УДК 621:395

АНАЛІЗ ЗАГРОЗ ТА ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ТЕЛЕФОННИХ ЛІНІЙ

М. Я. Микитюк

НУ «Львівська політехніка», кафедра захисту інформації
вул. Степана Бандери, 12, Львів, 79013, Україна

У статті описано загальний погляд на проблему несанкціонованого доступу до телефонних ліній. Проаналізовано загрози для інформації, яка циркулює в абонентських телефонних лініях. Описано способи захисту абонентських телефонних ліній, та методи обмеження або унеможливлення фізичного доступу на ділянці абонентських телефонних ліній.

Ключові слова: *телефонний канал, телефонна лінія, абонентська телефонна лінія, технічний захист інформації.*

Постановка проблеми. В загальному комплексі заходів щодо забезпечення національної безпеки держави важливе місце займають заходи, пов'язані із безпосереднім захистом інформації від загроз, реалізація яких може нанести особі, суспільству, державі політичні, економічні, фінансові та інші збитки. Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

1. Здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Незважаючи на позитивні зміни в міжнародній обстановки навколо України, діяльність технічних розвідок іноземних держав із здобування інформації продовжується. Проти України безперервно ведеться розвідка багатофункціональними космічними, повітряними, наземними, морськими системами та комплексами технічної розвідки. Провідні країни світу продовжують модернізувати свої розвідувальні служби, вдосконалюють технічну розвідку, нарощують її можливості.

Наявні можливості технічних розвідок практично вже сьогодні дають змогу забезпечити безперервне спостереження за всією територією України, і у подальшому, засоби технічної розвідки, зокрема космічної компоненти, будуть мати виключно високі характеристики, які дозволять забезпечити постійне стеження за всією територією держави в реальному масштабі часу.

2. Несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування систем обробки інформації.

За умови недостатньої номенклатури засобів обробки інформації та програмного забезпечення вітчизняної розробки в інформаційно- телекомуніка-

ційних системах широко використовуються продукти іноземного виробництва, які здебільшого не мають об'єктивних оцінок механізмів захисту, а також створюють передумови впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило широке розгортання інформаційно-телекомунікаційних систем, різке збільшення обсягів інформації, яка обробляється, зберігається в цих системах, значне збільшення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів тощо.

При цьому, за відсутності конкурентоспроможних вітчизняних зразків перевага надається інформаційним технологіям та технічним засобам обробки інформації іноземного виробництва, які здебільшого не забезпечують захист інформації, а також створюють передумови неконтрольованого використання спеціальних програмних та апаратних засобів ("закладних пристроїв").

У світі зберігається тенденція поширення масштабів комп'ютерної злочинності, розповсюдження комп'ютерних вірусів, насамперед, з

використанням Інтернет, істотно зростає небезпека наслідків неправомірних дій, технічних і технологічних помилок та збоїв при застосуванні інформаційно-телекомунікаційних систем, що є особливо актуально в умовах широкого входження вітчизняних інформаційно-телекомунікаційних систем до глобальних.

Окремими державами реалізується "концепція інформаційного протиборства , яка полягає в реалізації заходів щодо спеціального впливу на інформаційну інфраструктуру з метою ураження (знищення) інформаційних ресурсів та руйнування системи управління в сферах оборони, економіки, безпеки, фінансів тощо.

3. Витік інформації з обмеженим доступом технічними каналами внаслідок виникнення побічних електромагнітних випромінювань і наводів, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об'єкту інформаційної діяльності.

В процесі здійснення інформаційної діяльності для зберігання, обробки та передавання інформації, в тому числі й інформації з обмеженим доступом, широко використовуються технічні засоби різного призначення (засоби обчислювальної техніки, оргтехніка, засоби зв'язку, автоматизовані системи тощо). На об'єктах інформаційної діяльності здійснюється обговорення службових питань за різними напрямками діяльності установи, в ході яких може озвучуватися інформація з обмеженим доступом.

Проте, окремі фізичні процеси, що відбуваються в технічних засобах та під час обговорення інформації, та інші фактори створюють об'єктивні передумови для появи технічних каналів витоку інформації, що зумовлює необхідність реалізації заходів зі створення комплексів (систем) технічного захисту інформації, спрямованих на запобігання витоку інформації цими каналами.

Аналіз останніх досліджень та публікацій. Питання повязані з аналізом загроз інформації і її безпеки в телефонних лініях висвітлив у своїх публікаціях Хома В.В. Також, значний вклад в даній проблематиці, зробив та представив у

своїй праці С.О. Ємельянов. Також дану проблематику описала у своїй праці Мелешко О.О.. Питання захисту та безпеки телефонних ліній вивчали такі науковці, як: Цибуляк Б. З. та Хорев А.А.. Попри стрімкий розвиток інших технологій зв'язку, традиційний телефонний зв'язок і надалі залишається одним з найпоширеніших і водночас найвразливіших. Тому проблематика пов'язана з безпекою телефонних ліній потребують подальших досліджень.

Мета статті — дослідити основні загрози та способи захисту телефонних ліній щодо унеможливлення та запобігання несанкціонованого доступу до них.

Виклад основного матеріалу дослідження. ***Аналіз загроз для інформації в телефонних мережах зв'язку.*** Завдання захисту інформації під час переговорів, які ведуться у приміщенні на контрольованій території, може бути вирішене ціною певних витрат та незручностей для осіб, що приймають участь у переговорах. Значно складніше забезпечити захист інформації в каналах зв'язку, які за своєю суттю завжди більше піддані зовнішнім загрозам. Телефонний зв'язок є одним з найбільш незахищених.

Загроза конфіденційності проявляється у:

- підслуховуванні телефонних розмов (піднята телефонна трубка);
- прослуховування приміщень, у яких знаходиться телефонний апарат.

Підслуховування телефонних розмов можливе за допомогою досить простих технічних засобів, оскільки голосові повідомлення передаються у відкритому вигляді. Утворення елементами телефонного апарату *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.

У телефонних мережах обмін інформацією між абонентськими термінальними пристроями, наприклад, телефонними апаратами (ТА), відбувається через телефонний тракт, що утворюється за допомогою фізичного з'єднання абонентської телефонної лінії (АТЛ), елементів комутаційного поля автоматичної телефонної станції (АТС), каналів з'єднувальних ліній та систем передачі (рис. 1).

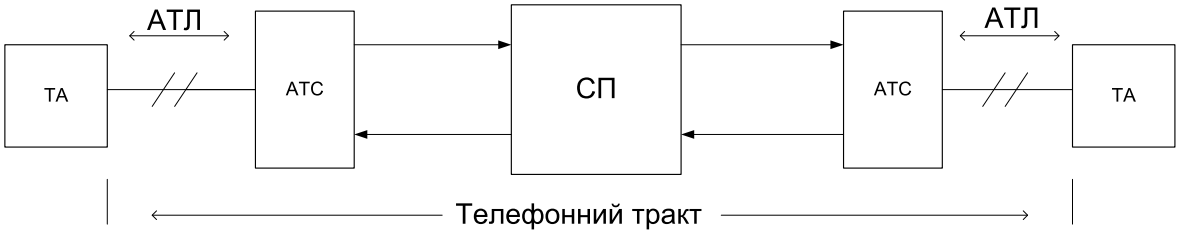

Рис. 1. АТЛ як складова телефонного тракту

Абонентська телефонна лінія є неоднорідною за своєю будовою — у стандартному варіанті в її складі можна виділити три ділянки (див. рис. 2).

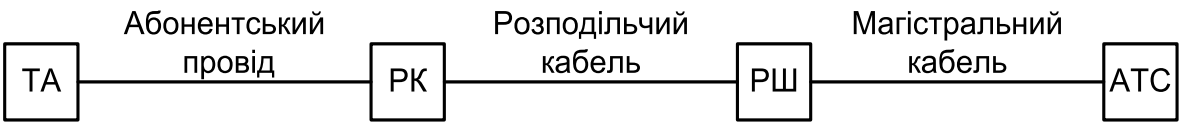

Рис. 2. Елементи телефонної лінії: РК—розподільна коробка, РШ—розподільна шафа

Ділянка ТЛ у вигляді прокладеного під землею магістрального багатопарного телефонного кабелю від АТС до розподільної шафи є найдовшою. Далі від розподільної шафи до внутрішньої розподільної коробки ТЛ має продовження також у вигляді багатопарного телефонного кабелю, але порівняно із магістральним меншої ємності та протяжності. Від розподільної коробки до кожного абонента розводка виконується двопровідним телефонним проводом марки ТРП або ТРВ.

Довжина магістрального кабелю становить кілька кілометрів (у середньому 2 — 3 км), розподільного — приблизно сотні метрів, а абонентського проводу порівняно невелика — кілька десятків метрів.

Загрози для інформації реалізуються через під'єднання до ТЛ засобів технічної розвідки. На ділянці багатопарних телефонних кабелів таке під'єднання малоймовірне (особливо це стосується магістральної ділянки, на якій кабель прокладено у підземних комунікаціях). Найпростішим, а значить, і вірогідним, є під'єднання до відкритих ділянок абонентської проводки, телефонної розетки, телефонного апарата, розподільної коробки чи шафи (рис.2).

Аспекти захисту телефонних ліній та телефонних апаратів. При захисті телефонних ліній та телефонних апаратів, як каналів витоку інформації необхідно враховувати:

- ТА (навіть при покладеній трубці) може бути використаний для перехоплення акустичної мовної інформації з приміщень, у яких він встановлений, тобто для підслуховування розмов у цих приміщеннях;
- ТЛ, що проходять через приміщення, можуть використовуватися як джерела живлення акустичних закладок, встановлених в цих приміщеннях, а також для передачі перехопленої інформації;
- перехоплення (підслуховування) телефонних розмов шляхом гальванічного або через індукційний датчик підключений до ТЛ закладок (телефонних ретрансляторів), диктофонів і інших засобів несанкціонованого знімання інформації.

ТА має декілька елементів, здатних перетворювати акустичні коливання в електричні сигнали (мікрофонний ефект). До них відносяться коло дзвінка, телефонний і, звичайно, мікрофонний капсулі. За рахунок електроакустичних перетворень в цих елементах виникають інформаційні (небезпечні) сигнали.

При покладеній трубці телефонний і мікрофонний капсулі гальванічно відключені від ТЛ і при підключенні до неї спеціальних високочутливих низькочастотних підсилювачів можливе перехоплення небезпечних сигналів, що виникають в елементах кола дзвінка. Амплітуда цих небезпечних сигналів, як правило, не перевищує часток мВ.

При використовуванні для знімання інформації методу «високочастотного нав›язування», не дивлячись на гальванічне відключення мікрофону від телефонної лінії, сигнал нав›язування завдяки високій частоті проходить в мікрофонне коло і модулюється по амплітуді інформаційним сигналом. Отже, в телефонних апаратах необхідно захищати як коло дзвінка, так і коло мікрофону.

Для захисту телефонних апаратів від витоку акустичної (мовної) інформації через електроакустичний канал використовуються як пасивні, так і активні методи і засоби.

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

- сигналізація про нелегальні підключення;
- блокування нелегальних підключень;
- заборона набору номера;
- кодування доступу до телефонної лінії;
- контроль тривалості використання телефонних послуг.

Одержання інформації про нелегальне підключення до телефонної лінії є ключовим у роботі як пасивних пристроїв технічного захисту, які лише сигналізують про факт такого підключення, так і для пристроїв активного захисту, що використовують таку інформацію для блокування телефонної лінії з метою унеможливлення набору номера із піратського телефонного апарата.

Основні технічні способи одержання інформації про стороннє підключення до лінії базуються на таких ознаках:

- відсутність напруги в телефонній лінії;
- зниження в 3-4 рази напруги живлення в лінії при покладеній трубці телефонного апарата;
- піддзвонювання телефонного апарата, зумовлене імпульсами набору номера із піратського ТА;
- наявність частотних посилок DTMF коду при покладеній трубці ТА;
- непроходження виклику із АТС на телефонний апарат.

Більш складні способи виявлення несанкціонованого підключення базуються на контролі за резонансним включенням пристроїв до абонентського шлейфу. Під резонансним настроюванням телефонного апарата розуміють робота обладнання АТС із конкретним телефонним апаратом. У випадку підключення телефону з іншими параметрами, чи приєднанні в іншому місці шлейфу „АТС-абонент", відбувається неузгодженість (непопадання в резонанс), що приводить до спрацьовування індикатора нерезонансного підключення.

Параметри, що характеризують стан узгодження, можуть бути наступними:

- еквівалентний опір ТА при піднятій трубці;
- еквівалентний опір при покладеній трубці;
- індивідуальні параметри номеронабирача;
- комплексний опір розмовної частини;
- струм споживання при виклику;
- струм споживання в розмовному режимі;

Методи обмеження фізичного доступу до ТЛ

Крім, власне, методів захисту інформації від перехоплення телефонними закладками, вже під'єднаними до ТЛ, важливими є методи і засоби, націлені на запобігання встановленню телефонних закладок, виявлення факту їх під'єднання до ТЛ та фізичного знищення всіх несанкціоновано під'єднаних до ТЛ пристроїв. Оскільки використання телефонних закладок загрожує конфіденційності, то спільними є методи захисту, основані як на обмеженні фізичного доступу до засобів телефонного зв'язку (запобігання встановленню телефонних закладок), так і на *виявленні несанкціонованих під'єднань* або навіть на фізичному знищенні вже встановлених телефонних закладок контактного типу, наприклад, електричним випалюванням.

Обмеження фізичного доступу до ТЛ передбачає унеможливлення або хоча б ускладнення:

- безпосереднього під єднання зловмисником розвідувальної апаратури до телефонних апаратів чи окремих ділянок ТЛ;
- візуальної розвідки та отримання зловмисником допоміжної інформації про обладнання та організацію зв'язку на об'єкті, що надалі полегшить несанкціоноване під'єднання до ТЛ;
- використання зловмисником для перехоплення інформації електромагнітних полів у навколишньому просторі та наведень в колах живлення і заземлення, що перебувають у межах контрольованої зони.

Цілком очевидно, що застосування цього методу можливе лише в межах контрольованої зони, при цьому на основній протяжності (ділянка міського телефонного кабелю) телефонна лінія перебуває поза зоною адміністративного контролю. Крім того, застосування заходів обмеження фізичного доступу, як правило, є нереальним для абонента, що працює в «блукаючому» режимі.

Несанкціоноване під'єднання та знищення телефонних закладок

Контактні під'єднання до ТЛ змінюють її параметри, а тому принцип дії засобів виявлення несанкціонованих під'єднань ґрунтується на контролі змін параметрів ТЛ та виявленні сторонніх сигналів. Засоби виявлення несанкціонованих під'єднань можуть використовуватися у сторожовому режимі (ТЛ у робочому стані) та під час пошукових робіт (ТЛ у робочому стані або знеструмлена).

Для виявлення несанкціонованих під'єднань до ТЛ, яка перебуває у робочому стані, використовують методи контролю сталої напруги живлення, струму короткого замикання, навантажувальної характеристики, а також низькочастотних сигналів телефонних закладок та сигналів високочастотного нав'язування та накачки.

Арсенал методів виявлення несанкціонованих під'єднань знеструмленої ТЛ значно ширший: вимірювання параметрів імпедансу ТЛ (активного опору, ємності та індуктивності), асиметрії проводів ТЛ, вольт-амперної характеристики ТЛ для визначення нелінійності імпедансу. Крім того, у знеструмленому стані методом імпульсної рефлектометри можна визначати віддаленість до неоднорідностей лінії, привнесених контактними під'єднаннями.

Метод «випалювання» реалізується подаванням в лінію при від'єднаному телефонному апараті високовольтних імпульсів, що призводить до знищення вхідних каскадів пристроїв перехоплення інформації і блоків живлення, гальванічно під'єднаних до лінії.

Висновки. Отже, попри величезний поступ у розвитку телекомунікаційних технологій традиційний телефонний зв›язок і надалі залишається одним із найпоширеніших і затребуваних засобів комунікацій. Серед загроз інформаційної безпеки абонентів телефонного зв'язку найімовірнішими є перехоплення телефонних повідомлень та прослуховування приміщень, оснащених телефонними апаратами. Найчастіше такі загрози реалізуються шляхом несанкціонованого під'єднання засобів технічної розвідки (телефонних закладок) до абонентських телефонних ліній.

В статті проаналізовано основні аспекти, на які необхідно зважати при реалізації захисту телефонного каналу, а також базові методи доступу до телефонної лінії. Показано, що застосування методу обмеження фізичного доступу можливе лише в межах контрольованої зони, а використання методу «випалювання» вимагає додаткових технічних засобів, які електрично знищують пристрій перехоплення інформації.

Подальше дослідження даної проблематики є досить актуальним, оскільки розвиток електротехніки стрімко росте і в умовах сучасності телефонне шахрайство і злочинність набувають все більших обертів.

Список використаних джерел

1. Хома В.В. «Методи і засоби технічного захисту інформації на абонентських телефонних лініях» / Автоматика, вимірювання та керування. — Львів.: Вид-во Нац. ун-ту «Львів. політехніка». — 2009. — № 639. — С. 87—93
2. Ємельянов С. О. «Систематизація методів та засобів технічного захисту інформації в телефонних каналах та лініях зв'язку» / Сучасна спеціальна техніка. - 2011. - № 2. - С. 128-132..
3. Цибуляк Б. З. «Захист інформації від витоку каналами телефонного зв'язку» / Вісник Національного технічного університету України «Київський політехнічний інститут». Сер. : Радіотехніка. Радіоапаратобудування. - 2013. - Вип. 55. - С. 143-148.
4. Мелешко О.О. «Проблеми, які виникають при захисті телефонних ліній» / О.О. Мелешко, І.О. Лебединська, А.В. Палазюк, А.І. Ткачук [Електронний ресурс]. http://www.rusnauka.com/35_OINBG_2010/Informatica/76208.doc.htm

References

1. Khoma V. (2009). Methods and means of technical protection of information on the user's telephone lines / automation, measurement and control. - Lions .: Izd Nat. Univ «Lviv. Polytechnic». № 639. - S. 87-93 (in Ukrainian)
2. Emelyanov C. A. (2011). Organizing methods and technical protection of information in telephone channels and lines / modern special equipment. № 2. - S. 128-132 . (in Ukrainian)
3. Tsybulyak B.Z. (2013). Protecting information from leaking via telephone / Bulletin of National Technical University of Ukraine «Kyiv Polytechnic Institute». Avg. : Radio. Radioaparatobuduvannya. Vol. 55. - P. 143-148. (in Ukrainian)

4. Meleshko O.O. The problems that arise in the protection of telephone lines / O.O. Meleshko, I.A. Lebedynska, A.V. Palazyuk, A.I. Tkachuk [electronic resource]. http://www.rusnauka.com/35_OINBG_2010/Informatica/76208.doc.htm(in Ukrainian)

ANALYSIS OF THREATS AND PREVENTION OF UNAUTHORIZED ACCESS TO THE PHONE LINE

M.Y. Mykytyuk

Lviv Polytechnic National University, Department of Information Security
12, S.Bandera St., Lviv, 79013, Ukraine
mykytyuk.my@gmail.com

This article describes the general approach to the problem of unauthorized access to telephone lines. It analyzes the threats to information which circulates in subscriber telephone lines. We describe how to protect the user's telephone lines, and methods of preventing or limiting physical access to the site of the user's telephone lines.

Keywords: *telephone channel, telephone line, subscription telephone line, technical information security.*

Стаття надійшла до редакції 15.03.2016.
Received 15.03.2016.