абонентська телефонна лінія (АТЛ). Вона може бути об'єктом технічної розвідки не лише як джерело конфіденційних даних, що передаються в сеансах зв'язку. Через недосконалість електричної схеми і конструкції звичайні телефонні апарати допускають витік мовної інформації, що циркулює у приміщенні у режимі покладеної слухавки [2,3]. У разі застосування методів високочастотного нав'язування та "підкачки" цю інформацію можна передавати на значні відстані.

Сьогодні існує чимало пристроїв виявлення несанкціонованих під'єднань до АТЛ, але, на жаль, вони не повністю задовольняють вимоги технічного захисту інформації, зокрема через постійне вдосконалення засобів технічної розвідки. Тому актуальними є пошук нових та вдосконалення існуючих методів і засобів виявлення несанкціонованих під'єднань до АТЛ.

Опис способів під'єднань та принципів роботи засобів технічної розвідки на ділянці абонентських телефонних ліній

Сучасні засоби технічної розвідки на ділянці АТЛ, або короткотелефонні закладки (ТЗ) використовуються не лише для перехоплення телефонних розмов, але і для прослуховування приміщень, де розташовано телефонний апарат. На рис. 1 наведено узагальнену структуру телефонних закладок [4]. Основою ТЗ є телефонний адаптер, що забезпечує знімання сигналу із АТЛ. Наступним важливим елементом є вузол опрацювання сигналу, до функцій якого належить

виділення інформативного сигналу на тлі різного роду перешкоджальних факторів та його підсилення до рівня, придатного для подальшого використання.

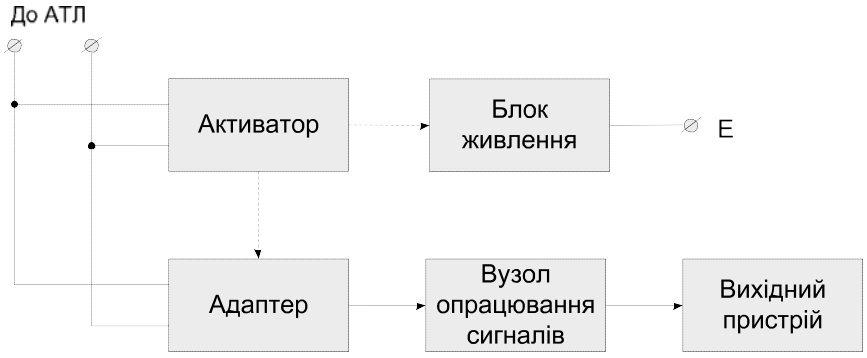

Рис. 1. Узагальнена структура засобів техрозвідки, призначених для використання в АТЛ

Перехоплені за допомогою телефонних закладок сигнали можуть використовуватися для:

– прослуховування розмови в реальному часі;

– запису розмовного сигналу;

– ретрансляції сигналу за межі контрольованої зони.

Для прослуховування використовується перетворювач електричного сигналу на акустичний, для запису – пристрій фіксації мовного сигналу на магнітну стрічку чи флеш-пам'ять цифрового диктофона, а для ретрансляції – радіопередавач, що випромінює перехоплені з телефонної лінії сигнали в ефір з подальшим їх прийманням на радіоприймач. Для приховування радіоканалу можна використовувати спеціальні формати кодування та модуляції, зокрема технологію шумоподібних сигналів [5].

Можлива також комбінація другого і третього способів. Це так звані диктофони із пострілом. Такі пристрої стискають і записують мовну інформацію упродовж деякого часу, а потім сигналом таймера чи із пульта дистанційного керування передають стиснені дані радіоканалом. Оскільки таке передавання нетривале, засікти його важко. Отже, поєднання цих методів нівелює основні їх недоліки: підвищується оперативність другого методу і прихованість третього [6].

Залежно від способу під’єднання до абонентських телефонних ліній розрізняють безконтактні та контактні ТЗ. Контактні ТЗ, своєю чергою, бувають послідовного і паралельного типів. За цією класифікаційною ознакою передовсім визначається тип телефонного адаптера. Так, безконтактний адаптер може бути виготовлений у вигляді індуктивного знімача, який у найпростішому варіанті представляє собою навиту на розрізане феритове кільце котушку. При охопленні кільцем одного із проводів АТЛ перетворюються електромагнітні коливання, створені проходженням розмовного струму по лінії, на електричні коливання, що після підсилення надходять на пристрій відтворення чи запису [3,4].

Безконтактні ЗТР неможливо виявити вимірюванням електричних параметрів телефонної лінії, але якість відтворення чи запису на диктофон не дуже висока через чутливість індуктивного знімача до різних електромагнітних перешкод. Крім того, габарити безконтактних пристроїв доволі великі, що ускладнює їх камуфлювання.

Контактні адаптери мають гальванічний контакт із телефонною лінією і тому здатні забезпечити значно вищу якість. Паралельний адаптер під’єднується до лінії паралельно і відрізняється високим вхідним опором і малою вхідною ємністю, що утруднює його виявлення (рис. 2, а). Послідовний адаптер вмикається в розрив одного з проводів телефонної лінії (рис. 2, б). Має вхідний опір 200....500 Ом і значну вхідну ємність, що полегшує його виявлення [1,4].

Живлення телефонних закладок може здійснюватися двояко: безпосередньо від АТЛ або від автономного джерела. За першим варіантом блок живлення реалізується у вигляді спеціального узгоджувального пристрою і забезпечує практично необмежений термін дії, хоч може бути виявлений за ознакою додаткового навантаження АТЛ. Другий варіант має протилежні властивості.

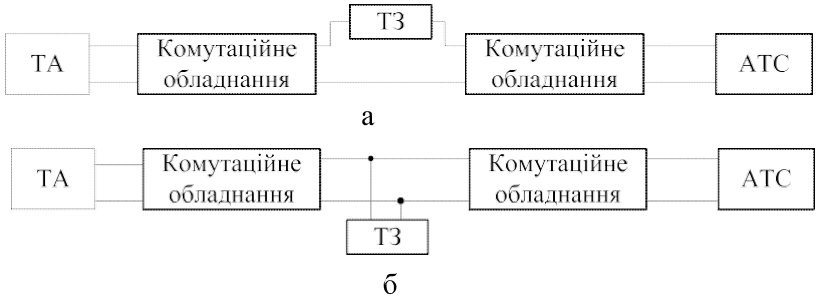

Рис. 2. Паралельне (а) та послідовне (б) під'єднання телефонної закладки (ТЗ)

Для заощадження ресурсу та маскування автономних джерел живлення до складу телефонних закладок вводять спеціальні пристрої-активатори. Їх робота може ґрунтуватися на аналізі стану телефонної лінії (активація ТЗ відбувається після піднесення трубки) або на детектуванні розмовного сигналу в АТЛ (так званий акустозапуск).

Характеристика методів і засобів виявлення несанкціонованих під'єднань до АТЛ

Загрози інформаційній безпеці абонентів телефонних мереж найчастіше реалізуються через контактні під'єднання засобів технічної розвідки до абонентських телефонних ліній. Методи виявлення несанкціонованих під'єднань до АТЛ базуються та тому, що безпосереднє під'єднання до них сторонніх пристроїв (засобів технічної розвідки, "піратських" телефонних апаратів тощо) викликає зміну електричних параметрів ліній, насамперед напруги, струму, а також імпедансу. Крім того, працюючі телефонні закладки передають телефонними лініями чи випромінюють в ефір сигнали, тому можна використовувати методи, які забезпечують їх виявлення та ідентифікацію [3,7]. Основними демаскувальними ознаками, що можуть використовуватися для виявлення телефонних закладок, є:

- незначний (від декількох десятків до кількох Вольт) спад напруги при покладеній чи піднятій трубці;
- наявність струму витоку (від одиниць до кількох десятків мА) при від'єднаному телефонному апараті.

Розвиток технологій і елементної бази позначається на удосконаленні методів маскування закладних пристроїв та зумовлює значне зменшення їх масо-габаритних показників, що ускладнює їх візуальне виявлення. Як відомо [3, 4], методи виявлення несанкціонованих під'єднань до АТЛ поділяють на дві групи:

- які вимагають знеструмлення АТЛ, тобто від'єднання АТЛ від автоматичної телефонної станції (рис. 3, а);
- придатні для контролю параметрів АТЛ у робочому стані (рис. 3, б).

Для виявлення несанкціонованих під'єднань до знеструмлених АТЛ найчастіше застосовують методи вимірювання таких параметрів лінії: опір, ємність, індуктивність та асиметрія, вольт-амперна, Лісажу та перехідна характеристики. Результати контролю змін параметрів АТЛ, зумовлених сторонніми під'єднаннями, зазвичай достовірніші, особливо на ділянці від абонента до розподільчого обладнання.

Перевагами методів цієї групи є:

- широкий вибір методів контролю, що ґрунтуються на різних фізичних принципах;
- можливість від'єднання міського телефонного кабелю (найпротяжнішої частини АТЛ) знижує дестабілізуючий вплив на параметри контрольованої ділянки АТЛ.

До недоліків можна віднести:

- можливість застосування лише для періодичних планових чи позапланових пошукових робіт;
- непридатність до виявлення так званих "сторожових закладних пристроїв", які не завжди під'єднано до АТЛ, а активуються лише за певним алгоритмом.

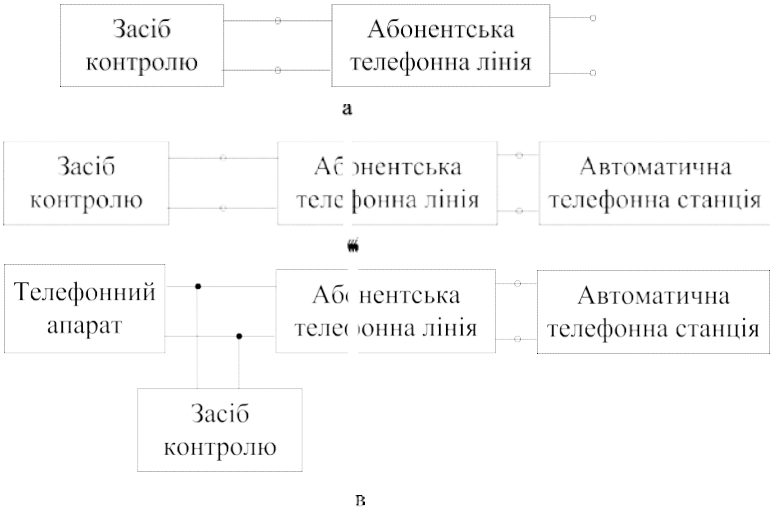

Рис. 3. Способи під'єднання засобів виявлення несанкціонованих під'єднань до:
а – знеструмленої АТЛ; б – АТЛ у робочому стані; в – АТЛ у робочому режимі

Задля усунення зазначених недоліків застосовують методи виявлення несанкціонованих під'єднань до АТЛ, що знаходиться у робочому стані. Особливо привабливим і зручним було б застосування контролю АТЛ у робочому режимі (рис. 3, в), коли пристрій контролю працює як сторожовий, а не як пошуковий. Це б дало змогу фіксувати сторонні під'єднання у реальному часі і негайно сигналізувати абоненту про факт такого під'єднання.

Формулювання вимог та аналіз шляхів удосконалення характеристик сторожових засобів контролю АТЛ

На рис. 3, в наведено схему під'єднання засобів контролю АТЛ у сторожовому режимі. Можна сформулювати такі вимоги до характеристик сторожових пристроїв:

– під'єднання пристрою до АТЛ не повинно знижувати якість телефонного зв'язку;

– пристрій повинен забезпечувати високу чутливість до зміни контрольованих параметрів АТЛ і водночас забезпечувати інваріантність до впливу неінформативних параметрів та дії завад;

– пристрій повинен працювати в режимах покладеної і піднятої слухавки;

– в режимі покладеної слухавки пристрій повинен фіксувати час під'єднання стороннього пристрою.

Для вимірювання параметрів досліджуваних ліній можна використовувати як універсальні, так і спеціалізовані вимірювальні пристрої, що побудовані для проведення пошукових робіт і оснащені спеціальними адаптерами для під'єднання до різного типу ліній. Існуючі засоби контролю провідних ліній, як правило, реалізують кілька методів вимірювання параметрів АТЛ. Серед сучасних засобів контролю проводових ліній найчастіше використовуються такі як Ulan-2, ТСМ-03, СРМ-700, РТ-030, ПТУ-5В та ін.

Аналізуючи функціональні можливості існуючих засобів контролю провідних ліній, зазначимо деякі важливі, на наш погляд, недоліки та обмеження вищевказаних приладів, а саме:

– відсутність комплексності та універсальності проведення всіх вимірювань характеристик ліній, одним приладом із зіставленням результатів;

– недостатня чутливість, а відтак і достовірність результатів контролю параметрів досліджуваних ліній;

– не всі прилади оснащено інтерфейсом для передавання результатів контролю АТЛ на персональний комп'ютер для подальшого опрацювання та формування звітної документації;

– не всі прилади мають функції запам'ятовування і відтворення записаної інформації для проведення аналізу;

– зазвичай контроль абонентської телефонної лінії у робочому стані зводиться лише до аналізу наявних в лінії сигналів.

Ціновий діапазон пристроїв виявлення несанкціонованого під'єднання до АТЛ коливається від десятків до декількох тисяч доларів. Однак ці пристрої не дозволяють з високою достовірністю гарантувати факт виявлення в лінії "закладок", що зумовлено низкою об'єктивних факторів, які перешкоджають ефективному вирішенню завдання контролю:

– параметри телефонних ліній, особливо тих, що експлуатуються тривалий час, можуть значно відхилятися від паспортних (навіть у специфікації на стандартні параметри сигналів міських АТС передбачено значний розкид);

– значний вплив на параметри лінії зв'язку різних наведень, коливань напруги живлення;

– для більшості телефонних ліній не задокументовано або не збережено даних про параметри лінії на момент монтажу та в процесі експлуатації.

Висновок

Отже, розроблення нових методів дослідження телефонних ліній у робочому стані та оптимізація структури засобів виявлення пристроїв несанкціонованого отримання інформації з проводових комунікацій є актуальним завданням. Реалізація методів аналізу параметрів лінії в активному режимі дасть змогу покращити виявні властивості пристрою, оскільки зможе індифікувати наявність пристроїв несанкціонованого отримання інформації різного призначення та технічної реалізації.

Не менш важливим завданням є розроблення методик інструментального контролю наявності пристроїв несанкціонованого отримання інформації з телефонних ліній зв'язку та розроблення структури паспорту ліній зв'язку та множини параметрів, які підлягають документуванню.

1. Хорев А. А. Способы и средства защиты информации: Учеб. пособие. – М.: МО РФ, 2000. – 316 с. 2. Лагутин В. С., Петраков А. В. Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1996. – 304 с. 3. Захист засобів і каналів телефонного зв'язку: навч. посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Львів: Видавництво Львівської політехніки, 2012. – 212 с. 4. Хома В. В. Інформаційна безпека абонентів стаціонарних телефонних мереж // Вісник Нац. ун-ту "Львівська політехніка".– 2008. – № 608. – С. 74–85. 5. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. 2-е изд., испр.: Пер. с англ. – М.: Изд. Дом "Вильямс", 2003. – 1104 с. 6. Вернигоров Н. С. Особенности НКУ и методы их блокировки. – Томск: Изд-во "Пиллад", 2006. 7. Хома В. В. Методи і засоби технічного захисту інформації на абонентських телефонних лініях // Вісник Нац. ун-ту "Львівська політехніка". – 2009. – № 639. – С. 87–94. 8. НД ТЗІ 4.7-001-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань. 9. Ulan-2 Универсальный анализатор проводных коммуникаций: Техническое описание и инструкция по эксплуатации.