УДК 004.056.53

ЗАХИСТ ВІД ПРОСЛУХОВУВАННЯ ПРИМІЩЕННЯ

Галайчук О.О.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Під час проведення нарад чи переговорів інформація передається за допомогою людської мови. Людська мова це звукові хвилі, які поширюються однаково на всі сторони від джерела звуку і заповнюють весь об'єм приміщення. Під час розмови виникає акустичний канал витоку інформації, який складається з джерела небезпечного сигналу, фізичного середовища поширення (наприклад – повітря, земля, вода, будівельні конструкції та інше) та технічного засобу приймання, що визначає фізичний шлях, яким зловмисник здійснюватиме несанкціоноване отримання інформації. Інформацію можна прослуховувати безпосередньо по стінах, вікнах, дверях, трубах опалення, системах пожежогасіння, металевих балках і конструкціях та інших предметах, що знаходяться у приміщенні [1].

У залежності від ситуації для прослуховування використовують дуже різні методи та засоби. В основному пристрої для прослуховування поділяють на дві групи: ті, що прослуховують на відстані та ті, які знаходять безпосередньо біля джерела звуку (рис. 1).

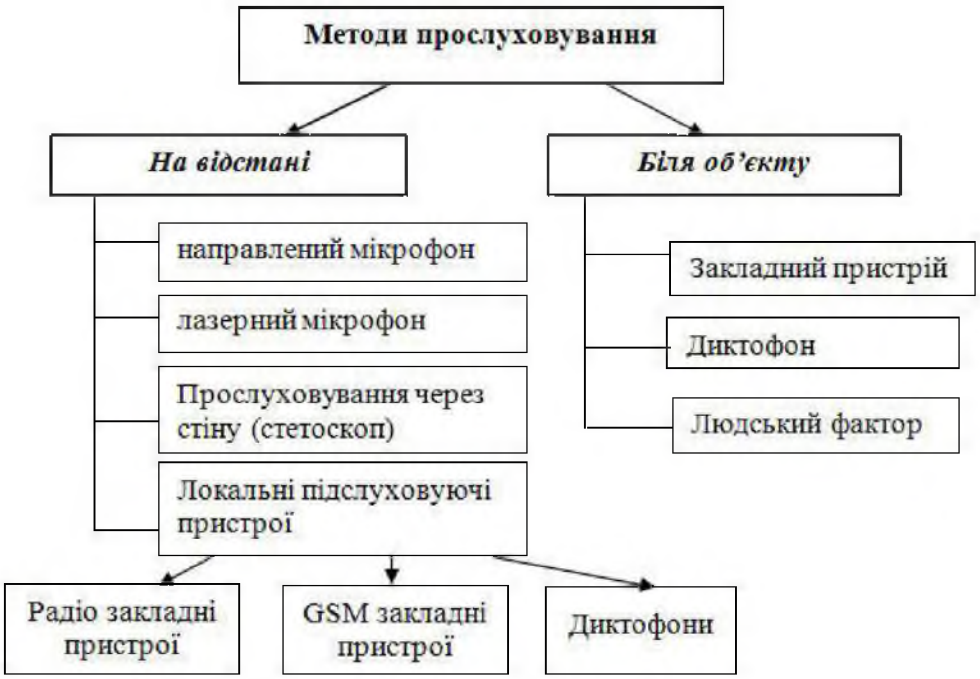

Рис. 1. *Класифікація методів прослуховування приміщення*

Захист від прослуховування – сучасний спосіб забезпечення збереження конфіденційних даних із застосуванням технічних засобів, що блокують деякі канали витоку інформації або виявляють електронні пристрої [2].

Методи захисту мовної інформації поділяють на пасивні, активні, організаційні. *Пасивні методи* – збільшення звукоізоляції огороджуючи конструкцій за рахунок: подвійних дверей з тамбуром і ущільнювачем, багатошарових стін, використання звукопоглинаючих матеріалів. *Активні методи* – це активне і віброакустичне зашумлення.

Методи захисту акустичної інформації [2-3] спрямовані на:

- створення маскувальних вібраційних і акустичних перешкод для зменшення співвідношення сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення інформаційного акустичного сигналу засобом розвідки;
- створення маскувальних електромагнітних перешкод у сполучних лініях чи лініях електроживлення, що мають у своєму складі електроакустичні перетворювачі (володіють мікрофонним ефектом), з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки;
- електромагнітне чи ультразвукове приглушення диктофонів у режимі запису;
- створення прицільних радіоперешкод акустичними і телефонними радіозакладками з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки;
- порушення функціонування (придушення) засобів несанкціонованого підключення до телефонних ліній;
- виведення з ладу (знищення) засобів несанкціонованого підключення до телефонних лініях.

В основі активних методів захисту акустичної інформації є використання спеціальної техніки, тобто різного типу генераторів шумових сигналів, вібровипромінювачів, подавлювачів GSM сигналів, диктофонів і закладних пристроїв, нелінійні локатори, детектори поля та ін.

Література

1. Андрианов В.И. Шпионские штучки и устройства для защиты объектов и информации: справочное пособие / Андрианов В.И., Бородин В.А., Соколов А.В.– Спб.: Лань, 1996. – 272 с.

2. Технічний захист інформації (приміщень). [Електронний ресурс]. – Доступно з: http://ssbb.com.ua/uk/tehnichniy-zahist-informatsiyi-primishhen-2.

3. Захист від прослуховування. [Електронний ресурс]. – Доступно з: http://sirius.kiev.ua/index.php?option=com_content&view=article&id=206&Itemid=&lang

4. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації. [Електронний ресурс]. – Доступно з: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat