УДК 621.391:[004.056:004.934

ТЕХНІЧНІ КАНАЛИ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ ЗА РАХУНОК ЗАСОБІВ ДИСТАНЦІЙНОЇ АКУСТИЧНОЇ РОЗВІДКИ

Льозіна О.О.
Науковий керівник – проф. Олейніков А.М.
Харківський національний університет радіоелектроніки, каф. ІРТЗІ
м. Харків, Україна
e-mail: oleksandra.lozina@nure.ua

With the development of information influence, there are requirements for saving information from leaking. Thesis is about the problems of information leakage through acoustic channels. Devices for listening information are described. Special attention is paid to the various microphones. As a result, the methods of combating information leakage are indicated.

Сьогодні інформація відіграє важливу роль в нашому житті. Це не є великим секретом, що витік інформації може завдати великі збитки для бізнесу, компанії чи тощо. В період електротехнічного прориву захист мовленнєвої інформації від несанкціонованого зйому або прослуховування є однією з найважливішою задачею для збереження конфіденційності.

Вухо людини не є найкращим апаратом для прослуховування конфіденційної інформації, бо це передбачає находження людини на об’єкті з потрібною нам інформацією та має неефективний поріг чутності порівнюючи з технічними засобами. Можна використовувати людину зі стетоскопом, але проблема виявлення людини на об’єкті залишається відкритою. Найбільш економічним та ефективним методом дистанційного прослуховування інформації є використання додаткового обладнання, а саме: вузько спрямовані мікрофони, закладні пристрої, лазерні системи акустичної розвідки.

Вузько спрямовані мікрофони поділяються на комбіновані, параболічні та групові. Остання група поділяється на лінійну групу, плоскі решітки та трубчасті.

Лінійна група мікрофонів- це термін, який описує систему мікрофонів, де мікрофони розташовані з кроком d. Кожний мікрофон в лінійній групі може мати свою доріжку, що дозволить оператору вільно змінювати параметри та маніпулювати звуковим образом.

Плоску решітку використовують для підвищення спрямованості лінійної групи мікрофонів. Це грубо кажучи мікрофон який складається з декількох мікрофонів лінійної групи, які мають спільний суматор.

Тубчаті мікрофони органного типу складаються з декількох трубочок, довжина яких збільшується з кроком d. Ці трубочки збираються в один пучок, де найдовша знаходиться в центрі, коротші йдуть по спіралі. В свій час трубчастий щілинний приймач конструктивно являє собою трубку з поздовжньою щілиною. Трубка з’єднується з капсулем, у якому знахо-

диться мікрофон. Внутрішня поверхня капсуля й зовнішній кінець трубки закритий поглинаючою тканиною (або повстю), щоб уникнути утворення стійних хвиль. Таку трубку можна розглядати як множину трубок різної довжини.

Будь-який мікрофон складається з мембрани та механічно-електричної системи. Якщо подивитись на поширення звуку в приміщеннях, можна зрозуміти, що вікно може виконувати роль мембрани. Нам лише потрібен лазер та його приймач, який буде знімати коливання звуку. Це принцип роботи лазерної системи акустичної розвідки. В теорії цей вид обладнання буде найкращим, для шпигування, але в нього є мінуси, такі як вартість та обмежена проникливість.

Для прослуховування інформації найкраще використовувати закладні пристрої. Акустичні закладні пристрої поділяються на велику кількість груп, залежно від того, що в них мікрофон чи вібродатчики, який вид передачі сигналу, по тому як вони керуються та тощо. Найбільша загроза полягає в тому, що вони можуть бути замасковані під різні прибори, такі як: лампочки, калькулятори, запальнички, ручки та йще багато різних предметів.

Для передачі даних можуть використовуватись радіоканали, інфрачервоні сигналі та провідні лінії(наприклад, лінії стаціонарних телефонів).

На деяких видах підприємств, досі використовуються стаціонарні телефони для зв’язку в середині об’єкта, але через ймовірне використання пристроїв НВЧ нав’язування варто відмовлятись від них, тим паче вже є багато альтернатив.

Підсумовуючи, для забезпечення захисту акустичної інформації треба дотримуватись таких дій:

- Зробити організаційні засоби для захисту інформації, такі як контроль людей, які заходять на об’єкт, де вони знаходяться та що приносять.
- В приміщеннях де потрібна інформація, треба захищати вікна від лазерних мікрофонів. Вішати жалюзі та можливо навіть ставити спеціальні пристрої, які будуть робити акустичні перешкоди.
- Шифрувати акустичний сигнал.
- Проводити перевірку кімнат на наявність закладних пристроїв.
- Зробити гарну звукоізоляцію кімнат.

У роботі проводиться аналіз ступеня загроз, які несуть у собі ці канали витоку інформації та методів захисту від витоку інформації.

Список використаних джерел:

1. Олейніков А. М. «Методи та засоби захисту інформації» Навчальний посібник для студентів вищих навчальних закладів (з гріфом МОН України). Харків: НТМТ, 2014. 298с.