УДК 621.39:534.87]:004.056.5 **DOI:10.30837/rt.2025.1.220.11**

А.М. ОЛЕЙНІКОВ, канд. техн. наук, Ю.В. ЛИКОВ, канд. техн. наук, Я.С. ПАВЛЕНКО

ОСОБЛИВОСТІ ВИЯВЛЕННЯ АКУСТОЕЛЕКТРОМАГНІТНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Вступ

У сучасному технологічному середовищі, що характеризується стрімким розвитком інформаційних технологій та цифрових систем, забезпечення інформаційної безпеки набуває критичного значення. Однією з основних загроз для конфіденційності даних є технічні канали витоку інформації, серед яких особливу увагу привертають акустоелектромагнітні канали. Ці канали формуються внаслідок акустоелектромагнітних перетворень, коли акустичні хвилі взаємодіють із елементами технічних пристроїв, перетворюючи звукову енергію на електричну або електромагнітну. Такі канали часто мають прихований характер і залишаються непомітними під час стандартних перевірок систем інформаційної безпеки, що робить їх надзвичайно небезпечними.

Акустоелектромагнітні канали витоку інформації є особливо підступними через свою здатність виникати навіть у повсякденних умовах. Звичайні пристрої, що оточують, можуть стати джерелами небажаних сигналів, які потенційно можуть бути використані для несанкціонованого доступу до даних. Ці канали утворюються завдяки дії акустичних хвиль на чутливі елементи технічних засобів, такі як трансформатори, п’єзоелементи, котушки індуктивності, гучномовці, мікрофони або інші компоненти з високою реакцією на звукові коливання. Вплив акустичних хвиль на ці елементи викликає зміну електричних параметрів або генерує нові сигнали, які можуть містити конфіденційну інформацію [1].

Окрім технічних особливостей, проблема виявлення акустоелектромагнітних каналів витоку інформації посилюється складністю аналізу їх фізичних властивостей. Сигнали такого типу можуть бути слабкими, маскуватися під природний шум або зливатися з робочими сигналами пристроїв. Це вимагає розробки нових підходів до моніторингу, виявлення та аналізу акустоелектромагнітних явищ у технічних засобах.

1. Типи акустоелектомагнітних каналів витоку інформації та фізичні процеси, що відбуваються в них

Акустоелектричні канали витоку інформації поділяються на два основні типи: прямі та модуляційні. Прямі акустоелектричні канали утворюються внаслідок безпосереднього перетворення акустичних коливань в електричні сигнали (рис. 1). Модуляційні акустоелектричні канали виникають тоді, коли акустичні коливання впливають на елементи високочастотнних генераторів, викликаючи модуляцію їх сигналів за частотою або амплітудою відповідно до параметрів мовного сигналу.

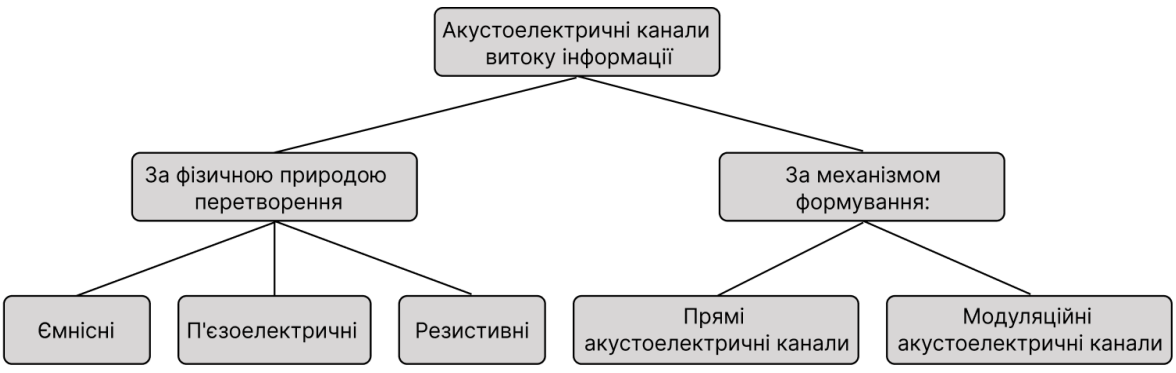

Рис. 1. Класифікація акустоелектричних каналів витоку інформації

Акустомагнітні канали також поділяються на прямі та модуляційні. Прямі акустомагнітні канали формуються через індукцію магнітних полів у феромагнітних матеріалах під впливом акустичних хвиль. У цьому випадку звуковий вплив створює магнітну індукцію, яка може бути виявлена в магнітопроводах чи обмотках пристроїв (рис. 2). Модуляційні акустомагнітні канали виникають тоді, коли звукові коливання змінюють параметри магнітної індукції, впливаючи на характеристики магнітопроводів чи котушок, що використовуються у технічних системах [2].

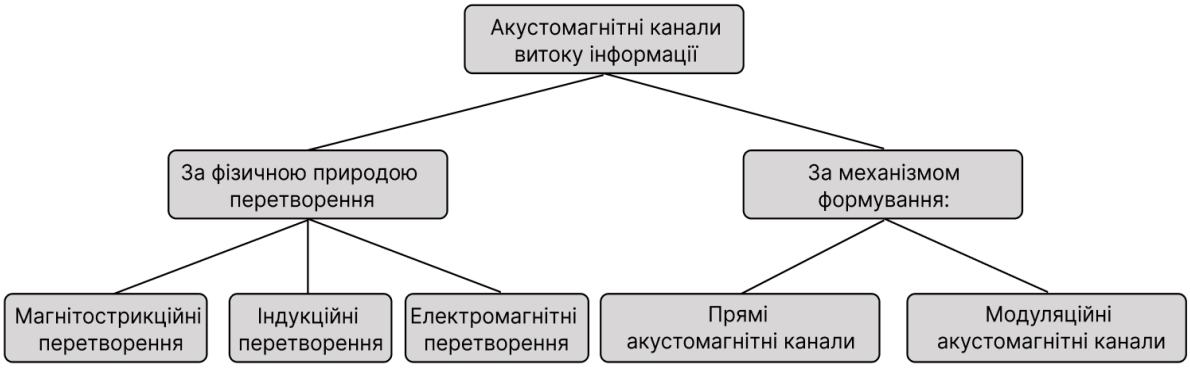

Рис. 2. Класифікація акустомагнітних каналів витоку інформації

Серед акустичних перетворювачів розрізняють індуктивні, ємнісні, п’єзоелектричні, електромагнітні, оптичні, магнітострикційні та акусторезистивні пристрої. Індуктивні перетворювачі працюють за принципом зміни індуктивності під впливом механічної дії. Ємнісні перетворювачі змінюють свою ємність під впливом акустичного тиску, що робить їх надзвичайно чутливими до звукових впливів. П’єзоелектричні перетворювачі базуються на використанні п’єзоелектричного ефекту, коли механічне навантаження викликає появу електричного заряду. Ці елементи мають високу стабільність параметрів перетворення і широко застосовуються в радіотехнічних пристроях, але можуть стати потенційним джерелом витоку інформації.

Фізичні процеси, що лежать в основі акустоелектричних перетворень, пов’язані з механічними коливаннями, які змінюють електричні параметри сигналів. Наприклад, акустичний сигнал впливає на дифузор гучномовця, внаслідок чого акустична енергія перетворюється в механічну, змінюючи положення котушки в магнітному полі, що викликає появу електрорушійної сили в електричному колі котушки. Якщо гучномовець підключений до мережі через трансформатор, небезпечний сигнал може збільшитися в кілька разів, поширюючись мережею живлення [3].

У трансформаторах зміна параметрів обмоток під впливом звукових хвиль може призводити до модуляції сигналів, що передаються мережею. П’єзоелементи перетворюють механічні коливання на електричний заряд, а оптичні перетворювачі можуть змінювати свій вихідний сигнал під впливом акустичних хвиль, які модулюють світловий потік.

Іншим прикладом є домофонні апарати, де динаміки або дзвінкові механізми можуть генерувати сигнали під впливом звукових хвиль, передаючи їх телефонною лінією. Особливу небезпеку становлять датчики охоронно-пожежної сигналізації, які оснащені п’єзоелементами, що реагують на звукові хвилі, створюючи електричні сигнали, які можуть бути використані для перехоплення інформації.

Для оцінки ефективності перетворення звукової енергії в електричну чи магнітну використовують коефіцієнт перетворення (КПД). Це безрозмірна величина, що визначає, яка частка вхідної акустичної енергії перетворюється у вихідний сигнал. Ефективність перетворення п’єзоелементів може досягати 20 – 30 %, що робить їх потенційно небезпечними у контексті витоку інформації.

Формули для розрахунку КПД для акустичного перетворювача:

$$K_{ae} = \frac{P_{\text{вих}}}{P_{\text{вх}}} \cdot 100\%, \quad (1)$$

де $P_{вих}$ – вихідна потужність сигналу, $P_{вх}$ – вхідна акустична потужність.

Для визначення $P_{вих}$ для акустоелектричного перетворення проводиться розрахунок ЕРС.

1) Для п'єзоелектричного перетворення:

$$E = k_0 \cdot F \cdot v, \quad (2)$$

де E – електрорушійна сила (ЕРС); k_0 – коефіцієнт п'єзоефекту; F – механічна сила; v – швидкість деформації.

Для визначення $P_{вих}$ для акустомагнітного перетворення проводиться розрахунок:

2) Для акустомагнітного перетворення:

$$B = \mu \cdot \frac{F}{S}, \quad (3)$$

де B – магнітна індукція, μ – магнітна проникність, F – акустична сила, S – площа магнітопроводу.

Для акустоелектричних каналів, таких як гучномовці та п'єзоелементи, напруга сигналу, що наводиться у гучномовцях, зазвичай становить 2 – 3 мВ/Па. У модуляційних акустоелектричних каналах, які базуються на високочастотних генераторах, величина модуляції сигналу може становити 0,5 – 1 % від амплітуди несучої частоти. Цього рівня достатньо, щоб забезпечити можливість перехоплення інформації. Щодо акустомагнітних каналів, таких як трансформатори або магнітопроводи, індуковані сигнали в них можуть досягати 1 – 5 мВ, залежно від параметрів магнітної проникності та акустичного тиску звукової хвилі. Проте коефіцієнт перетворення магнітного типу зазвичай не перевищує 10 – 15 % через значні втрати у магнітних матеріалах, що обмежує ефективність таких каналів у порівнянні з акустоелектричними [4].

2. Методики виявлення акустоелектричних каналів витоку інформації та їх особливості

Виявлення акустоелектричних каналів витоку інформації (АЕКВІ) базується на використанні експериментальних підходів, які дозволяють визначити взаємозв'язок між акустичними впливами та електричними сигналами, що генеруються технічними пристроями. Основними методами є дослідження прямих і модуляційних каналів витоку інформації. Кожен із цих підходів вимагає окремих схем випробувань, налаштування відповідного обладнання та специфічних методик вимірювань.

Для прямого акустоелектричного каналу використовується функціональна схема (рис. 3.), яка складається:

- з джерела акустичних сигналів (акустичний генератор), який створює електричний сигнал з визначеною частотою та амплітудою;
- випромінювача звуку (динамік або ультразвуковий випромінювач), який передає акустичний сигнал у зону дослідження;
- об'єкта дослідження (потенційне джерело АЕКВІ) – це технічний пристрій (гучномовець, п'єзоелемент, трансформатор, тощо), який піддається впливу звукових хвиль;
- пристрою реєстрації сигналів – спектроаналізатор вимірює електричні сигнали, які виникають у досліджуваному об'єкті;
- комп'ютера з АЦП та програмним забезпеченням для обробки даних і побудови залежностей між акустичними і електричними параметрами.

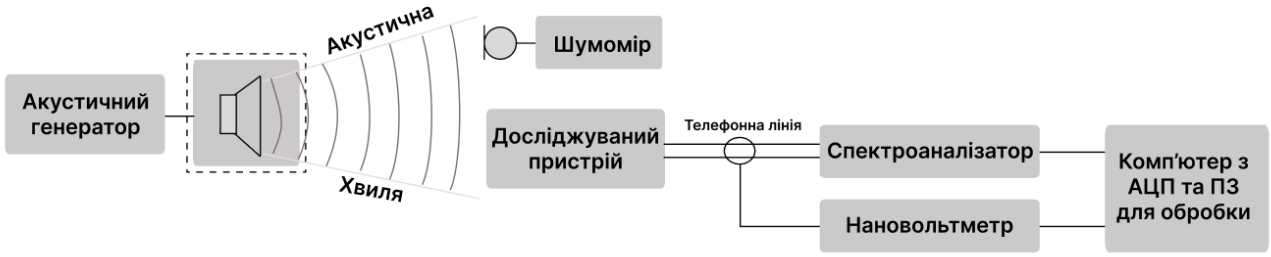

Рис. 3. Функціональна схема для дослідження прямого каналу витоку інформації

Методика дослідження включає поступове підвищення частоти звукового сигналу, вимірювання амплітуд вихідних електричних сигналів та їх аналіз для визначення рівня чутливості об'єкта до акустичних впливів (рис. 4).

Для модуляційного каналу схема включає наступні компоненти:

- акустичний генератор, який створює коливання змінної частоти;
- випромінювач акустичних хвиль передає сигнал у зону розташування високочастотного генератора;
- досліджуваний пристрій, у якому утворюється модуляція сигналу через акустичний вплив;
- антена, радіоприймач та аналізатор спектра реєструють модульовані сигнали та оцінюють їх характеристики;
- комп'ютер з програмним забезпеченням для аналізу частотного спектра, визначення глибини модуляції та виявлення небезпечних сигналів.

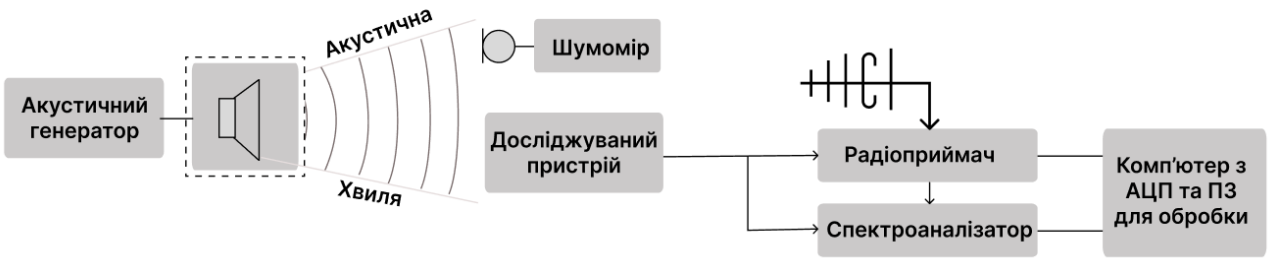

Рис. 4. Функціональна схема для дослідження модуляційного каналу витоку інформації

У цьому випадку проводиться аналіз вихідних сигналів досліджуваного пристрою, їх амплітудної чи частотної модуляції під впливом акустичних хвиль, а також оцінка параметрів модуляції, які можуть бути використані для витоку інформації.

Для проведення експериментів використовуються акустичний генератор із широким діапазоном частот, випромінювач звукових хвиль (динаміки, ультразвукові перетворювачі), осцилограф для візуалізації електричних сигналів у реальному часі, спектроаналізатор для аналізу частотного спектра сигналів, що генеруються об'єктом, нановольтметр із високою чутливістю для точного вимірювання низькоамплітудних сигналів, АЦП, комп'ютер із програмами для обробки даних і побудови графіків залежності сигналів від акустичного впливу.

Акустичні системи (АС), що використовуються для дослідження акустоелектричних каналів витоку інформації, повинні створювати контрольовані акустичні сигнали з параметрами, що дозволяють моделювати вплив звукових хвиль на технічні засоби. АС мають працювати у широкому частотному звуковому та ультразвуковому діапазоні, забезпечувати стабільну амплітуду сигналу з мінімальними спотвореннями (менше 1 %) та зберігати стабільність випромінювання з відхиленням не більше ±1 – 2 %. Важливі вимоги включають спрямованість звуку, можливість регулювання потужності випромінювання (0,1 – 50 Вт),

а також стійкість корпусу до вібрацій і відсутність побічних електромагнітних або механічних випромінювань. Для забезпечення такого захисту використовується щільне електромагнітне екранування колонок, яке зменшує вплив електромагнітних випромінювань на досліджуваний пристрій. Інколи для спеціальних завдань використовуються так звані механічні свистки які не створюють електромагнітного випромінювання, тому їх часто використовують у дослідженнях, де важливо уникнути впливу електромагнітних полів.

АС повинні підтримувати калібрування та забезпечувати сумісність з вузькосмуговими чи ультразвуковими випромінювачами для розширення можливостей дослідження. Виконання цих вимог гарантує точність і надійність експериментів, спрямованих на виявлення і аналіз потенційних загроз [5].

Важливо забезпечити ізольованість досліджуваної зони від сторонніх акустичних та електромагнітних перешкод. Приміщення має бути звукоізольованим, а кабелі – екранованими. Для прямого каналу основна увага приділяється виявленню сигналів, які генеруються технічними засобами безпосередньо під впливом звукових хвиль. Для модуляційного каналу ключовим є визначення параметрів модуляції (частоти, амплітуди), які можуть бути використані для перехоплення мовної інформації.

Важливим етапом в виявленні акустоелектричних каналів витоку інформації є спеціальні перевірки та обстеження, що мають на меті ідентифікацію потенційних каналів витоку, оцінку їхньої небезпеки та розробку заходів для їх нейтралізації. Це комплексна процедура, яка базується на використанні сучасного обладнання, програмних засобів і методик, спрямованих на захист конфіденційної інформації.

Проведення перевірок починається з попереднього аналізу об'єкта. На цьому етапі визначаються можливі джерела витоку інформації, включаючи технічні засоби, які можуть бути вразливими до акустичних, електромагнітних чи інших впливів. Аналізуються планування приміщень, типи використовуваних технічних засобів і комунікаційні мережі [6].

Для визначення першопричини виникнення акустоелектричного каналу витоку інформації необхідно провести комплексний аналіз об'єкта дослідження, враховуючи можливість впливу як електромагнітних, так і акустичних хвиль для прояви електричного відгуку. Основна мета – з'ясувати, чи джерелом небезпечного сигналу є акустична хвиля, а не електромагнітна.

Методика виявлення акустоелектричних каналів витоку інформації включає кілька етапів, які дозволяють визначити природу виникнення сигналу та встановити основні причини витоку.

На першому етапі здійснюється попередній аналіз об'єкта дослідження. Пристрій або система перевіряється на наявність фізичних елементів, які можуть спричинити витік інформації. Аналізуються конструктивні особливості, такі як наявність котушок, конденсаторів чи п'єзоелементів, магнітострикційні елементи, тип матеріалів, з яких виготовлено елементи (феромагнітні, п'єзоелектричні або діелектричні), а також робочі режими пристрою, включно з напругою, частотою та потужністю.

На другому етапі проводиться вимірювання електричних параметрів у контрольованих умовах. Об’єкт ізолюється від будь-якого акустичного впливу і досліджується його робота в звичайних режимах. Вимірюється рівень електричних сигналів, які генеруються пристроєм, перевіряється наявність побічних випромінювань у спектрі частот і електромагнітних завад, що можуть вказувати на внутрішні електричні джерела сигналу.

На третьому етапі моделюється акустичний вплив. Використовується акустичний генератор і випромінювач для створення контрольованого звукового сигналу з заданими параметрами частоти й амплітуди. Об'єкт піддається дії звукових хвиль у різних частотних діапазонах, а результати впливу фіксуються. Реєструються вихідні електричні сигнали, що виникають у пристрої, досліджується їхня амплітудно-частотна залежність та визначається затримка між акустичним впливом і генеруванням сигналу, що дозволяє виявити можливі

механічні ефекти. Зрозуміло, що навіть добре екранована колонка створює деякі електричні та магнітні поля, наведення від яких не повинні вносити похибки у вимірювання [7].

Найпростіший спосіб визначити, що ми спостерігаємо – наведення тест-сигналу від акустичного випромінювача, вимірювального тракту генератор-підсилювач потужності та з'єднувальних кабелів або безпосередньо сигнал АЕП, полягає в закриванні лицьової панелі акустичного випромінювача звукопоглинальною шторкою з метою зміни (зниження) рівня акустичного сигналу, що впливає на технічний засіб (ТЗ), контрольованого за допомогою шумоміра. У цьому випадку наведення через вплив електромагнітного поля генераторного обладнання на технічний засіб, якщо воно існує, залишиться незмінним, тобто показання вимірювального приладу, підключеного до технічного засобу, не зміняться або, в крайньому разі, зміняться непропорційно зниженню рівня акустичного сигналу. У першому випадку вимірювана величина тест-сигналу – це «чисте» наведення, у другому – суміш порівнюваних за рівнями сигналів наведення та акустоелектричних перетворень.

Інший, досить ефективний спосіб визначення достовірності вимірювання саме сигналу акустоелектричного перетворення при тій же вимірювальній схемі полягає в зміні відстані між генераторним обладнанням, включаючи акустичний випромінювач, і досліджуваним технічним засобом. При лінійній зміні сигналу акустоелектричного перетворення залежно від відстані вимірюваний сигнал є наслідком акустичного впливу на технічний засіб, а при зміні вимірюваного сигналу за законом $1/R^2 – 1/R^3$ – наведення через електричні або магнітні поля генераторного обладнання. Цей спосіб зручно використовувати для визначення того, яка з компонент електромагнітного поля переважає у сигналі наведення [8].

Далі проводиться порівняльний аналіз результатів. Якщо електричні сигнали виникають в умовах відсутності акустичних впливів, то першопричина має електричну природу, наприклад, через електромагнітну взаємодію між компонентами або конструктивні недоліки пристрою. Якщо ж сигнали з’являються лише під впливом звукових хвиль, це вказує на акустичну природу явища, наприклад, механічні коливання або п'єзоелектричний ефект. У випадку, коли спостерігається комбінація електричних і акустичних впливів, аналізуються їх характеристики, такі як амплітуда, частота й затримка, щоб встановити домінуючий вплив.

Розуміння природи утворення сигналу наведення визначає і заходи боротьби з ним. При електричному наведенні, як правило, достатньо організувати правильну схему заземлення вимірювального комплексу в цілому. При магнітному наведенні значне зниження можна досягти тільки симетруванням, застосуванням екранованих симетричних кабелів зі скрученими парами та рознесенням елементів вимірювального (генераторного) тракту і технічних засобів.

Ця методика дозволяє не тільки виявити акустоелектричний канал витоку, але й зрозуміти його основні первопричини, що є ключовим для ефективного усунення загроз.

Окремим напрямом є виявлення модуляційних каналів, де високочастотні генератори модулюються акустичними сигналами. Такі канали можуть виникати в складних системах, які включають автогенератори, резонансні контури чи волоконно-оптичні кабелі. Методика передбачає аналіз змін частоти чи амплітуди сигналів, що генеруються пристроями.

Обстеження приміщень також включає виявлення паразитних електромагнітних випромінювань. Наприклад, деякі пристрої можуть випромінювати сигнали, що відображають мовну інформацію. Перевірки такого типу проводяться із застосуванням антен для виявлення сигналів у різних діапазонах частот.

Під час перевірок увага приділяється виявленню пристроїв із мікрофонним ефектом, які можуть діяти як непрямі джерела витоку. Для цього використовуються методики створення акустичного резонансу, що дозволяє точно визначити чутливість пристрою до звукового впливу.

Таким чином, спеціальні перевірки та обстеження є обов'язковим компонентом комплексного захисту інформації. Вони дозволяють виявити приховані технічні канали витоку та

розробити ефективні заходи для їхньої нейтралізації, забезпечуючи надійну конфіденційність даних [9].

3. Рекомендації щодо захисту технічних каналів від витоку за рахунок акустоелектромагнітних перетворень

Рекомендації щодо захисту технічних каналів від витоку інформації через акустоелектромагнітні перетворення спрямовані на мінімізацію ризику перетворення акустичних хвиль у електричні та електромагнітні сигнали, які можуть бути використані для несанкціонованого доступу до даних. Ефективний захист включає технічні, конструктивні та організаційні заходи.

Одним із ключових методів є екранування технічних засобів для зменшення впливу акустичних хвиль. Металеві або композитні екрани можуть ефективно блокувати проникнення звукових хвиль до чутливих елементів пристроїв. Особливо це актуально для гучномовців, трансформаторів і п’єзоелементів. Використання шумопоглинальних матеріалів також є важливим. Акустично поглинаючі панелі чи ізоляційні матеріали навколо пристроїв допомагають знижувати інтенсивність звукових хвиль, які можуть спричинити акустоелектричні перетворення. Оптимізація конструкцій пристроїв дозволяє знизити їх чутливість до акустичних впливів. Наприклад, ущільнення обмоток трансформаторів, використання матеріалів із низьким п’єзоефектом або зміна геометрії деталей може зменшити ефект перетворення [10].

Пасивний захист від мікрофонного ефекту та ВЧ нав'язування здійснюється обмеженням слабких сигналів та фільтрацією або вимкненням лінії, якою поширюється небезпечний сигнал. У схемах обмежувачів використовують зустрічно-паралельно включені напівпровідникові діоди, опір яких для малих (перетворених) сигналів, що становить десятки мегаом, перешкоджає їх проходженню в слаботочну лінію.

Для зниження небезпеки слід застосовувати фільтри на електричних лініях живлення та передачі сигналів. Вони блокують поширення небажаних сигналів поза робочим діапазоном пристрою, що виникають через акустичні перетворення.

Організаційні заходи включають регулярні перевірки приміщень і обладнання на наявність акустоелектричних каналів витоку. Сюди також входить моніторинг акустичного середовища за допомогою спеціалізованих пристроїв, наприклад, спектроаналізаторів, що дозволяють виявляти небажані сигнали [11].

Рекомендується використовувати маскувальні сигнали у приміщеннях із високими вимогами до інформаційної безпеки. Це можуть бути звукові генератори шуму, які створюють фон, що ускладнює роботу акустоелектричних каналів.

Для особливо важливих об’єктів слід розглядати ізоляцію технічних засобів у спеціальних приміщеннях зі звукоізоляційними конструкціями. Це гарантує, що акустичні хвилі не потрапляють до пристроїв, а отже, ймовірність витоку зменшується [12].

Навчання персоналу також відіграє важливу роль. Співробітники повинні знати про потенційні загрози акустоелектричних каналів і дотримуватися заходів безпеки, таких як вимкнення допоміжних пристроїв під час обробки конфіденційної інформації.

Загалом, реалізація цих заходів у комплексі дозволяє значно знизити ризик витоку інформації через акустичні перетворення та забезпечити високий рівень захисту технічних засобів.

Висновки

Акустоелектричні та акустомагнітні канали становлять серйозну загрозу інформаційній безпеці через свою здатність перетворювати акустичну енергію на електричні або магнітні сигнали, що можуть містити конфіденційні дані. Встановлено, що такі канали можуть виникати в технічних пристроях повсякденного використання, зокрема в трансформаторах, п’єзоелементах, телефонних апаратах і датчиках, завдяки прямим або модуляційним ефектам.

Запропоновані методики виявлення акустоелектричних каналів базуються на створенні контрольованих акустичних впливів, аналізі електричних вихідних сигналів та оцінці їхніх характеристик. Важливу роль у дослідженнях відіграють спектроаналізатори, осцилографи та інше сучасне обладнання, яке дозволяє визначати взаємозв'язок між акустичними та електромагнітними параметрами.

Рекомендації з нейтралізації каналів витоку охоплюють технічні, конструктивні та організаційні заходи, включаючи екранування пристроїв, використання шумозаглушувальних матеріалів, оптимізацію конструкцій технічних засобів і впровадження маскувальних сигналів. Особлива увага приділяється організації перевірок і навчання персоналу, що забезпечує високий рівень захисту в умовах зростання технологічних загроз.

Таким чином, виявлення і запобігання акустоелектричним каналам витоку інформації є важливою складовою забезпечення інформаційної безпеки. Складність цих каналів, їх прихований характер і залежність від фізичних властивостей технічних засобів вимагають комплексного підходу до їх виявлення і нейтралізації.

Подальший розвиток технічних засобів аналізу і захисту дозволить знизити ризики витоку інформації, забезпечуючи надійний захист навіть в умовах зростання технічних загроз.

Список літератури:

1. Бобала Ю. Я., Горбатий І. В. Інформаційна безпека. Львів : Львів. політехніка, 2019. 580 с.
2. Голев Д., Кононович В., Хомич С. Методики оцінки інформаційної захищеності телекомунікацій. Одеса : ОНАЗ, 2013. 218 с.
3. Остапов С.Е., Євсеєв С.П., Король О.Г..Технології захисту інформації. Львів : Новий світ-2000, 2023. 678 с.
4. Бузов Г. А. Захист від витоку інформації по технічним каналам. Москва : Гаряча лінія, 2015. 586 с.
5. Солодкий В., Тимофеєв В. Технічні засоби захисту інформації з обмеженим доступом. Харків : ХНУРЕ, 2013. 229 с.
6. Засоби та системи технічного захисту інформації : навч. посіб. 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.
7. Луньова С.А. Електроакустика. Київ : КПІ, 2020. 198 с.
8. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем. Київ : Держ. торг.-екон. ун-т, 2023. 376 с.
9. Олейніков А. М. Методи та засоби захисту інформації. Харків : НТМТ, 2014. 298 с.
10. Громико І. А. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання. Харків : ХНУ ім. В. Н. Каразіна, 2014. 216 с.
11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ : ДУТ-КНУ, 2016. 178 с.
12. Іванов В. М., Дмитрієв О. М. Безпека інформаційних систем. Київ : Вид-во "Центр учбової літератури", 2018. 368 с.

Надійшла до редколегії 15.01.2025

Відомості про авторів:

Олейніков Анатолій Миколайович – канд. техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; e-mail: anatoly.oleynikov@nure.ua; ORCID: https://orcid.org/0000-0002-4458-8833

Ликов Юрій Володимирович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; e-mail: yurii.lykov@nure.ua; ORCID: https://orcid.org/0000-0001-7120-3276

Павленко Ян Сергійович – Харківський національний університет радіоелектроніки, студент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; email:yan.pavlenko@nure.ua; ORCID: https://orcid.org/0009-0000-9378-9319