УДК 621.395

В.В. Хома
Національний університет “Львівська політехніка”,
кафедра захисту інформації,
Політехніка Опольська, інститут автоматики і інформатики

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ АБОНЕНТІВ СТАЦІОНАРНИХ ТЕЛЕФОННИХ МЕРЕЖ

Проаналізовано актуальний стан інформаційної безпеки абонентів комутованих телефонних мереж загального користування. Розкрито специфіку загроз для інформації у телефонії, описано відомі способи несанкціонованого доступу та використання абонентських телефонних ліній. Подано характеристику відомих методів і засобів виявлення несанкціонованих під’єднань до абонентських телефонних ліній, забезпечення конфіденційності телефонних розмов, захисту від прослуховування приміщень та запобігання несанкціонованому використанню телефонного зв’язку.

The information security relevant state public switched telephone network subscribers of is analyzed in the article. The specific of information threats in telephony is exposed and the known methods of unauthorized access and use of subscriber telephone loops are described. The existent methods and facilities description of the unauthorized connecting detection to the subscriber telephone loops, providing of confidentiality of telephone talks, defense, from listening of locations and prevention of the unauthorized use of telephony is given.

1. Характеристика загроз інформації у телефонних мережах загального користування. Незважаючи на бурхливий розвиток комп’ютерних мереж і медіатехнологій, передавання голосових повідомлень продовжує домінувати у загальному трафіку сучасної телекомунікації [1]. Це зумовлено передовсім простотою та доступністю телефонного зв’язку. Разом з тим, телефонний зв’язок є одним з найбільш незахищених у сенсі інформаційної безпеки.

Як відомо [2, 3], захист інформації розуміють у таких трьох аспектах, як:

- конфіденційність (забезпечення інформаційної системи від витоку інформації);
- доступність (можливість у будь-який момент отримати сервіс заданої якості);
- цілісність (запобігання фальшуванню та несанкціонованій модифікації інформації).

Щодо телефонного зв’язку загроза конфіденційності проявляється у:

- підслуховуванні телефонних розмов (режим піднятої телефонної трубки);
- прослуховування приміщень, у яких розміщений телефонний апарат (режим відкладеної телефонної трубки).

Підслуховування телефонних розмов можливе за допомогою доволі простих технічних засобів, оскільки голосові повідомлення передаються у відкритому вигляді. Утворення елементами телефонного апарата паразитних сигналів створює загрозу прослуховування приміщень.

Загрозу доступності можна розглядати як блокування доступу внаслідок пошкодження елементів телефонного тракту чи спотворення службових сигналів на етапі встановлення з’єднання. Крім того, значне погіршення стану каналів зв’язку, а відтак і зниження якості голосових повідомлень також можна розглядати як вид блокування.

Загроза цілісності щодо телефонного зв’язку має певну специфіку. Насамперед модифікувати телефонні голосові повідомлення складно через їхню природу (передавання повідомлень у реальному часі мережами із комутацією каналів). Фальшування телефонних повідомлень між знайомими абонентами також малоймовірне через натуральний спосіб взаємної автентифікації за

голосом, манерами розмовляти, можливістю задати будь-яке питання, щоб зняти підозри. Проблема автентичності виникає, коли абоненти не є знайомими. Загалом автентичність абонента можна було б пов'язати із його абонентським номером і з метою зменшення ризику фальшування розірвати з'єднання та здійснити повторне віддзвонювання, але недостатня захищеність абонентських телефонних ліній від несанкціонованих під'єднань залишає це питання відкритим. Є ще один аспект загрози цілісності системи телефонного зв'язку – це телефонне шахрайство, тобто несанкціоноване використання засобів телефонного зв'язку. Порушення цілісності системи телефонного зв'язку відбувається у формі гальванічного під'єднання до абонентської телефонної лінії.

2. Аналіз телефонного зв'язку з позицій інформаційної безпеки. Телефонний тракт (рис.1) утворюється за допомогою фізичного з'єднання абонентської лінії, елементів комутаційного поля автоматичної телефонної станції (АТС), каналів з'єднувальних ліній та систем передачі [4, 5]. Перехоплення голосових повідомлень у з'єднувальних лініях і магістральних каналах систем передачі є складним через потребу демультиплексації групових сигналів. АТС також є доволі захищеним елементом телефонного тракту, особливо порівняно із абонентською телефонною лінією (АТЛ). Проте і загрози для інформації на АТЛ є неоднаковими на різних її ділянках.

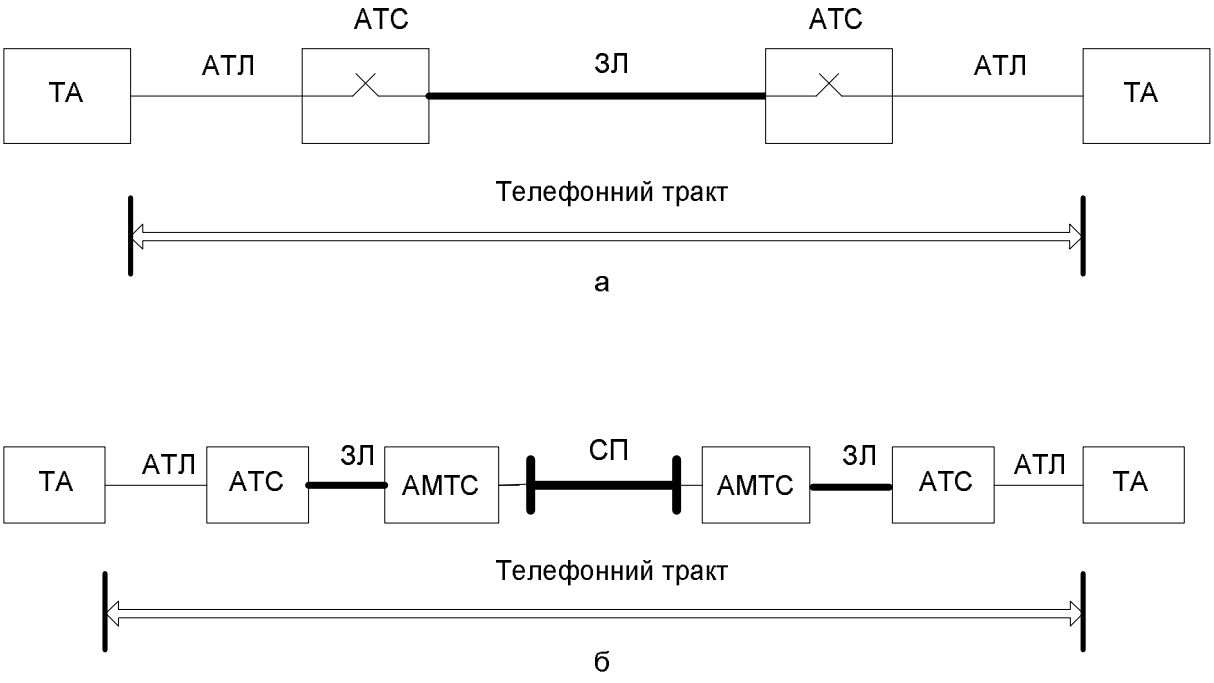

Рис.1. Елементи телефонного тракту міської (а) та міжміської (б) мереж: ТА – телефонний апарат; ЗЛ – з'єднувальна лінія; СП – система передачі; АМТС – автоматична міжміська телефонна станція

Найуразливішою з погляду перехоплення та блокування інформації є ділянка абонентської телефонної лінії від телефонної розетки до розподільної скриньки, виконана двопровідним телефонним проводом ТРП (рис. 2).

У телефонних мережах загального користування кожна АТЛ асоціюється із конкретним абонентом цієї мережі, тобто автентифікація абонентів здійснюється лише на основі фізичного під'єднання до АТЛ. Зважаючи на відкритість та доступність прикінцевих ділянок АТЛ, існує доволі велика загроза інформаційній безпеці шляхом несанкціонованих підключень [5, 6].

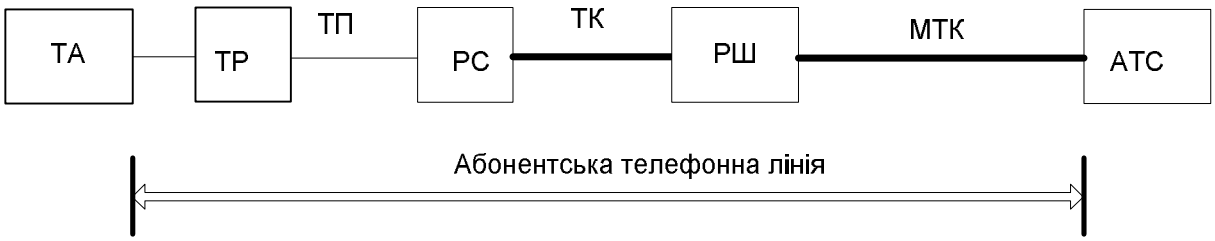

Рис.2. Елементи абонентської телефонної лінії:
ТР – телефонна розетка; РС – розподільна скринька; РШ – розподільна шафа;
ТП – телефонний провід; ТК – телефонний кабель; МТК – міський телефонний кабель

3. Способи несанкціонованого під'єднання та принципи побудови телефонних закладок. Підслуховувати телефонні розмови можна, під'єднавшись до АТЛ за допомогою паралельного телефону, "монтерської" слухавки чи звичайних навушників для плеєра. Проте такі під'єднання погіршують якість зв'язку, тому можуть бути порівняно легко виявлені навіть без спеціальних пристроїв контролю.

Сьогодні поширеними є спеціальні засоби технічної розвідки – так звані телефонні закладки (ТЗ), які можуть використовуються як для перехоплення телефонних розмов, так і для прослуховування приміщень, де розташовано телефонний апарат. На рис.3 наведено узагальнену структуру телефонних закладок. 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 та тлі різного роду перешкоджаючих факторів та його підсилення до рівня, придатного для подальшого використання.

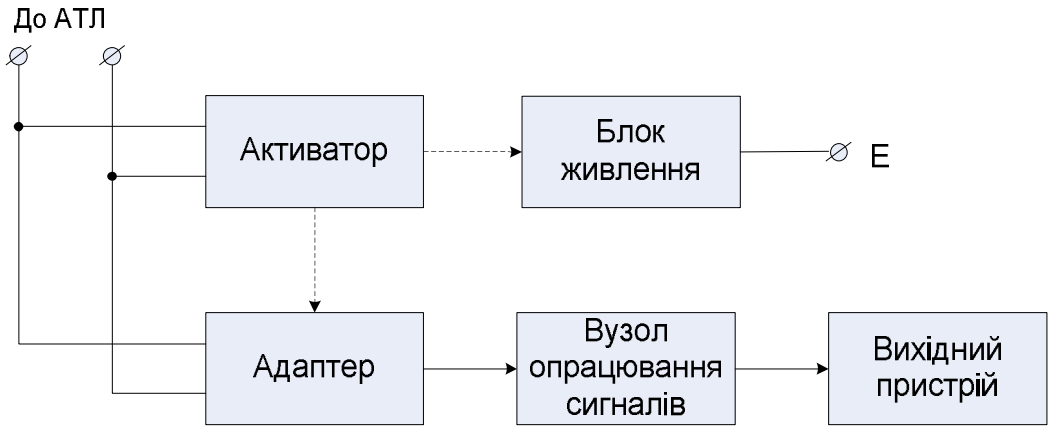

Рис.3. Узагальнена структура засобів техрозвідки, призначених для використання в АТЛ

У телефонних засобах техрозвідки можливі такі способи використання перехоплених сигналів:

– прослуховування розмови у реальному часі;

– запис розмовного сигналу;

– ретрансляція 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, а для ретрансляції – радіопередавач, що реалізує випромінювання перехоплених з телефонної лінії сигналів в ефір з подальшим їхнім прийманням на радіоприймач. Для приховування радіоканалу можуть використовуватися спеціальні формати кодування та модуляції, зокрема технологія шумоподібних сигналів.

Живлення телефонних закладок може здійснюватися двояко – безпосередньо від АТЛ або від автономного джерела. У першому варіанті 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 володіє протилежними властивостями.

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

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 являє собою навиту на розрізане феритове кільце котушку. При охопленні кільцем АТЛ відбувається перетворення електромагнітних коливань, створених проходженням розмовного струму по лінії в електричні коливання, що після підсилення надходять на пристрій відтворення чи запису.

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.

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 ускладнює його виявлення (рис. 4, а). Послідовний адаптер під'єднується в розрив одного з проводів телефонної лінії (рис. 4, б). Має вхідний опір 200....500 Ом і значну вхідну ємність, що полегшує його виявлення [7].

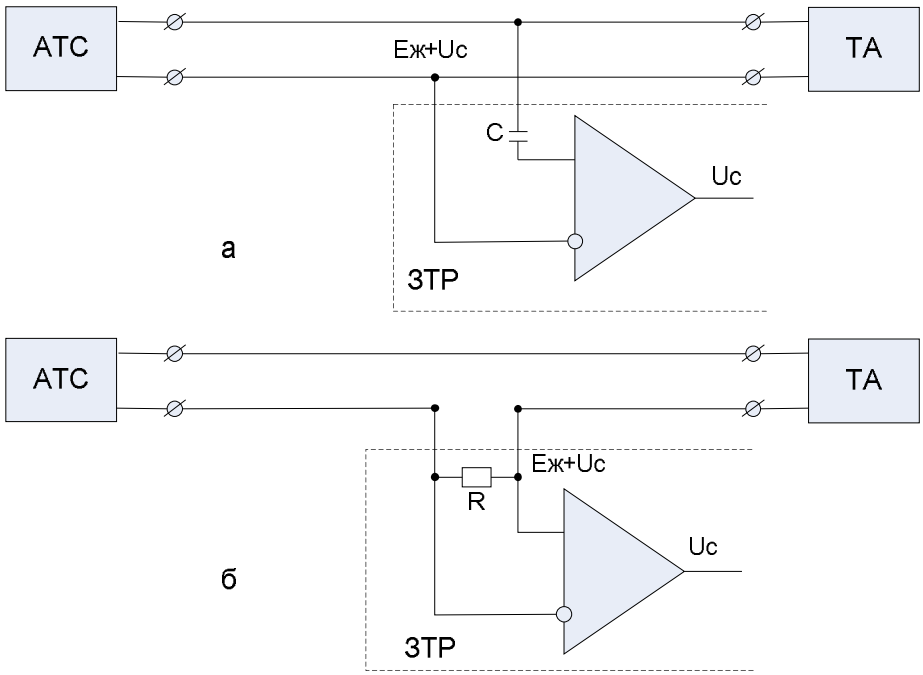

Рис.4. Паралельне (а) та послідовне (б) під'єднання ТЗ до АТЛ

Наприклад, комбінований телефонний радіопередавач під'єднується до телефонної лінії паралельно, а живлення надходить від телефонної лінії (споживаний струм 3...5 мА). Якщо покладена трубка на телефонному апараті, передається акустична інформація з приміщення, в

якому встановлений радіопередавач, якщо знята трубка, радіопередавач переходить у режим трансляції телефонних переговорів, що проходять по цій лінії [7].

4. Прослуховування приміщень через абонентські телефонні лінії. Під'єднаний до АТЛ телефонний апарат у режимі очікування виклику (покладена слухавка) утворює технічні канали витоку акустичної інформації, яка циркулює у приміщенні. Причиною виникнення сигналу витоку інформації (небезпечного сигналу) є так званий мікрофонний ефект, що проявляється у небажаному паразитному перетворенні акустичних звукових коливань на електричні сигнали деякими елементами телефонного апарата – електромагнітним дзвінком, електронною і телефонною капсулою. Крім того, корпус апарата є додатковим резонуючим пристроєм.

У режимі очікування до абонентської телефонної лінії під'єднаними є лише елементи дзвінкового кола, а телефонна і мікрофонна капсули – гальванічно від'єднані. Тому найнебезпечнішим джерелом мікрофонного ефекту стосовно рівня сигналу витоку є електромагнітний дзвінок телефонного апарата. Будучи електромеханічним перетворювачем із дуальними властивостями, електромагнітний дзвінок перетворює не лише електричні сигнали на механічні коливання (основний режим роботи), але і навпаки, через коливання якоря дзвінка під дією акустичних коливань в його обмотці, що розташована в полі постійного магніту, виникає електрорушійна сила електромагнітної індукції. Як показали дослідження [7], для деяких типів телефонних апаратів ЕРС, що наводиться в телефонній лінії, може досягати кількох мілівольт.

Перехоплення інформаційних сигналів, що виникають в елементах дзвінкового кола, можливе за допомогою гальванічного під'єднання до телефонної лінії спеціальних високочутливих низкочастотних підсилювачів. Проте внаслідок малої амплітуди сигналів дальність перехоплення інформації, як правило, не перевищує декількох десятків метрів.

Щоб зменшити рівень шумів у лінії а, отже, підвищити якість і дальність перехоплення інформації, низкочастотний підсилювач під'єднують до лінії через пристрій аналізу стану телефонної лінії, що включається в розрив телефонної лінії [7]. Цей пристрій при покладеній трубці телефонного апарата відключає його від телефонної лінії і АТС, а оскільки опір розв'язки перевищує 20 Мом, вплив завад із боку АТЛ практично усувається. У разі підняття слухавки чи появи сигналів виклику пристрій від'єднує спеціальний низкочастотний підсилювач і під'єднує телефонний апарат до лінії АТС.

Для істотного збільшення дальності перехоплення інформації використовують метод "високочастотного нав'язування", який має два варіанти реалізації – послідовний і паралельний. При застосуванні цього методу у послідовному варіанті в один із проводів телефонного кабелю щодо деякого спільного провідника (наприклад, проводу заземлення чи труби опалення) вводиться високочастотний гармонічний сигнал з частотою від 50 кГц до 1 МГц. Високочастотне коливання, проходячи через елементи дзвінкового кола телефонного апарата, модулюється акустичним сигналом. Отже, електромагнітний дзвінок виконує роль самовільного амплітудного модулятора, а високочастотне коливання – несучої модульованого сигналу. Приймальна частина приладу під'єднується до іншого проводу телефонного кабелю та спільного провідника. Амплітудний детектор дає змогу отримати низькочастотну огинаючу для подальшого підсилення і запису. Не зв'язані електрично, але близько розташовані елементи конструкції телефонного апарата, за рахунок явища індукції проводять високочастотні сигнали. Для якісної роботи подібного пристрою необхідно зменшувати взаємний індуктивний вплив проводів, тому подання у лінію високочастотного коливання та прийом промодульованого сигналу здійснюються екранованим кабелем.

Суть методу "високочастотного нав'язування" у паралельному варіанті полягає у такому. Завдяки високій частоті сигнал "нав'язування" може проходити не лише у дзвінкове коло, але й у мікрофонне і телефонне кола та модулюватися інформаційним сигналом, що виникає внаслідок акустоелектричних перетворень. Оскільки нелінійні або параметричні елементи телефонного

апарата для високочастотного сигналу, як правило, є неузгодженим навантаженням, промодульований мовним сигналом високочастотний сигнал буде відбиватися від нього і поширюватися в зворотному напрямку по лінії. Далі відбитий високочастотний сигнал приймається й опрацьовується спеціальним приймальним пристроєм, що також під'єднаний до телефонної лінії (рис.5). Пристрій аналізу стану телефонної лінії виконує функції, розглянуті вище.

Дальність перехоплення інформації у разі використання методу "високочастотного нав'язування" може становити декілька сотень метрів.

Поряд із розглянутими електроакустичними каналами витоку інформації для прослуховування розмов у приміщеннях застосовуються спеціальні телефонні закладки, які ще називають виносними мікрофонами. Зрозуміло, що встановлення таких пристроїв вимагає фізичного доступу в приміщення.

Спільною особливістю виносних мікрофонів є те, що вони передають інформацію по телефонних лініях без випромінювання в ефір, причому передаваний сигнал може додатково модулюватися чи навіть перетворюватися у цифрову форму із подальшим кодуванням, що запобігає її перехопленню прямим прослуховування лінії. Для додаткового маскування може використовуватися накопичення і стискання даних і швидке передавання у визначений час або за командою приймача.

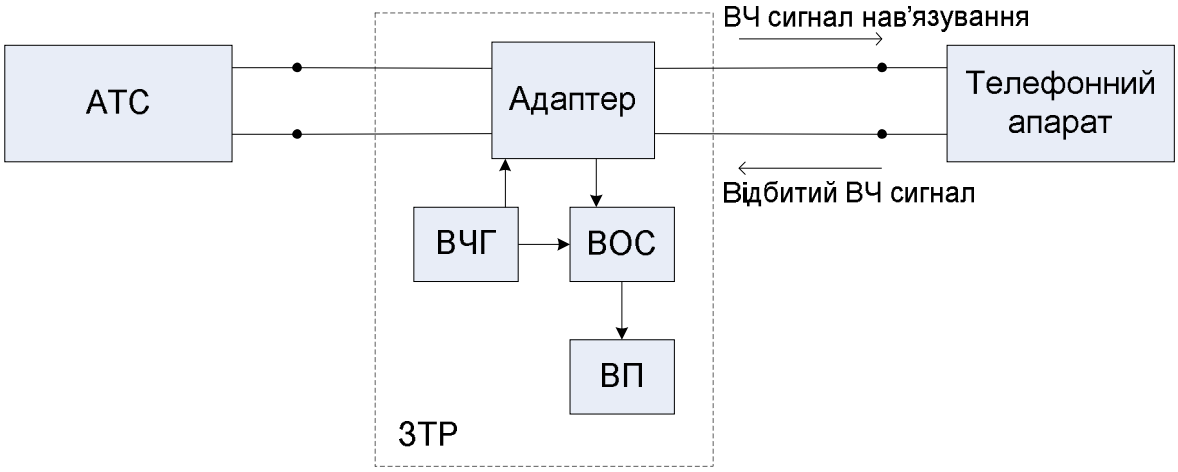

Рис.5. Схема реалізації методу високочастотного нав'язування:
ВЧГ – високочастотний генератор; ВОС – вузол опрацювання сигналів; ВП – вихідний пристрій

Телефонні закладки можуть мати живлення від телефонної лінії або мати автономне живлення. При живленні від телефонної лінії термін їхньої служби практично необмежений, але їх легше знайти через додаткове споживання струму і внесення додаткового опору. Виносні мікрофони з автономним живленням складніше виявляти і вони можуть працювати, крім телефонних ліній, так само на лініях пожежно-охоронної сигналізації, але термін їхньої служби обмежений ємністю елементів живлення.

Принцип роботи виносних мікрофонів простий: якщо на телефонному апараті покладена трубка (на лінії висока напруга) виносний мікрофон сприймає акустичні коливання в приміщенні і передає їх на лінію. Приймання сигналу можливо вздовж усієї траси АТЛ від телефону до АТС. Для приймання сигналів можна використати під'єднаний паралельно до телефонної лінії підсилювач з великим вхідним опором. При знятті трубки на телефонному апараті чи при надходженні на телефонний апарат сигналу виклику від АТС виносний мікрофон припиняє передавання сигналів на телефонну лінію й очікує звільнення лінії (відкладення слухавки).

Найдосконалішим засобом техрозвідки цього призначення є виносний мікрофон з активацією і використанням телефонної лінії в стандартному режимі. Такий пристрій ще називають монітором приміщення по телефонній лінії або “телефонним вухом”.

Встановлюється пристрій між телефонним апаратом і АТЛ, а тому контролює сигнали від АТС. Для прослуховування приміщення здійснюється активація монітора через телефонну мережу.

Активація пристрою “телефонне вухо” відбувається за таким алгоритмом:

– набір номера телефону абонента, приміщення якого прослуховується;

– утримування АТЛ у режимі виклику обмежений час; монітор блокує надходження кількох перших імпульсів виклику (гудків) на телефонний апарат;

– завчасна відмова виклику до підіймання слухавки, наприклад, після трьох гудків;

– поновний набір номера і очікування спрацювання монітора (під’єднання виносного мікрофона до АТЛ);

– передавання звукової інформації на телефон, з якого здійснюється активація.

Отже, з погляду роботи АТС робота монітора відбувається у стандартному режимі телефонної розмови. Прослуховування приміщення відбувається через мікрофон монітора з передаванням в канал зв’язку, тобто відбувається “віртуальне” підняття слухавки.

Монітор є “прозорим” для звичайних дзвінків, хоча привносить певну затримку на етапі встановлення з’єднання внаслідок “проковтування” кількох перших імпульсів виклику. Практика показує, що такий алгоритм забезпечує високий рівень маскування монітора і ускладнює виявлення факту його встановлення.

5. Класифікація методів захисту інформації у телефонних мережах. Характеристика засобів виявлення та знищення телефонних закладок. Сьогодні на ринку є доволі широкий асортимент засобів захисту інформації в телефонних мережах. За призначенням і функціями захисту ці засоби можна поділити на такі категорії:

– виявлення несанкціонованих під’єднань до АТЛ;

– знищення засобів техрозвідки, під’єднаних до АТЛ;

– забезпечення конфіденційності телефонних розмов;

– захист від прослуховування приміщень засобами телефонного зв’язку;

– запобігання несанкціонованому використанню ресурсів телефонного зв’язку.

Наведена класифікація є умовною у тому сенсі, що деякі засоби захисту можуть одночасно виконувати кілька функцій із наведеного переліку.

Залежно від застосованого методу вимірювання та контрольованих параметрів засоби виявлення несанкціонованих під’єднань до АТЛ можна поділити на три класи:

– прилади контролю сигналів у абонентській телефонній лінії (підсилювачі низькочастотних сигналів, індикатори високочастотних коливань, детектори модульованих сигналів);

– вимірювачі нормалізованих параметрів АТЛ (напруги і струму, навантажувальної характеристики, імпедансу);

– пристрої виявлення аномалій як реакції телефонних закладок на спеціальні зовнішні стимули (вимірювання асиметрії, нелінійності, неоднорідності).

Засоби виявлення несанкціонованих підключень можуть працювати у сторожовому (завжди увімкнені) та пошуковому режимах. Крім того, деякі методи вимірювань, що застосовуються у пошукових пристроях, вимагають від’єднання контрольованої ділянки АТЛ від АТС (так званий знеструмлений режим). Це стосується пристроїв другого і третього класу.

Засоби виявлення несанкціонованих під’єднань, що належать до першого класу, дають змогу:

– прослуховувати низькочастотні сигнали в телефонній лінії в контексті його кореляції із акустичними сигналами в приміщенні з метою виявлення технічних каналів витоку, зумовлених мікрофонним ефектом чи виносними мікрофонами);

– виявляти сигнали високочастотного нав’язування у послідовному та паралельному варіантах реалізації;

– демодулювати сигнали різних видів модуляції та встановлювати зв’язок із акустичними сигналами в приміщенні.

Принцип дії засобів другого класу наведеної класифікації полягає у виявленні відмінностей нормалізованих параметрів абонентських телефонних ліній за відсутності та наявності несанкціонованих під’єднань до них. Серед нормалізованих параметрів є як активні величини (напруга і струм в режимі покладеної і піднятої слухавки), так і низка пасивних величин (опір постійному струму, опір ізоляції, ємність, індуктивність та активний опір на частоті зондувального сигналу). Треба зазначити, що прилади цього класу представлені спеціалізованими вимірювачами напруги, струму, опору та складових імпедансу, які адаптовані до вимірювань у проводових лініях із введеною в схему вимірювань необхідною комутацією, автоматизацією, інтерпретацією результатів вимірювань тощо [7]. Оскільки виявляюча здатність засобів контрою нормалізованих параметрів АТЛ обмежується природним розкидом параметрів реальних ліній, то більша достовірність досягається у разі їхнього використання у сторожовому режимі, а не у пошуковому із зіставленням заміряних параметрів із раніше одержаними на конкретній лінії чи середньостатистичними значеннями “чистих” ліній.

Третій клас засобів контролю телефонних ліній представлений насамперед імпульсними рефлектомірами та нелінійними локаторами проводових комунікацій.

Імпульсні рефлектометри призначені для виявлення неоднорідностей хвильового опору аналізованої лінії. Їхній принцип дії ґрунтується на подаванні в лінію імпульсного сигналу і прийманні відбитого від неоднорідності лінії сигналу. За запізненням відбитого сигналу за відомих параметрів лінії можна визначити відстань до неоднорідності, зумовленої деякою аномалією, наприклад, дефектом (обривом, коротким замиканням) чи несанкціонованим підключенням. Враховуючи відмінності хвильового опору різних типів ліній, на практиці кожна конкретна лінія вимагає калібрування приладу. Застосування імпульсних рефлектометрів ефективне, якщо “зберігати образ” завідомо “чистої” конкретної лінії і виконувати порівняння з поточними результатами при періодичному її контролі. Як показують дослідження [7], паралельні телефонні закладки із вхідним імпедансом в декілька десятків кОм не виявляються рефлектомірами, що пов’язано із обмеженою чутливістю.

Нелінійні локатори проводових ліній, засновані на виявленні в лінії гармонійних складових випробувального сигналу, викликаних під’єднанням до неї пристроїв з нелінійним вхідним імпедансом. Вимірювачі асиметрії є особливо ефективними у виявленні послідовних телефонних закладок. Їхній вхідний вимірювальний блок побудований за мостовою схемою, що забезпечує високу чутливість (можливе виявлення послідовних закладок із опором близько сотні Ом) [8].

На ринку є доступними комплексні системи моніторингу телефонних ліній, що забезпечують виявлення несанкціонованих під’єднань до АТЛ за трьома класифікаційними ознаками.

Робота пристроїв знищення ґрунтується на електричному “випалюванні” підключених до АТЛ засобів техрозвідки. Пристрої цієї категорії видають в телефонну лінію один або кілька імпульсів високої напруги (діапазоні понад 1000 В), що призводить до руйнування напівпровідникових елементів вхідних каскадів телефонних закладок і блоків живлення, гальванічно під’єднаних до лінії. При використанні цих приладів, необхідно відключити від лінії телефонний апарат, оскільки він може так само вийти з ладу. Знищення паралельно під’єднаних телефонних закладок здійснюється при розімкненні, а послідовно під’єднаних – при закороченні телефонної лінії на віддаленому кінці. Метод також ефективний і для знешкодження безконтактних пристроїв. Якщо в лінії встановлений, наприклад, індуктивний адаптер для диктофона, то зазвичай виходить з ладу не сам адаптер, а вхідний підсилювач диктофона. До пристроїв, які реалізують цей метод, належать “ПТЛ-1500”, “КС-1300”, “Кобра” [9].

6. Методи та засоби забезпечення конфіденційності телефонних переговорів. По телефонних каналах доволі часто передається конфіденційна інформація. Це пов'язано із оперативністю та зручністю використання телефонного зв'язку. Тому пряме перехоплення телефонних переговорів є дуже результативним із погляду несанкціонованого одержання інформації [10]. Сьогодні для забезпечення конфіденційності в каналах телефонного зв'язку використовують три методи:

- накладання маскувальних перешкод на телефонні повідомлення;
- приховування семантичного змісту повідомлення за допомогою скремблювання, тобто перестановок часо-частотних параметрів сигналів мовлення;
- оцифровування телефонного сигналу, його компресія та шифрування.

Можна виділити три варіанти реалізації методу накладання маскувальних перешкод на телефонні повідомлення залежно від:

- способу введення у лінію маскувальних сигналів (послідовний чи паралельний);
- спектральних та часових характеристик маскувальних сигналів.

За першим варіантом маскування здійснюється введенням у кожен із проводів АТЛ відносно додаткового спільного провідника узгоджених псевдовипадкових імпульсних послідовностей, спектральна густина потужності яких зосереджена у тональному діапазоні (300-3400 Гц). Ефективність маскування досягається лише для послідовних телефонних закладок, оскільки у послідовних закладках, як і у телефонному апараті, такі перешкоджаючі сигнали компенсують один одного, не створюючи завад для сигналу мовлення.

У другому варіанті для маскування використовують білий шум або псевдовипадкові імпульсні послідовності із надтонального 6–20 кГц та ультразвукового (понад 20 кГц) діапазонів. Параметри перешкоджаючих маскувальних сигналів підбираються так, щоб ці сигнали, з одного боку, не погіршували якість телефонних розмов, а з іншого – після проходження селективних кіл адаптера їхній рівень виявився достатнім для придушення корисного сигналу. Негативний вплив перешкод на телефонний апарат усувається спеціальним низкочастотним фільтром із граничною частотою 3,4 кГц. Встановлені на міських АТС смугові фільтри виконують аналогічну роль, а от подібна фільтрація у телефонних закладках ускладнюється габаритами низькочастотних фільтрів. До цієї категорії пристроїв захисту належить Sel SP-17/D [11].

Пристрої, що реалізують описані варіанти маскування, необхідно встановлювати на телефонних лініях кожного із абонентів, при цьому сигнал мовлення та АТС та магістральних лініях цілком незахищений від підслуховування. У цьому сенсі очевида перевага на боці так званих односторонніх пристроїв маскування – третього варіанта реалізації методу накладання маскувальних перешкод на телефонні повідомлення. Принцип дії таких пристроїв полягає у зашумленні телефонного тракту аналоговим або цифровим сигналом, спектр якого перекриває смугу частот телефонного повідомлення. Пристрій може відфільтрувати заваду із вхідного повідомлення, оскільки її параметри відомі. Однак нестабільність параметрів телефонного тракту ускладнює виділення телефонного повідомлення на тлі переважаючих завад. Розв'язання цієї задачі стало можливим лише із розвитком методів і засобів цифрового оброблення сигналів, зокрема із побудовою на швидкодіючих сигнальних процесорах адаптивних фільтрів, які здатні забезпечити швидку і точну адаптацію до характеристик каналу зв'язку. Як приклад можна назвати пристрій "Туман'' [11].

Захист телефонних переговорів за методом скремблювання забезпечує конфіденційність телефонних переговорів впродовж всього тракту – від абонента до абонента; обидва абоненти повинні мати однакові скремблери. Під скремблюванням розуміють таку зміну характеристик мовного сигналу, щоб скрембльований сигнал ставав нерозбірливим і займав ту саму смугу спектра, що і початковий. Найпростішим, але разом з тим і найменш ефективним скремблером є односмуговий інвертор спектра [11].

Високий рівень захисту забезпечують цифрові скремблери, які виконують такі операції:

– виконують аналого-цифрове перетворення сигналу мовлення;

– здійснюють перетворення у частотну область за алгоритмом швидкого перетворення Фур'є;

– під керуванням криптоблока виконують мозаїчні перестановки у часо-частотній площині;

– здійснюють перетворення у часову область за алгоритмом зворотного швидкого перетворення Фур'є;

– виконують зворотне цифроаналогове перетворення, щоб забезпечити можливість передачі аналоговими АТЛ.

Найвищий рівень захисту від перехоплення телефонних переговорів досягається за допомогою шифрування. Сьогодні використання шифраторів наштовхується на проблему так званої "останньої милі", тобто неспроможність АТЛ доставити до абонента "оцифрований голос" (64 кбіт/с) через обмежену пропускну здатність каналу тональної частоти. Саме тому у шифраторах здійснюється стиснення оцифрованого сигналу мовлення на передачі, з подальшим його шифруванням. Вибір системи формування і розподілу ключів може виявитися важливішим, ніж вибір криптоалгоритму. Для шифрування телефонних повідомлень доцільно використовувати швидкі симетричні алгоритми у потоковому режимі шифрування (наприклад, DES, ГОСТ 28147-89), а для обміну криптографічними ключами – асиметричні, такі, як RSA чи Діффі–Хелмана.

Варто зазначити, що ні скремблери, ні шифратори не захищають телефонну лінії від отримання акустичної інформації з приміщення у перервах між телефонними переговорами [11].

7. Принципи захисту від прослуховування приміщень та запобігання несанкціонованому використанню ресурсів телефонного зв'язку. Прослуховування приміщень відбувається в режимі очікування, тобто при покладеній слухавці. Це, загалом, спрощує реалізацію цієї функції захисту порівняно із забезпеченням конфіденційності. Серед пристроїв захисту цієї категорії розрізняють пасивні та активні.

Пасивні засоби захисту представлені нелінійними розв'язуючими пристроями та загороджувальними фільтрами. Робота нелінійних пристроїв ґрунтується на нелінійних властивостях p-n переходу напівпровідникових діодів. Зустрічне увімкнення діодів унеможливлює проходження в телефонну лінію сигналів малої амплітуди від "мікрофонного ефекту" і практично не впливає на сигнали у режимі телефонної розмови.

Загороджувальні фільтри застосовуються для захисту телефонних апаратів від "високочастотного нав'язування". Найчастіше такі фільтри є LC-фільтрами нижніх частот, смуга пропускання яких розрахована на проходження тональних сигналів і блокування високочастотних. Загороджувальні фільтри вмикаються між АТЛ і телефонним апаратом.

Активні засоби блокування технічних каналів витоку представлені генераторами шуму. Їхня дія ґрунтується на створенні і "закачуванні" в лінію при покладеній трубці шумового сигналу діапазону частот 300–3400 Гц і амплітудою кілька вольт, внаслідок чого:

– створюються перешкоди роботі виносних мікрофонів що використовують телефонну лінію для передавання інформації;

– вмикається система активації запису диктофонів, що змушує їх записувати тільки шум у проміжках між телефонними розмовами;

– маскуються сигнали, що виникають від "мікрофонного ефекту".

До сертифікованих в Україні пасивних засобів захисту, що поєднують фільтр і обмежувач, належить пристрій "Скеля-1", а активні засоби лінійного зашумлення представлені пристроєм "Скеля-2".

Для запобігання несанкціонованому використанню ресурсів телефонного зв'язку, зокрема телефонному шахрайству, використовуються такі способи:

– сигналізація про паралельні під'єднання;

– блокування паралельних під’єднань;
– заборона набору номера;
– кодування доступу до телефонної лінії;
– контроль тривалості використання телефонних послуг.

Сигналізація про паралельні під’єднання здійснюється пристроями пасивного типу, так званими індикаторами стану телефонної лінії. Принцип роботи індикатора ґрунтується на контролі рівня напруги АТЛ. Якщо рівень напруги перевищує пороговий (наприклад 40 В), то давач напруги перебуває у нормальному стані, блокуючи роботу генератора імпульсів. Якщо ж на певній ділянці лінії була піднята трубка із паралельного телефонного апарата або відбувся обрив (більш ніж на 1 секунду), спрацьовує давач напруги, запускається генератор імпульсів і звуковипромінювач подає неперервний звуковий сигнал, що сигналізує про використання чи обрив лінії. При поверненні телефонної лінії в стан очікування (напруга більше за 40 В) індикатор знову переходить у початковий стан [6].

Активний технічний захист телефонної лінії від самовільного під’єднання, на відміну від пасивного, передбачає не лише сигналізацію (звукову чи світлову) про цю подію, але і безпосереднє втручання у встановлення зв'язку із піратського телефонного апарата [6]. Усі типи апаратури, що реалізують активний захист ліній, можуть встановлюватися як на вихідних клемах АТС, так і на боці абонента. Перевагою встановлення захисних пристроїв на кросі АТС є захист абонентської телефонної лінії по всій її довжині навіть у разі її розриву. До переваг індивідуального встановлення пристроїв захисту належать оперативність реагування на випадки самовільних під’єднань, а також невтручання до протоколу роботи АТС.

Найпростішим типом пристрою активного захисту від паралельних під’єднань є блокатор типу “заглушка”. Такий пристрій призначений для захисту АТЛ за тривалої відсутності абонента (відрядження, відпустка тощо). Блокатор типу “заглушка” виконує дві основні функції:

– при спробі набору номера з паралельно під’єднаного апарата здійснює заборону набору шунтуванням лінії;
– при прийманні посилок виклику від АТС (100 В, 25 Гц) пристрій не шунтує лінію (система заборони не вмикається).

Блокатор паралельного під’єднання, що працює у сторожовому режимі (разом з основним телефонним апаратом), виконує такі функції:

– заборона набору номера у разі паралельного набору;
– прозорість при прийманні посилок виклику з АТС (немає шунтування лінії);
– автоматичне від’єднання системи заборони набору номеру при піднятті трубки основного ТА.

Телефонні мережі використовують технологію оперативної комутації каналів, тобто існує етап встановлення з’єднання. Тому блокатори паралельного під’єднання перешкоджають передаванню адресної інформації на етапі встановлення з’єднання, тобто виконують функції заборони набору номера, використовуючи такі способи:

– короткочасний розрив лінії з метою встановлення апаратури АТС у вихідний стан “лінія вільна”, (йдеться про розрив одного з лінійних проводів, що за ДЕСТ 7153 становить не менше ніж 400–800 мс);
– шунтування лінії резистивно-ємнісною ланкою (за допомогою резистора обмежується амплітуда імпульсів набору номеру, що не дає змоги АТС визначити номер і здійснити з'єднання, а ємність призначена для придушення посилок тонового набору або сигналів мовлення, якщо з'єднання все ж відбулося);
– перешкоди імпульсному і частотному набору номера спотворенням форми імпульсів набору, зменшення їхньої кількості тощо, що не дає змоги однозначно визначити номер і встановити зв'язок.

Блокатори міжміських сполучень унеможливлюють передавання на першій позиції цифри “8’’, яка використовується для виходу на рівень АМТС. Крім того, може використовуватися обмеження формату набору, наприклад, чотрима цифрами (блокування виходу в місто) чи сімома (блокування міжміських сполучень).

Існують також пристрої, які запобігають несанкціонованому використанню послуг телефонного зв’язку в спосіб кодування доступу до телефонної лінії [6]. На підприємствах ефективним може виявитися принцип захисту, що ґрунтується на контролі використання службових телефонів фіксуванням тривалості чи архівацією телефонних розмов.

Висновки. У статті із єдиних позицій виконано всебічний аналіз загроз інформаційній безпеці абонентів телефонних мереж загального користування, описано принципи побудови телефонних закладок і способи несанкціонованого їхнього під’єднання до абонентських телефонних ліній з метою підслуховування телефонних розмов та прослуховування приміщень, у яких розміщений телефонний апарат. Наведено огляд і характеристику методів і засобів технічного захисту засобів телефонного зв’язку. Незважаючи на доволі широкий асортимент засобів захисту АТЛ, високий рівень інформаційної безпеки забезпечується лише за умови використання багаторівневого комплексного захисту із застосуванням різних методів і принципів побудови пристроїв захисту. Нині існує кілька багатофункціональних систем захисту телефонних переговорів, наприклад мікропроцесорні системи STEALTH чи ANTIFLY. Проте вкрай важливо поєднувати технічні засоби захисту із так званими організаційними заходами.

1. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов; под ред. профессора В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия – телеком, 2005. – 647 с. 2. Безопасность информационных технологий. Методология создания систем защиты / В.В.Домарев. – К.:ООО “ТИД ДС”. 2001. – 698 с. 3. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь. 1999.– 368 с. 4. Системы электросвязи: Учебник для вузов / Под ред. В.П. Шувалова. – М.: Радиосвязь. 1987, с. 512. 5. Берлик Б.З., Брискер А.С. и др. Справочник. Городская телефонная связь. — М.: Радио и связь, 1987г. — 280 с. 6. Балахничев И.Н., Дрик А.В., Крупа А.И. Борьба с телефонным пиратством. Мн.: Наш город, 1998г. — 116 с. 7. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия РФ, 1998. – 320 с. 8. Быков С.В. Классификация устройств съема информации в телефонной линии – Новосибирск. Сборник научных трудов НГТУ № 2. – 1999. 9. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах.– М.: Энергоатомиздат, 1996. – 304 с. 10. Кравченко В.Б. Защита речевой информации в каналах связи // Специальная техника, 1999, № 4. 11. Абалмазов Э.И. Новая технология защиты телефонных разговоров // Специальная техника. 1998, № 1. – С. 4 – 8.