УДК 621.396

КОЗУБЦОВ І.М. - *капітан, кандидат технічних наук, доцент кафедри* (військових телекомунікаційних транспортних систем та технічного забезпечення зв'язку) *Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут", м. Полтава;*

КОЗУБЦОВ М.М.

АНАЛІЗ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВ РАДІОМОНІТОРИНГОМ

В статті розглянуто основні відомості про радіомоніторинг каналів витоку конфіденційної інформації в цивільних та спеціалізованих підприємствах та службах.

Радіомоніторинг, конфіденційна інформація, канал витоку інформації

Будь-яке сучасне підприємство при ринковій економіці змушено працювати в умовах конкуренції [1]. При цьому, однак, можлива несумлінна конкуренція, що полягає в порушенні очевидних прав власника на промислову або інтелектуальну власність. Вона виявляється в несанкціонованому оволодінні технології відтворення чужої продукції, торгово-фінансовими секретами, втручаннями в ділову діяльність організації або особисте життя її співробітників.

З відродженням ринку та появою конкуренції з'явилося промислове шпигунство – являє собою несанкціонований доступ до комерційно важливої інформації допомогою розвідувальних технічних систем негласного її знімання, потай встановлених у приміщеннях зацікавлених комерційних об'єктів, де циркулюй конфіденційна інформація [1]. Асортимент цих засобів на сьогоднішній день досить великий і містить у собі різновид радіомікрофонів (закладки телефонні, та іншу спецтехніку), з якісними технічними параметрами з гарною якістю камуфлювання і простотою установки на об'єкті. З їх допомогою можлива передача інформації на відстань до кількох сотень метрів, а тривалість роботи складає від кількох годин до року і навіть більше. Окремі типи пристроїв, підслуховування, взагалі не мають потреби в спеціальній установці а достатньо їх підкинуті в зацікавлене приміщення у будь-який зручний час.

За цих умов звичайно практикумі періодичні перевірки службових приміщень, автомобілів і житлових квартир на наявність радіозакладок стають все менш ефективними. Обумовлено це постійною загрозою підкидання таких пристроїв. Серйозними проблемами є також організація контролю за лояльністю співробітників, що ведуть переговори з використанням стільникових радіотелефонів, а також виявлення побічних випромінювань технічних засобів обробки, збереження і передачі інформації, що експлуатуються на об'єкті. З огляду на вищевикладене сучасна концепція захисту конфіденційної інформації, що циркулює в приміщеннях або технічних системах, комерційного підприємства (об'єкта), вимагає не періодичного, а практично постійно контролю всіх радіовипромінювань у зоні розташування об'єкта [2, 3, 4].

Радіомоніторингові (РМ) ефіру, як середовищу передачі даних у телекомунікаційних системах загального користування, приділяється особлива увага в сучасних вимірювальних технологіях [5,6,7]. Важливим достоїнством РМ є безперервність одержання, вірогідних і актуальних даних, що добуваються. Безперервність досягається сталістю роботи засобів РМ, вірогідність документальним характером інформації, що надходить, а актуальність сучасністю одержання необхідних для приймання рішення даних.

В даний час для РМ використовуються багатоканальні скануючи приймачі. Вони дозволяють здійснювати постійний автоматичний контроль та пошук радіосигналів в заздалегідь заданих частотах Ефектив-

ність і результативність РМ залежать не тільки від наявності дорогої апаратури (частотоміри, індикатори поля, аналізатори спектру, широкосмугові антени, смугові фільтри, малошумлячі антенні підсилювачі, високочастотні кабелі з малими втратами), правильного монтажу, але і від методів роботи, кваліфікації та досвіду радіооператорів. Спостереження за радіоефіром – це постійна напружена робота кваліфікованих фахівців по ідентифікації, вимірюванню параметрів радіосигналів, запису, збереження та обробки інформації, одержаної в процесі проведення радіомоніторингу [8,7,9,10].

Радіомоніторинг здатний вирішити наступні основні задачі по забезпеченню безпеки комерційного об'єкта: виявлення випромінювань радіозасобів несанкціонованого знімання інформації у приміщення об'єкта, та їх локалізацію; контроль дотримання дисципліни зв'язку при використанні співробітниками відкритих каналів радіозв'язку; виявлення інформативних побічних випромінювань, що виникають при роботі засобів оргтехніки, комп'ютерів і т.п.; оцінку ефективності використовуваних на об'єкті технічних засобів захисту інформації; контроль за місцезнаходженням і станом транспортних засобів фірми в реальному масштабі часу з використанням супутникових навігаційних систем; накопичення даних радіоелектронної обстановки в зоні розміщення об'єкту.

В процесі РМ потрібно враховувати сукупність ряду основних умов, без виконання яких не можна забезпечити ефективність проведеного заходу. До цих обов'язкових умов необхідно віднести:

1. Плановість і регулярність проведення радіомоніторингу в зоні об'єкта, оптимальний підбор та розміщення технічних засобів.

2. Обов'язкова наявність спеціальної підготовленості роботи операторів та знання структур систем радіозв'язку, методів передачі інформації, характерних ознак і основних діапазонів роботи радіозасобів негласного знімання інформації.

3. Обов'язкове складання і регулярне відновлення спеціальних карт та таблиць завантаженості радіоефіру в зоні об'єкта, знання частотних діапазонів, режимів роботи і параметрів сигналів "легальних" засобів зв'язку, радіомовлення і телебачення, контрольованих у зоні об'єкта.

4. Ретельний аналіз всіх одержаних у процесі радіомоніторингу даних, порівняння їх з режимом роботи об'єкта та раніше накопиченою інформацією з радіообстановки в оточенні об'єкта.

Розгляд проблем РМ спеціального призначення у відриві від упровадження сучасних вимірювальних технологій у телекомунікаційних системах (ТКС) загального застосування не дає цілісного представлення про взаємозв'язок цих родинних технологій вимірів, спільності і розходжень розв'язуваних задач в області радіочастотного контролю і моніторингу. З цією метою в роботі проводиться класифікація та принцип утворення каналів витоку конфіденційної інформації.

Класифікація технічних каналів радіомоніторингу. У контексті розглянутої проблеми РМ технічних об'єктів захисту інформація (ЗІ) на відстань може передаватися у виді фізичного поля – акустичного, оптичного або електромагнітного. Тобто поле є носієм інформації. Проведення різних методів досліджень компонентів ТКС ґрунтується на поняттях фізичних величин (ФВ), сигналів або процесів. Останнім і є об'єктом РМ або радіочастотного контролю (РЧК). ФВ і сигнал характеризуються матрицею параметрів: багатомірною інтенсивністю, довжиною в часі і просторі. Сигнал є матеріальним втіленням інформації у вигляді фізичного процесу. Якщо зміна ФВ представляється в логічно-структурованому вигляді, то сигнал також буде ФВ із параметрами, що змінюються, і, отже, логічно-структурованим (цифровий сигнал, наприклад). Тому що сигнал передається через деяке середовище, то радіомоніторингові і контролеві піддаються не тільки ФВ об'єкта, а і ФВ, що визначають середовище. Таким чином, виявляючи канали витоку інформації, оператор у цілому зіштовхується з проблемою розпізнавання й оцінки сигналів різної складності.

При розгляді проблеми РМ компонентів ТКС необхідно визначитися з окремими ключовими терміна-

ми, що позиціонують РМ щодо суб'єктів і об'єктів РМ-каналів витоку інформації [11]. Під технічним каналом витоку інформації розуміється фізичний шлях від джерела інформації (рис.1) до зловмисника, за допомогою якого може бути здійснений несанкціонований доступ до конфіденційної інформації. Витік це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, якою вона довірена.

Рис. 1. Структура каналу витоку інформації

Будь-яка система передачі інформації складається з джерела інформації, передавача, каналу передачі інформації, приймача й одержувача зведень. Ці системи використовуються в повсякденній практиці у відповідності зі своїм призначенням і є офіційними засобами передачі інформації, робота яких контролюється з метою забезпечення її надійності, вірогідності безпеки, що виключають неправомірний доступ до інформації з боку конкурентів. Однак існують визначені умови, при яких можливо, утворення системи передачі інформації з однієї точки в іншу незалежно від об'єкта і джерела. При цьому, природно, такий канал у явному вигляді не повинний себе виявляти. За аналогією з каналом передачі інформації такий канал називають каналом витоку інформації. Він також складається з джерела сигналу, фізичного середовища його поширення і приймальні апаратури на стороні зловмисника. Рух інформації в такому каналі здійснюється тільки в одну сторону – від джерела до зловмисника. Таким чином, під каналом витоку інформації мається на увазі фізичний шлях від джерела конфіденційної інформації до зловмисника, по якому, можливі витік або несанкціоноване одержання охоронюваних зведень.

Класифікація каналів витоку інформації, розглянутих як потенційні об'єкти РМ, приведена на рис.2 [12, 13, 14]. Таким чином, радіомоніторинг здійснимо тільки стосовно деяким із загального числа можливих каналів витоку інформації. Поєднуючи малу сукупність каналів загальним поняттям "радіоканалів", розглянемо їхнього різновиду за наступними критеріями - природі утворення, діапазонові випромінювання і середовищу поширення.

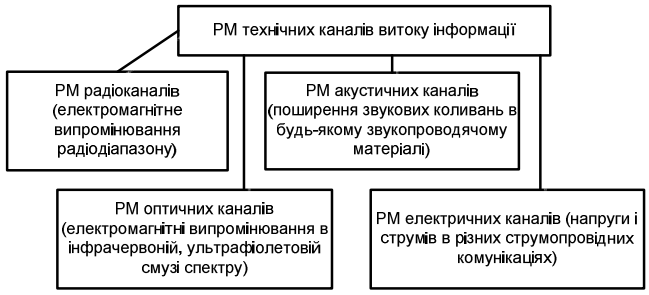

Рис.2. Види РМ технічних каналів витоку інформації

У результаті проведеного узагальнення виділені радіотехнічні канали витоку інформації, класифікація яких приведена на рис.3.

Причини і форми утворення радіоканалів витоку інформації. Причинами утворення радіоканалів витоку інформації, що є по суті можливими каналами РМ, є наступні фактори [11,15,16]: недосконалість елементної бази технічних об'єктів; недосконалість схемних рішень та проектування виробів; експлуатаційний знос і старіння об'єктів РМ; злочинні дії (створення проблемної ситуації, блокування засобів захисту, зміна характеристик об'єктів). Утворенню каналів РМ повинні сприяти визначені просторово-почасові й енергетичні умови, а також відповідні засоби сприйняття і фіксації інформації, як з боку зловмисника, так і з позиції можливого РМ. Стосовно до існуючої практики прояву відзначених умов. визначальну фізичну природу утворення каналів витоку інформації, можна вказати на наступні їхні класифікаційні групи: електромагнітні (включаючи електричні і магнітні); акустичні (включаючи безліч різновидів перетворення і проявів акустичного сигналу); візуально-оптичні.

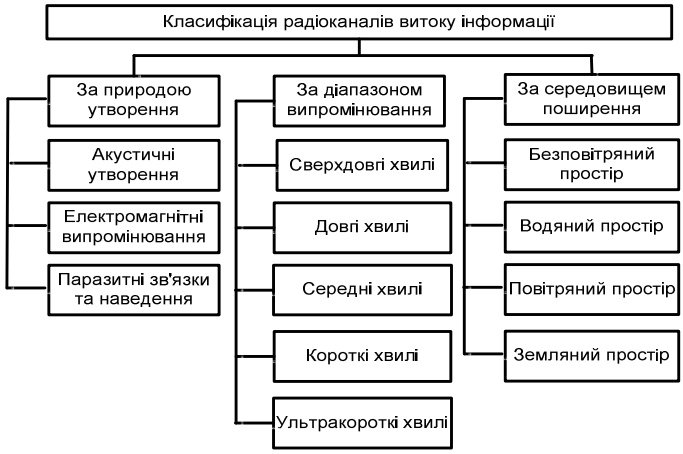

Рис.3. Радіоканали витоку інформації

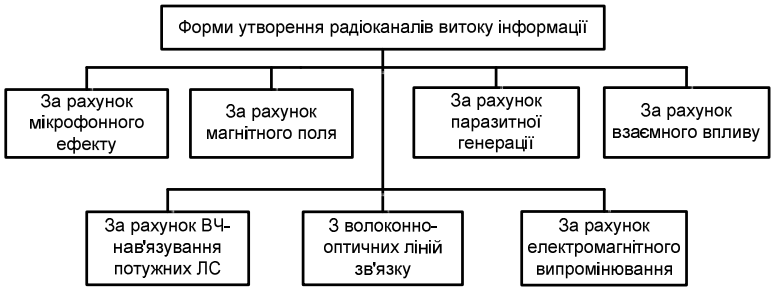

Рис.4. Форми утворення радіоканалів витоку інформації

Відповідно до зазначених фізичних характеристик каналів витоку інформації (і можливого їх РМ) утворяться їхні різновиди, що відрізняються формою утворення радіоканалів. Класифікація останніх приведена на рис. 4.

Розглянемо більш докладно деякі "екзотичні" форми утворення каналів витоку інформації, до яких відносяться канали "взаємного впливу".

Паразитна генерація підсилювачів виникає через неконтрольований позитивний зворотний зв'язок за рахунок конструктивних особливостей схеми або старіння елементів. Самозбудження може виникнути і при негативному зворотному зв'язку, через те, що на частотах, де підсилювач разом з ланцюгом зворотного зв'язку вносить зсув фази на 180° негативний зворотний зв'язок перетворюється в позитивний. Самозбудження підсилювачів звичайно відбувається на високих, частотах, що виходять за межі робочої смуги частот. Частота самозбудження модулюється акустичним сигналом, що надходить на підсилювач, і випромінюється в ефір як звичайним радіопередавачем. Дальність поширення такого сигналу визначається потужністю підсилювача (тобто передавача) і особливостями діапазону радіохвиль. Як захисні міри застосовується контроль підсилювачів на самозбудження за допомогою радіоприймачів (індикаторів поля), що працюють у досить широкому діапазоні частот. Так забезпечує пошук небезпечного сигналу.

Класифікація способів і засобів несанкціонованого знімання інформації. Внаслідок наявності визначених форм утворення радіоканалів витоку інформації (рис.5) зловмисник знаходить адекватні способи її перехоплення. Найбільш поширеним в практиці промислового шпигунства знайшли способи негласного знімання інформації: підслуховування розмов у приміщенні або автомашині за допомогою радіотехнічних засобів знімання інформації (РЗЗІ); контроль проводових телефонних і факсимільних ліній зв'язку з використанням РЗЗІ; контроль радіотелефонів, систем персонального виклику і радіостанцій використанням засобів РМ; знімання інформації з технічних засобів обробки та збереження за допомогою РЗЗІ; дистанційне перехоплення з використанням засобів РМ інформативних побічних випромінювань технічних засобів, експлуатованих на об'єкті; знімання акустичної інформації (мікрофонний ефект). Для реалізації зазначених способів несанкціонованого доступу до каналів витоку інформації зловмисник повинний скористатися адекватними засобами її зняття. Приведені засоби несанкціонованого знімання інформації (рис.5) диференціюються по ряду ознак на

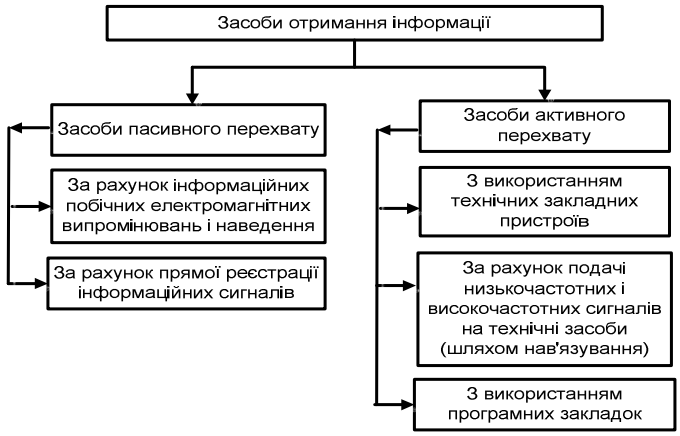

Рис.5. Класифікація можливих засобів зняття інформації з радіотехнічних каналів

більш дрібні підгрупи, що відрізняються специфікою використання конкретних технічних засобів.

Аналіз радіоканалів витоку інформації засобів обчислювальної техніки (ОТ). Засоби ОТ мають радіотехнічні канали витоку інформації рис. 6. У загальному випадку організація і проведення РМ об'єктів ОТ розглядається на рівні підприємства, для якого проектується система захисту інформації (СЗІ). У цьому випадку: вивчаються схеми засобів і систем електроживлення, заземлення, автоматизації, пожежної й охоронної сигналізація, а також інженерних комунікацій; досліджуються інформаційні потоки і технологічні процеси обробки інформації; визначається наявність і технічний стан засобів забезпечення системи ТЗІ; складається приватна модель погроз, і аналізуються можливі канали витоку інформації: зняття інформації з ЕПТ-моніторів; TEMPEST-атака; Soft TEMPEST; ПЕМІ-вірус; порти і схований витік інформації; витік інформації на програмному рівні. На рис. 7 надана коротка наочна характеристика деяких каналів витоку інформації з ЕПТ-моніторів, кабельної системи та ланців електроживлення.

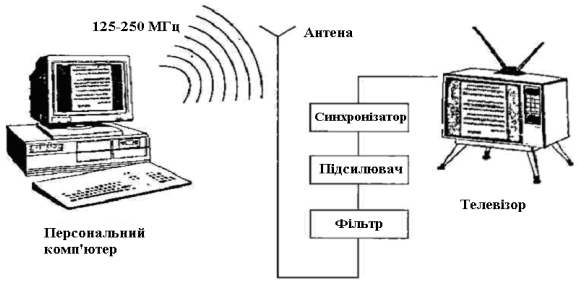

Рис. 6. Схема радіотехнічного зняття інформації з комп'ютера

Цифрові автоматичні телефонні станції як об'єкти радіомоніторингу. Об'єктами радіомоніторингу абонентської телефонної лінії й АТС можуть бути наступні елементи радіоканалів витоку інформації: телефонний апарат, телефонна розетка, розподільні коробки, шафи і власне АТС [16]. Для з'ясування інших місць можливого несанкціонованого знімання інформації розглянемо умовну схему з'єднання зазначених елементів, зображену на рис. 8. Таким чином, крім перерахованих елементів абонентської лінії, зонами РМ є ланцюги електроживлення, магістральний і розподільний кабелю, абонентська проводка, а також радіоефір, локальна комп'ютерна мережа. Радіовипромінювання зазначених елементів мають наступний характер - акустичний, ПЕМІ, паразитні випромінювання. Інші можливі канали витоку інформації будуть визначатися номенклатурою допоміжного і функціонального устаткування організації, інфраструктурою сучасного офісу.

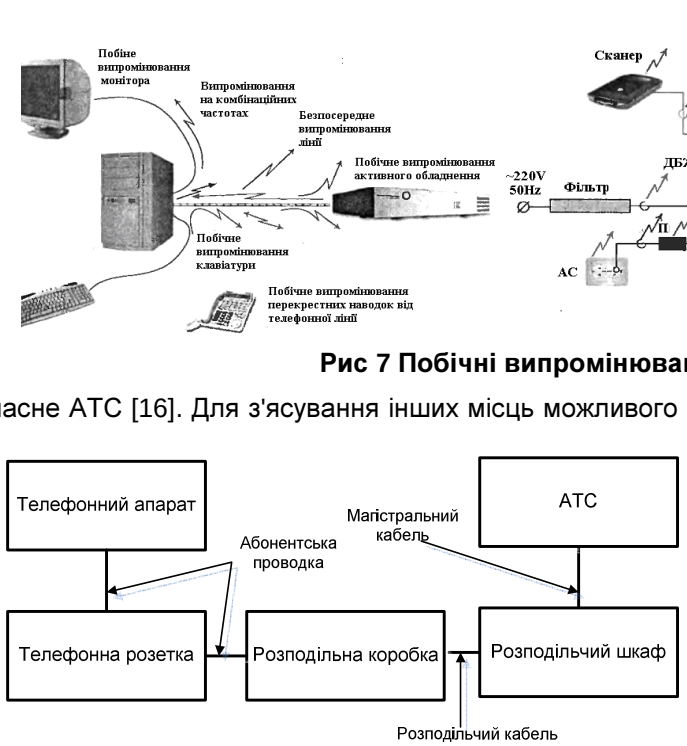

Рис 7 Побічні випромінювання

Рис.8. Схема з'єднання об'єктів РМ АТС

ВИСНОВКИ

Проведений аналіз каналів витоку конфіденційної інформації приватного підприємства дозволяє отримати та напрацювати методологію РМ можливих каналів витоку інформації в спеціалізованих підприємствах та під час роботи з інформацією, що носить конфіденційність та комерційну цінність. Проте забезпечити повну гарантію унеможливлення зняття інформації цілковито не можливо. Доки будуть існувати різні інтереси та зацікавленості в інформації доки буде існувати небезпека в її витоку, незалежно від того від ОТ чи то від самої людини [1].

ЛІТЕРАТУРА

1. *Катарин Ю.Д.* Антишпнонские штучки. Энциклопедия промышленного шпионажа. – СПб: «Полигон», 1999. – 512 с.

2. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределительных корпоративных сетях и системах. – М.: ДМК Пресс. 2002. – 636 с.

3. *Журиленко Б.Е., Хорошко В.А.* Системы и устройства защиты информации (прибор УИП-88 и методика его применения). – К.: НАУ, 2004. - 63 с.

4. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб: БХВ – Петербург, 2003. – 725 с.

5. *Ступак В.С., Долматов С.О.* Основи радіочастотного контролю. – К.: Український державний центр радіочастот, 2004. – 231 с.

6. *Кирюшин Г.В.* Проектирование, развитие и электромагнитная безопасность сетей сотовой связи стандарта GSM. – М: Радио и связь, 2000 – 148 с.

7. *Логинов Н.А.* Актуальные вопросы радиоконтроля в РФ. – М: Радио и связь, 2000. – 240 с.

8. Справочник по радиоконтролю. – Женева: МСЭ, 1995. – 442 с.

9. *Феер К.* Беспроводная цифровая связь. – М.: Радио и связь, 2000. – 520 с.

10. Ергономічне забезпечення розробки і експлуатації військової техніки зв'язку: Звіт про НДР «Ергономіка» (підсумковий). – К.: ВІТІ НТУУ «КПІ», 2006 – 50 с.

11. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К.: 2003. – 214 с.

12. *Хорев А.А.* Способы и средства защиты информации. – М.: МО РРФ, 2000. – 316 с.

13. *Конахович Г.Ф.* Защита информации в телекоммуникационных системах. – К.: «МК-Пресс», 2005. – 288 с.

14. НДТЗІ 1.5-001-2000. Захист інформації. Технічний захист інформації. Радіовиявлювачі. Класифікація. Загальні технічні вимоги.

15. *Зегжда Д.П.* Основы безопасности информационных технологий. – СПб, 2001. – 164 с.

16. *Лагутин В.С., Пеграков А.В.* Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1996. -304 с.

Стаття рекомендована до друку кафедрою (військових телекомунікаційних транспортних систем та технічного забезпечення зв'язку) Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут" м. Полтава.

Рецензент: Кокотов О.В. – кандидат технічних наук, доцент, начальник кафедри бойового застосування систем і засобів засекреченого військового зв'язку Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут", м. Київ.

Контактний телефон 80687122500,
E-mail: venera1@mail.ru

„___" _____ 2008 р. _____ І.М. Козубцов
„___" _____ 2008 р. _____ М.М. Козубцов