АКУСТИЧНІ ТА ВІБРОАКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Мовна інформація, що обробляється в телекомунікаційних системах (ТКС), залишається вразливою ще до перетворення на електричний сигнал: її можна перехопити в приміщенні, де розташовані телефонні апарати, термінали відеоконференцзв'язку та голосові асистенти. Такі канали не залежать від криптографічного захисту лінії зв'язку, тому їх часто недооцінюють під час проєктування систем захисту [1; 2].

Мета роботи – розглянути механізми утворення акустичних і віброакустичних каналів витоку інформації в ТКС та визначити основні напрями протидії.

Акустичні та віброакустичні канали витоку

Акустичний канал утворюється, коли звукові хвилі, створені мовцем, поширюються повітряним середовищем і потрапляють до мікрофона закладного пристрою або до чутливого елемента технічного засобу. Перехоплення можливе за допомогою направлених мікрофонів, радіомікрофонів, диктофонів і прихованих мікрофонів, підключених до ліній зв'язку [3].

У ТКС окрему небезпеку становлять *мікрофонний ефект і акустоелектричні перетворення*. Телефонний апарат у режимі «покладена трубка», гучномовці, дзвінки та електродинамічні елементи під дією звуку можуть генерувати електричний сигнал і передавати його в лінію. Так речова інформація потрапляє за межі контрольованої зони без жодного втручання в апаратуру [3; 4].

Віброакустичний канал виникає, коли звукові коливання збуджують механічні коливання огороджувальних конструкцій: стін, стель, вікон, труб опалення та водопостачання, повітроводів.

Їх фіксують контактні мікрофони та стетоскопи, а на великій відстані лазерні системи знімання вібрацій зі скла. Ці коливання поширюються конструкціями будівлі на значну відстань і дають змогу вести прослуховування з суміжних приміщень [4].

До джерел віброакустичних сигналів належать також корпуси серверного й комутаційного обладнання, клавіатури та вентилятори охолодження. За характером їхніх вібрацій можна відновити окремі відомості про оброблювані дані [3].

Оцінювання небезпеки каналів

У практиці технічного захисту інформації небезпеку акустичного й віброакустичного каналів оцінюють за *розбірливістю мови* на вході засобу перехоплення. Її визначають за співвідношенням «сигнал/шум» в октавних смугах частот та за формантним методом.

Канал вважають закритим, якщо розбірливість мови не перевищує нормованого значення.

Вимоги до проведення такого оцінювання містять нормативні документи системи технічного захисту інформації в Україні [2; 5].

Захист від витоку цими каналами має поєднувати організаційні та технічні заходи [5].

Організаційні: визначення виділених приміщень, контроль доступу, заборона несанкціонованого внесення технічних засобів, періодичне обстеження приміщень на наявність закладних пристроїв.

Пасивні технічні: звукоізоляція приміщень, подвійні двері й тамбури, віброізолювальні прокладки, фільтрація та відключення мікрофонних кіл апаратури.

Активні технічні: акустичне та віброакустичне зашумлення (генератори «білого» та мовоподібного шуму, вібраційні випромінювачі на вікнах, стінах і трубах), підбір рівня маскувального шуму за результатами вимірювань.

Контроль: використання індикаторів поля, нелінійних локаторів і детекторів диктофонів під час спеціальних обстежень.

Висновки

Акустичні та віброакустичні канали залишаються одними з найменш помітних каналів витоку в ТКС, тому що вони не залежать від захищеності лінії зв'язку. Ефективний захист потребує оцінювання розбірливості мови на межі контрольованої зони й узгодженого застосування організаційних, пасивних та активних заходів.

Перспективними напрямами є адаптивні системи зашумлення та автоматизований контроль стану виділених приміщень [6].

Список літератури

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

2. Положення про технічний захист інформації в Україні : затв. Указом Президента України від 27.09.1999 № 1229/99.

3. Юдін О. К., Богуш В. М. Захист інформації в мережах передачі даних. Київ : ТОВ «НТК», 2005.

4. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека : Основи термінології та вимоги до захисту. Київ : ДМК Прес, 2010.

5. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Київ : ДСТСЗІ СБ України, 2005.

6. А.М. Олейніков, П.М. Шкопотко Методи формування акустичних завад для засобів протидії несанкціонованому документуванню мовної інформації / Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2026. Вип. 224. С. 125 – 130. DOI:10.30837/rt.2026.1.224.12