ЗАХИЩЕНІСТЬ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ДИСТАНЦІЙНИХ ЗАСОБІВ АКУСТИЧНОЇ РОЗВІДКИ

Олейніков А.М., Пономаренко Є.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах розвитку технічних засобів спостереження виникає потреба у комплексному захисті об'єктів інформаційної діяльності від несанкціонованого зняття акустичної інформації. Сучасні засоби дистанційної акустичної розвідки здатні фіксувати коливання поверхонь або повітряних мас, спричинені мовленням людини, навіть на значній відстані від об'єкта [1]. Тому забезпечення належного рівня акустичної безпеки є критично важливим для організацій, які працюють з конфіденційною або державною інформацією.

Метою доповіді є аналіз технічних каналів витоку мовної інформації на об'єкті інформаційної діяльності (ОІД) від дистанційних засобів акустичної розвідки та розробка комплексу технічного захисту інформації на ОІД для забезпечення безпеки мовної інформації. До основних видів технічних загроз дистанційного акустичного знімання інформації належать використання вузькоспрямованих мікрофонів, які здатні приймати звукові сигнали на відстані до 100–150 м залежно від конкретного стану акустичного фону середовища поширення акустичних коливань, лазерні системи акустичної розвідки, які реєструють мікроколивання скла вікон на відстані декілька сотень метрів, а також деякі види пасивних радіоакустичних закладних пристроїв, в основі яких лежать методи високочастотного нав'язування при використанны високочастотних резонаторів [2]. У доповіді розглядаються питання створення комплексу технічного захисту інформації ОІД на основі використання звукопоглинальних матеріалів у конструкціях стін, підлоги, стелі застосування вікон із багатошаровими склопакетами, встановлення генераторів акустичних або вібраційних завад («маскувальних шумів»), використання плівок або фільтрів на скляних поверхнях, що знижують відбиття лазерного променя, створення звукоізольованих переговорних приміщень, забезпечення цілодобового радіомоніторингу та інше. Рекомендовано використовувати пасивні (звукоізоляційні) та активні (генератори шуму) методи захисту, а також проводити регулярні перевірки приміщень на наявність технічних засобів розвідки.

Список літератури

1. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО. / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. 2-е вид., перероб. і доп. – Харків: ХНУРЕ, 2024. – 266 с.

2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов. – К.: ІСЗІ НТУУ «КПІ», 2016. – 104 с.