УДК 004.056.5:004.934

ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ

Степуро О. В.
Науковий керівник – ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: oleksandra.stepuro@nure.ua

The work is devoted to the technical channels of speech information leakage: acoustic, vibroacoustic, electroacoustic and optoacoustic channels. The main means of acoustic language intelligence, possible places of their installation are considered.

Досягнення технічного прогресу дозволяють сьогодні використати широкий спектр методів і пристроїв передачі інформації, проте, і нині людська мова залишається одним з найважливіших шляхів інформаційної взаємодії. Одночасно посилюється потреба в забезпеченні конфіденційності мовного обміну. Захист мовної інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації.

Несанкціоноване ознайомлення із мовною інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками. Для цього може використовуватися широкий арсенал портативних засобів акустичної мовної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електроакустичним та оптико-акустичним каналами.

Основними засобами акустичної мовної розвідки є: диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки; спрямовані мікрофони; електронні стетоскопи; закладні пристрої з датчиками мікрофонного й контактного типів з передаванням перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні хвиль) та ультразвуковому каналах, мережі електроживлення, по телефонних лініях зв'язку, з'єднувальних лініях допоміжних технічних засобів або спеціально прокладених лініях; оптико-електронні акустичні системи та ін. [1].

Портативна апаратура звукозапису та закладні пристрої із датчиками мікрофонного типу можуть бути встановлені під час неконтрольованого перебування фізичних осіб безпосередньо у виділених приміщеннях. Ця апаратура забезпечує реєстрацію розмови середньої гучності на відстані 10-15 м від її джерела.

Електронні стетоскопи та закладні пристрої з датчиками контактного типу дають змогу перехоплювати акустичну інформацію без фізичного доступу до захищуваного приміщення. При цьому датчики закладних пристроїв установлюються переважно біля місць можливих витоків такої інформації.

Датчики закладних пристроїв мікрофонного типу встановлюються біля виходів кондиціонерів та вентиляційних каналів, датчики контактного типу (перетворювачі віброакустичних сигналів, що поширюються по будівельних конструкціях споруд, інженерних комунікаціях та ін.) - на зовнішніх поверхнях будівель, у віконних проймах та рамах, у суміжних приміщеннях за дверними проймами, на перегородках, трубах систем опалення та водопроводу, коробах вентиляційних та інших систем. За допомогою таких засобів розвідки можна перехопити мовну інформацію в залізобетонних будівлях через 1-2 поверхи, по трубопроводах через 2-3 поверхи і по вентиляційних системах 20-30 м завдовжки.

Застосування для ведення розвідки спрямованих мікрофонів і оптико-електронних (лазерних) акустичних систем не потребує проникнення фізичних осіб не тільки у виділені приміщення та суміжні з ними, а й на охоронну територію об'єкта. Розвідку можна вести із сусідніх будівель чи автомобілів, що перебувають на автостоянках біля будівлі. За допомогою спрямованих мікрофонів можна перехоплювати розмову із виділених приміщень за наявності в них вікон в умовах міста на відстані близько 50 м.

Максимальна відстань ведення розвідки з використанням оптико-електронних (лазерних) акустичних систем, які знімають інформацію з внутрішнього скла, в умовах міста при наявності інтенсивних акустичних перешкод, запиленості повітря, сягає 150-200 м [2].

Захисту мовної інформації можна досягти проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. Система захисту мовної інформації має забезпечити виявлення у приміщенні радіомікрофонів; виявлення і протидію занесеним диктофонам; протидію перехопленню інформації, переданої по телефонній лінії; протидію апаратурі, що використовується для передавання сигналів у мережу 220 В, кабельним і радіо-стетоскопам, засобам ведення оптико-електронної розвідки. У результаті аналізу технічних вимог до системи захисту інформації слід обрати варіант комплексу засобів захисту мовної інформації з використанням засобів, які є в Україні сертифікованими чи мають узгоджені технічні умови.

Список використаних джерел:

1. Захист мовної інформації. ТЗІ - інформаційна безпека та захист інформації URL: https://tzi.ua/ua/zahist_movno_nformac.html (дата звернення: 13.02.2024).

2. Канали витоку інформації. Pidru4niki. URL: https://pidru4niki.com/1512021051313/ekonomika/kanali_vitoku_informatsiyi (дата звернення: 09.02.2024).