МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

РИБАЛЬСКИЙ О.В., ХАХАНОВСЬКИЙ В.Г., КУДІНОВ В.А.

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ПОСІБНИК ДЛЯ КУРСАНТІВ ВНЗ МВС УКРАЇНИ

Київ - 2012

УДК 681.518 (075.8)

Р 93

Схвалено та затверджено рішенням Вченої ради НАВС.
Протокол № _____ від "___" _____ 2012 р.

Рецензенти: В.О. Хорошко, доктор технічних наук, професор,
завідувач кафедри систем захисту інформації
Науково-навчального інституту захисту інформації
Державного університету інформаційно-комунікаційних
технологій (м. Київ)
С.В. Лєнков, доктор технічних наук, професор,
начальник Науково-дослідного центру Військового інституту
Київського національного університету ім. Т. Шевченка (м. Київ)

Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

У посібнику надано основи інформаційної безпеки у обсязі, необхідному для правознавців, що мають нести подальшу службу у органах внутрішніх справ України.

Посібник написано у формі, зрозумілої для людей, які не мають технічної освіти, на базі рівня знань з математики та фізики, що надаються у курсі загальнообов'язкової середньої школи.

Призначений для курсантів вищих навчальних закладів МВС України, та може бути корисним для практичних працівників ОВС України.

ЗМІСТ

ПЕРЕДМОВА

Інформаційна сфера, як системоутворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України.

У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише їх формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу.

Розвиток наук, в першу чергу фундаментальних – математики, фізики, теорії інформації, теорії обробки сигналів та, як похідних від фундаментальних наук, радіоелектроніки, технологій виробництва радіокомпонентів, інформаційних технологій, призвели на сучасному етапі їх розвитку до виникнення інформаційного суспільства.

Основою такого суспільства є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості.

Зворотнім боком цієї "медалі" є тотальні незаконні зазіхання на чужу інформацію, що, в свою чергу, вимагає її захисту. Особливу небезпеку складають спроби викрадення інформації, що є власністю держави та містить державну або іншу таємницю.

Таким чином виникла нова наука – інформаційна безпека держави. Вона поєднує у собі як загальнодержавну нормативно-правову організаційну складову, так і складові криптографічного та технічного захисту інформації. В свою чергу криптографічний та технічний захист інформації містить питання організації, розробки та використання відповідних для цих аспектів інформаційної безпеки методів та засобів захисту. Ці складові відносяться до технічного аспекту інформаційної безпеки.

Метою посібника є надання необхідних теоретичних основ для засвоєння курсу майбутніми правоохоронцями та закріплення необхідних у подальшій роботі знань з основ інформаційної безпеки.

Матеріал дисципліни тісно пов'язаний зі спеціальними дисциплінами, що викладаються у вищих навчальних закладах правоохоронного профілю, а саме з оперативно-розшуковою діяльністю та спеціальною технікою.

У першому розділі посібника розглянуто нормативно-правову складову процесу організації та становлення в Україні всієї структури інформаційної безпеки. Розглянуто весь комплекс нормативно-правової бази, в тому числі основні концепції, які визначають сучасний стан та подальший розвиток національної та, як її складової, інформаційної безпеки України. Показані основні загрози суспільству та інформаційному ресурсу країни, що мають місце у нашій сучасності.

Другий розділ присвячений класифікації та вивченню потенційних каналів витоку інформації й способам її несанкціонованого зняття. Знання цих каналів і способів необхідні для подальшого свідомого сприйняття можливостей сучасних технічних методів і засобів захисту інформації, що застосовуються для блокування каналів витоку інформації.

У третьому роділі вивчаються сучасні методи та засоби технічного захисту інформації. Розглянуто сучасні прилади, що використовують для блокування каналів витоку інформації. Особлива увага приділяється виявленню та блокуванню каналів витоку акустичної та каналів витоку електромагнітної інформації. Подаються методики пошуку радіозакладних пристроїв. Показана необхідність суворого дотримання вимог нормативних документів, що визначають правила обробки інформації з обмеженим доступом засобами обчислювальної техніки.

До особливостей побудови посібника слід віднести виділення ***жирним курсивом*** термінів, що вперше зустрічаються у тексті, та виділення курсивом *визначень та понять*, які надають тлумачення цих термінів.

Додамо, що технічні терміни взяти з джерела [13]. Також відзначимо, що інші терміни та їх визначення, які безпосередньо відносяться до технічного захисту інформації, надаватимуться у посібнику в процесі надання матеріалу та взяті, у своїй більшості, з того ж самого джерела. Визначення деяких термінів запозичені з ряду законів України та підзаконних актів, зокрема [2, 3, 5, 7]. При наведенні термінів, взятих з інших джерел, у тексті надаються посилання на ці джерела.

РОЗДІЛ 1. КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Основні поняття та категорії. Інформаційна безпека як складова національної безпеки

Розглянемо основні поняття, категорії, визначення і терміни.

1. ***Інформаційна сфера*** – область діяльності, що відноситься до створення, передачі і використання інформації, включаючи особисту і суспільну свідомість, інформаційну і телекомунікаційну інфраструктуру та власне, інформацію. Інформаційна сфера – це частина соціальної діяльності суспільства, тому в ній проявляються загальні закони буття, загальні і специфічні закономірності соціального розвитку.

2. ***Єдиний інформаційний простір країни*** – це сукупність інформаційних ресурсів та інформаційної інфраструктури, що дозволяє на основі єдиних принципів і за загальними правилами забезпечувати безпечну інформаційну взаємодію держави, організацій і громадян при їх рівнодоступності до відкритих інформаційних ресурсів, а також максимально повне задоволення їх інформаційних потреб на всій території держави при збереженні балансу інтересів на входження у світовий інформаційний простір і забезпечення національного інформаційного суверенітету.

3. ***Інформаційні ресурси*** – інформаційна інфраструктура (апаратура і системи створення, обробки, збереження і передачі інформації), включаючи файли і бази даних та інформацію й інформаційні потоки.

4. ***Загроза інформаційній безпеці*** – це такий стан, коли проявляються наміри або дії, які можуть нанести шкоду інтересам особистості, суспільства та держави в галузі інформації.

5. ***Незаконне використання інформаційних і телекомунікаційних систем і інформаційних ресурсів*** – їх використання без відповідного дозво-

лу або порушення встановлених правил, законодавства чи принципів міжнародного права.

6. ***Інформаційна інфраструктура*** включає в себе:

- ***організаційні структури***, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове, фінансове забезпечення;

- ***інформаційно-телекомунікаційні структури*** – територіально розподілені державні і корпоративні комп'ютерні мережі, телекомунікаційні мережі і системи спеціального призначення та загального користування, мережі і канали передачі даних, засоби комутації і керування інформаційними потоками;

- ***телекомунікаційні технології;***

- ***системи засобів масової інформації.***

7. ***Інформаційна безпека*** – захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне ***інформацію*** та її ***параметри***, такі, як ***повнота, об'єктивність, доступність і конфіденційність.***

Інформаційна безпека є складовою ***національної безпеки.*** Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

На сучасному етапі основними реальними та потенційними ***загрозами національній безпеці*** України в інформаційній сфері є:

- прояви обмеження свободи слова та доступу громадян до інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп'ютерна злочинність та комп'ютерний тероризм;

- розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Додамо, що інші терміни та їх визначення, які безпосередньо відносяться до технічного захисту інформації, надаватимуться у посібнику в процесі надання матеріалу.

1.2. Нормативно-правове забезпечення інформаційної безпеки

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України [1].

Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності [2]. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону ***інформація*** визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Всі громадяни України, юридичні особи і державні органи мають ***право на інформацію***, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Розділ ІІ закону присвячено інформаційній діяльності, під якою розуміється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Визначено основні напрями та *види* інформаційної діяльності – одержання, використання, поширення та зберігання інформації.

У розділі ІІІ закону наведені галузі, види, джерела інформації та режим доступу до неї. Основними галузями інформації визначені: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна.

Основними ***видами інформації*** є: статистична; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

За ***режимом доступу*** інформація поділяється на ***відкриту інформацію*** та ***інформацію з обмеженим доступом***.

Держава здійснює контроль за режимом доступу до інформації.

Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Обмеження права на одержання відкритої інформації забороняється законом.

Інформація з обмеженим доступом за своїм ***правовим режимом*** поділяється на ***конфіденційну*** і ***таємну***.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До ***таємної інформації*** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю – це відомості науково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (в тому числі секрети виробництва – так зване ноу-хау), що мають дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці.

Порядок обігу таємної інформації, що не становить державної таємниці, та її захист визначається відповідними державними органами за умов додержання вимог Закону України “Про інформацію”.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Особливим видом таємної інформації є ***державна таємниця***. Вона охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановленому законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається Законом України “Про державну таємницю”, яким закладено правову основу створення та функціонування системи охорони державної таємниці в Україні [3].

Ступень таємності інформації визначається наданим ***грифом таємності*** "Таємно", "Цілком таємно" та "Особливої важливості". Гриф надається на певний термін, який залежить від ступеня таємності: для грифу "таємно" – 5 років, "цілком таємно" – 10 років, "особливої важливості" – 30 років.

У розділі IV закону визначені учасники інформаційних відноси, їх права та обов’язки. Основними учасниками цих відносин є: автори, споживачі, поширювачі, зберігачі (охоронці) інформації.

Кожний учасник інформаційних відносин для забезпечення його прав, свобод і законних інтересів має право на одержання інформації про: діяльність органів державної влади; діяльність народних депутатів; діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації; те, що стосується його особисто.

Розділ V закону присвячений охороні інформації, відповідальності за порушення законодавства про інформацію. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації. Стаття 45-1 забороняє цензуру та втручання в професійну діяльність журналістів і засобів масової інформації з боку органів державної влади або органів місцевого самоврядування, їх посадових осіб.

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом.

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Розділ VI закону присвячено міжнародній інформаційній діяльності, співробітництві з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації.

Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Стаття 53 закону визначає ***інформаційний суверенітет***. Основою інформаційного суверенітету України є національні інформаційні ресурси.

До ***інформаційних ресурсів України*** входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;

- створенням національних систем інформації;

- встановленням режиму доступу інших держав до інформаційних ресурсів України;

- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Узагальнена класифікація інформації [4] у відповідності до Закону України "Про інформацію" надана на рис. 1.1.

В ст.10 Закону України “Про основи національної безпеки України“ [5], визначені основні функції суб’єктів забезпечення національної безпеки України (інформаційна сфера окремо не виділена):

- вироблення і періодичне уточнення Стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;

- створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;

- удосконалення її організаційної структури;

- комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) системи;

- підготовка сил та засобів суб’єктів системи до їх застосування згідно з призначенням;

- постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

- систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;

- прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;

- розроблення науково-обгрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;

Рис. 1.1. Класифікація інформації у відповідності до Закону України “Про інформацію”

- запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;

- локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;

- оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на ці цілі;

- участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;

- спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у галузі безпеки.

Стаття 11 закону визначає загальні повноваження суб'єктів національної безпеки щодо контролю за здійсненням заходів забезпечення національної безпеки.

Необхідно відзначити, що цей закон був базовим для прийняття "Концепції національної безпеки України", схваленої Постановою Верховної Ради України від 16 січня 1997 року N 3/97-ВР [6].

Концепція визначала основні засади державної політики в сфері національної безпеки України та напрями її подальшого розвитку.

В її розділі III "Загрози національній безпеці України" у ряді загроз національній безпеці в інформаційній сфері виділено витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави.

А в розділі IV "Основні напрями державної політики національної безпеки України" для усунення цієї загрози запропоновано розробку і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

У розділі V концепції було сформульовано напрями та заходи для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній,

інформаційній та інших сферах створюється система забезпечення національної безпеки України.

Визначена система забезпечення національної безпеки – як організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України.

Крім того були прийняті Закони України "Про телекомунікації", "Про Національну програму інформатизації", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про науково-технічну інформацію", а у Кримінальний кодекс України було введено розділ XVI, в якому визначалася відповідальність за злочини в інформаційній сфері.

Наступним етапом створення законодавчої бази та організації системи захисту інформації в нашій державі було прийняття Постанови Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 р. [7].

Концепція на базі прийнятих законів, підзаконних актів та узагальнення їх застосування визначала державну політику України в сфері ***технічного захисту інформації***, основні напрями та організаційні засади подальшого розвитку ***системи захисту інформації*** в Україні.

А початок створення такої системи слід віднести до 1994 р., коли було затверджено Постанову Кабінету Міністрів України "Про затвердження Положення про технічний захист інформації в Україні" від 09.09.1994 р., яким визначалися першочергові дії держави щодо технічного захисту інформації. Фактично у положенні було використано ті науково-технічні та організаційні засади, що розроблялися у СРСР.

Згодом з'явилася нагальна необхідність в удосконаленні та розвитку як нормативної, так і науково-технічної бази технічного захисту інформації, що й призвело до появи "Концепції технічного захисту інформації в Україні".

У загальних положеннях “Концепції технічного захисту інформації в Україні” визначено основи державної політики у сфері захисту інформації інженерно-технічними заходами. Зокрема визначено, що технічний захист інформації (далі – ТЗІ) є складовою частиною забезпечення національної безпеки України.

Встановлено головні завдання, що має вирішуватися концепцією. Концепція має забезпечити єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) і служити підставою для створення програм розвитку сфери ТЗІ.

Також у загальних положеннях концепції визначено, що ***ТЗІ –*** *це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.*

Показано, що зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку ТЗІ.

Визначено, що напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації,

і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

При цьому приведення інформаційних відносин у сфері ТЗІ у відповідність з міжнародними стандартами сприятиме утвердженню України у світі як демократичної правової держави.

У розділі II концепції "Загрози безпеці інформації та стан її технічного захисту" показано, що впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо, радіотехнічної, оптико-електронної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок.

За таких умов створилися можливості ***витоку інформації, порушення її цілісності*** та ***блокування***. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформа-

ції, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері. Загрози безпеці інформації в Україні зумовлені:

- не виваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;

- діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

- недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;

- діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямованою на одержання переваги у політичній боротьбі та конкуренції;

- злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ (далі – засоби забезпечення ТЗІ);

- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Стан ТЗІ зумовлюється:

- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;

- недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення ТЗІ;

- незавершеністю створення системи сертифікації засобів забезпечення ТЗІ;

- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

У розділі ІІІ концепції "Система ТЗІ" визначено, що ***система ТЗІ*** – *це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами (далі – організаційні структури), нормативно-правова та матеріально-технічна база*.

Зазначено, що правову основу забезпечення ТЗІ в Україні становлять Конституція України, "Концепція (основи державної політики) національної безпеки України", Закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію", інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Принципами формування і проведення державної політики у сфері ТЗІ є:

- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;

- комплексність, повнота та безперервність заходів ТЗІ;

- відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

- узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;

- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях (далі – державні органи, підприємства, установи і організації);

- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій;

- покладення відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

- ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю у межах повноважень, визначених нормативно-правовими актами;

- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

- скоординованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;

- фінансова забезпеченість системи ТЗІ за рахунок Державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Основними функціями організаційних структур системи ТЗІ є:

- оцінка стану ТЗІ в державі, визначення пріоритетних напрямів його розвитку;

- розвиток правових засад удосконалення системи ТЗІ;

- виявлення та прогнозування загроз безпеці інформації;

- забезпечення інженерно-технічними заходами захисту інформації, що підлягає технічному захисту;

- створення умов для ТЗІ, що здійснюється суб'єктами інформаційних відносин на власний розсуд;

- формування та забезпечення реалізації державної політики щодо створення та впровадження вітчизняних засобів забезпечення ТЗІ;

- створення національної системи стандартизації та нормування у сфері ТЗІ;

- організація фундаментальних і прикладних науково-дослідних робіт та розробок у сфері ТЗІ;

- забезпечення взаємодії організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;

- організація створення та виконання програм розвитку ТЗІ;

- забезпечення ліцензування підприємницької діяльності в сфері ТЗІ;

- організація контролю за якістю засобів забезпечення ТЗІ шляхом їх сертифікації;

- організація контролю за відповідністю вимогам ТЗІ об'єктів, діяльність яких пов'язана з інформацією, що підлягає технічному захисту, шляхом їх атестації;

- організація контролю за ефективністю ТЗІ на об'єктах, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- забезпечення підготовки фахівців для роботи у сфері ТЗІ;

- сприяння залученню інвестицій і вітчизняного товаровиробника у сферу ТЗІ;

- організація міжнародного співробітництва в сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;

- забезпечення (кадрове, фінансове, нормативне, матеріально-технічне, інформаційне тощо) життєдіяльності складових організаційних структур системи ТЗІ.

Розділ IV концепції визначає основні напрями державної політики у сфері ТЗІ. Зокрема у ньому прийнято, що державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

Основними ***напрямами державної політики у сфері ТЗІ*** є:

- нормативно-правове забезпечення:

- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;

- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

- удосконалення правових механізмів організаційного забезпечення ТЗІ;

- удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;

- розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;

- удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації та засобів забезпечення ТЗІ;

- розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;

- розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ:

- у засобах обчислювальної техніки, в автоматизованих системах, оргтехніці, мережах зв'язку, комп'ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту;

- під час створення, експлуатації та утилізації зразків озброєнь, військової та спеціальної техніки;

- під час проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об'єктів;

- організаційне забезпечення:

- забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

- підготовка кадрів для роботи у сфері ТЗІ;

- залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

- розвиток міжнародного співробітництва в сфері ТЗІ;

- науково-технічна та виробнича діяльність:

- моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

- створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

- обґрунтування критеріїв та показників рівнів ТЗІ;

- створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

- створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

- системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

- пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

- створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є:

- створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

- визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

- визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ в органах державної влади та органах міс-

цевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;

- налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;

- завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;

- визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Значущість забезпечення ТЗІ, його наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади, академій наук.

Слід додати, що одночасно з створенням правових та організаційних основ ТЗІ були створені правові та організаційні основи криптографічного захисту інформації.

У травні 1998 р. прийнято Указ Президента України “Про Положення про порядок здійснення криптографічного захисту інформації в Україні” (відповідно, саме положення було підготовлено дещо раніше).

У липні 2002 року був прийнятий Закон України “Про Національну систему конфіденційного зв'язку“, у січні 2003 р. надано розпорядження Президента України **“**Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку“, з дорученням Президента Кабінету Міністрів щодо практичної організації такої системи.

Таким чином, створення необхідних правових та організаційних основ інформаційної безпеки було завершено.

Основні принципи, норми та положення прийнятих законів та підзаконних актів відповідають загальноприйнятим міжнародно-правовим стандартам, в тому числі міжнародним конвенціям з прав людини.

Цими законами було закладено основні підвалини інформаційної безпеки України. Подальший розвиток цієї сфери державного будівництва вимагатиме удосконалення інфраструктури захисту інформації та законів і численних підзаконних актів та нормативних документів, якими регламентується діяльність цієї інфраструктури, а також діяльність органів державного управління, установ та організацій науки й виробництва, які використовують у своїй діяльності інформацію з обмеженим доступом.

Висновки до розділу 1

На теперішній час в Україні розроблено основна правова та нормативна база, та створена інфраструктура, що має забезпечити надійний захист інформації у державі.

Разом з тим слід пам'ятати, що технічні способи несанкціонованого зняття інформації та засоби протидії цим протиправним діям знаходяться у постійному розвитку.

Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки.

Перелік питань для самоконтролю до розділу 1

1. Надайте визначення інформаційної сфери.
2. Надайте визначення єдиного інформаційного простору країни.
3. Надайте визначення інформаційних ресурсів.
4. Надайте визначення інформаційної війни.
5. Надайте визначення інформаційної зброї.
6. Надайте визначення загрози інформаційній безпеці.

7. Надайте визначення незаконного використання інформаційних і телекомунікаційних систем і інформаційних ресурсів.

8. Надайте визначення несанкціонованого втручання в інформаційні і телекомунікаційні системи й інформаційні ресурси.

9. Надайте визначення життєво важливих структур.

10. Надайте визначення міжнародного інформаційного тероризму.

11. Надайте визначення міжнародної інформаційної злочинності.

12. Які складові включає у себе інформаційна інфраструктура?

13. Надайте визначення організаційних структур.

14. Надайте визначення інформаційно-телекомунікаційних структур.

15. Надайте визначення інформаційної безпеки.

16. Які базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України?

17. Які правові основи інформаційної діяльності закладено у Закон України “Про інформацію”?

18. Надайте визначення інформації згідно зі ст. 1 Закону України “Про інформацію”.

19. Які основні види інформації визначаються у Законі України “Про інформацію”?

20. Як поділяється інформація за режимом доступу до неї?

21. Як здійснюється контроль за режимом доступу до інформації?

22. Як поділяється за своїм правовим режимом інформація з обмеженим доступом?

23. Яка інформація відноситься до конфіденційної?

24. Яка інформація не може бути конфіденційною?

25. Яка інформація відноситься до таємної інформації?

26. Чим та як визначається інформація, що складає державну таємницю?

27. Чим визначається ступень таємності інформації?

28. Які грифи таємності можуть надаватися інформації та який їх терміни дії?

29. Яка інформація входить до інформаційних ресурсів України?

30. Чим забезпечується інформаційний суверенітет України?

31. Які національні інтереси України потрібно захищати у відповідності до Закону України “Про основи національної безпеки України” та “Концепції національної безпеки України”?

32. Що визначає “Концепція національної безпеки України”?

33. Коли та як була затверджена “Концепція технічного захисту інформації в Україні”?

34. Що визначає та має забезпечити “Концепція технічного захисту інформації в Україні”?

35. Надайте визначення ТЗІ.

36. Чим зумовлені загрози безпеці інформації в Україні?

37. Чим зумовлюється стан ТЗІ в Україні?

38. Надайте визначення системи ТЗІ.

39. Що складає правову основу забезпечення ТЗІ в Україні?

40. Які принципи формування і проведення державної політики у сфері ТЗІ?

41. Які основні функції організаційних структур системи ТЗІ?

42. Які основні напрями державної політики у сфері ТЗІ?

43. Які першочергові заходи щодо реалізації державної політики у сфері ТЗІ?

Перелік рекомендованої літератури до розділу 1

1. Конституція України // Урядовий кур’єр, 13 липня 1996 р.

2. Закон України “Про основи національної безпеки України”// Урядовий кур’єр, 30 липня 2003 р.

3. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

4. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

5. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

6. Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.

7. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.

8. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.

9. Кримінальний кодекс України.

10. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР, 1984. – додаток до № 51. – Ст. 1122; із змінами 1985 – 2005 рр.

11. Наказ МВС України “Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації в органах і підрозділах внутрішніх справ України” від 25 липня 2002 р. № 745.

12. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : наказ МВС України від 12.10.2009 року № 436.

13. Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : наказ МВС України від 10.03.2010 року № 75.

14. Сайти з законодавства // Електронний ресурс: www.rada.gov.ua ; http://www.nau.kiev.ua.

15. Сайт Київської національної академії внутрішніх справ // Електронний ресурс: www.naiau.kiev.ua

РОЗДІЛ 2. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. СПОСОБИ НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ЇЇ ВИТОКУ

2.1. Поняття технічного каналу витоку інформації

ТЗІ призначений для її захисту від витоку по технічних каналах витоку інформації.

На теперішній час для несанкціонованого зняття інформації широко використовуються технічні канали витоку інформації (ТКВІ).

Що являють собою такі канали? Надамо спочатку загальне визначення. ***Технічний канал витоку інформації*** *– це сукупність небезпечних фізичних сигналів, середи їх розповсюдження та зберігання,* ***об'єкту технічної розвідки*** *й* ***способів*** *і* ***засобів*** *технічної розвідки, що можуть бути застосовані для зняття інформації з об'єкту, що охороняється* [8].

Небезпечний фізичний сигнал (*небезпечний сигнал*) *– це сигнал, що містить інформацію, яку необхідно захищати*.

В нашій країні прийнято поділяти ТКВІ за наступною класифікацією:

- ***акустичні канали витоку*** інформації, куди входять також канали з ***акустично-електричними перетвореннями***;

- ***радіотехнічні канали витоку*** інформації, куди входять, по-перше, відкриті канали радіотехнічного зв'язку та, по-друге, канали, що утворюються за рахунок ***паразитних випромінювань та наводок***;

- ***оптичні канали витоку*** інформації;

- ***речовий канал витоку*** інформації, який визначається людським фактором [8].

ТКВІ можуть бути ***природними*** та ***штучними***, в тому числі створеними навмисно. Природні ТКВІ утворюються на базі фізичних властивостей джерел виникнення небезпечних сигналів, самих небезпечних сигналів та середовища їх розповсюдження. Для навмисного створення ТКВІ можуть ви-

користовуватися зміни фізичних властивостей джерел та середовищ розповсюдження небезпечних сигналів, а також поданням спеціальних сигналів на окремі елементи приміщення. Це, за правило, робиться шляхом конструктивних змін джерел та конструкції об'єкту, де розповсюджуються небезпечні сигнали [9]. Але для зняття інформації з ТКВІ завжди використовується ***апаратура технічної розвідки***.

Крім того, сама апаратура технічної розвідки, розміщена на об'єкті, що охороняється, утворює ***навмисний канал витоку інформації.***

На рис. 2.1 показано загальну класифікацію видів інформації, яка може бути об'єктом злочинних посягань. Це оптична, акустична, електронна, електромагнітна та письмова (друкована) інформація.

Відповідно, всі види інформації мають різну фізичну природу її походження, носіїв і каналів розповсюдження та зберігання, або різні параметри одного й того ж явища, яке може бути покладене в основу для її переносу чи зберігання.

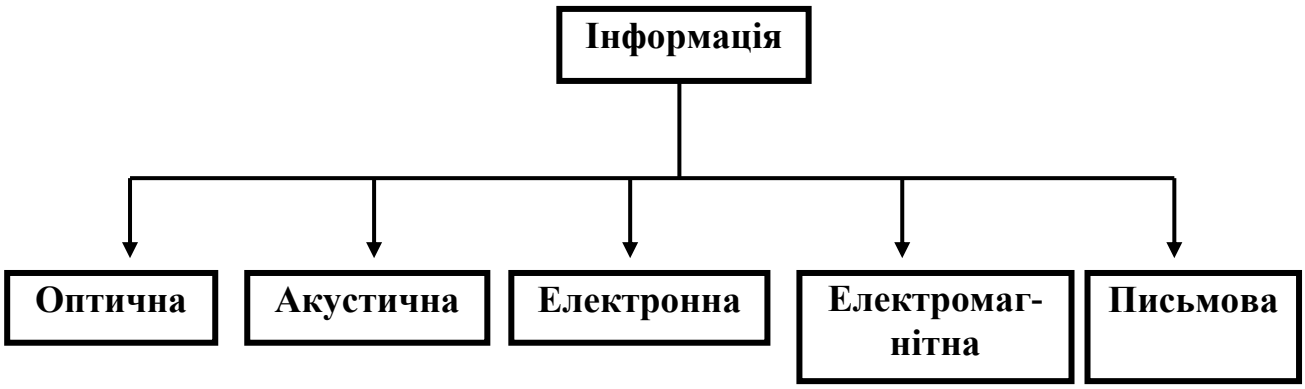

Рис. 2.1. Загальна класифікація видів інформації, що може бути об'єктом злочинних посягань

Зрозуміло, що проведення робіт з розробки, впровадженню та підтримки й перевірки працездатності системи ТЗІ на об'єкті, що охороняється, вимагає проведення певних ***організаційно-технічних заходів***.

Їх проведення призначено для забезпечення надійності захисту інформації на об'єкті. Одне з найважливіших завдань при цьому є виявлення та блокування всіх потенційних каналів витоку інформації з об'єкту.

Друге завдання – це постійна перевірка працездатності та надійності функціонування системи технічного захисту.

Саме в цих заходах полягає сутність ТЗІ.

2.2. Загальний підхід до технічного захисту інформації

Класична схема обробки та розповсюдження інформації відома з теорії інформації та показана на рис. 2.2.

Вона містить передавач інформації, ***канал зв'язку*** (або канал зберігання, чи обидва канали разом) інформації, та приймач (який може мати систему вторинної обробки) інформації.

З позиції класичної теорії інформації канал зв'язку є найбільш уразливою ділянкою для дії завади.

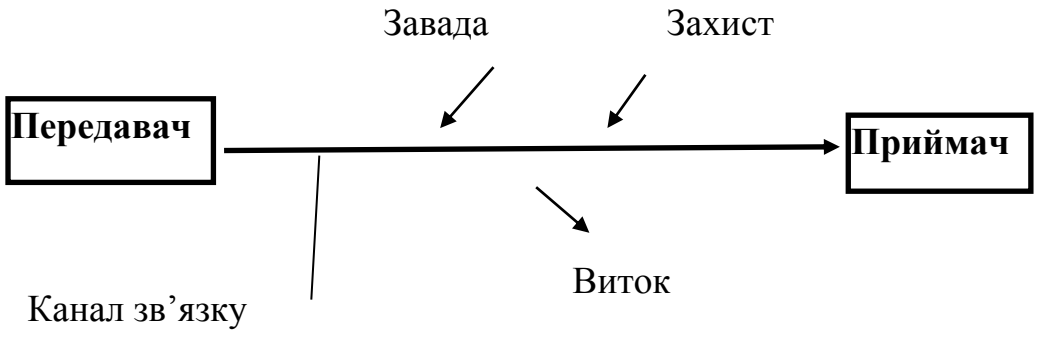

Рис. 2.2. Класична схема обробки, розповсюдження та захисту інформації

Це ж правило діє і при розгляді проблем захисту інформації. Але з точки зору захисту інформації канал зв'язку можна розглядати з двох позицій:

1. Як канал витоку.

2. Як ділянку, що зручна для захисту.

Це буде розглянуто далі при класифікації каналів витоку, яка випливає з класифікації способів несанкціонованого зняття інформації, та в наступних темах, присвячених методам і засобам її захисту. Але при розгляді каналів витоку інформації, способів її викрадення та методів блокування цих посягань ми не торкаємося звичайних способів крадіжки письмової інформації та її носіїв, оскільки це є речовий канал, розгляд якого у цьому посібнику не передбачається.

Основними об'єктами захисту інформації [8] є:

- інформаційні ресурси, які мають відомості, віднесені до таємної або конфіденційної інформації;
- засоби і системи інформації (інформаційно-обчислювальні комплекси), в тому числі: програмні засоби (системи управління базами даних, операційні системи та інше), автоматизовані системи управління, системи зв'язку і передачі даних, технічні засоби прийому, передачі і обробки інформації обмеженого доступу, їх інформативні фізичні поля. Тобто системи і засоби, що безпосередньо обробляють інформацію, яка віднесена до таємної або конфіденційної;
- системи, що не віднесені до засобів і систем інформатизації, але розташовані в приміщеннях, де оброблюється конфіденційна інформація. Такі технічні засоби і системи звуться ***додатковими технічними засобами і системами*** (ДТЗС). До них відносять: технічні засоби відкритого телефонного зв'язку, засоби оповіщення, системи пожежної та охоронної сигналізації, радіофікації, годинофікації, електропобутові прилади та інші, а також самі приміщення, що призначенні для обробки інформації з обмеженим доступом.

Окремі технічні засоби або група технічних засобів, що призначені для обробки конфіденційної інформації, разом з приміщеннями, де вони розташовуються, складають ***об'єкт технічних засобів прийому, переробки, зберігання і передачі інформації*** (ТЗПІ).

2.3. Фізичні основи утворення технічних каналів витоку інформації

У відповідності до прийнятої класифікації поділу ТКВІ розглянемо почергово фізику утворення акустичних, радіотехнічних та оптичних каналів.

Спочатку розглянемо фізичні основи утворення акустичних каналів витоку інформації, при цьому особливу увагу приділимо *акустично-електричними перетвореннями*.

Сама назва каналів витоку свідчить про те, що небезпечними сигналами, що можуть витікати через нього, є акустичні сигнали.

Що є акустичний сигнал? ***Акустичний сигнал*** **–** це механічні коливання часток пружного середовища [10].

Отже, виходячи з цього визначення, акустичні сигнали можуть розповсюджуватися у будь-якому пружному середовищі. Єдине середовище, в якому розповсюдження акустичного сигналу неможливо, – повний вакуум (відсутні частинки повітря, тобто немає пружної середи).

Саме цим пояснюється можливість проходження акустичних сигналів через елементи будівельних конструкцій (стіни, стелі, підлоги, двері, скло вікон, труби і т. інше).

Акустичний сигнал може безпосередньо прийматися слуховими органами людини та інших живих істот.

При цьому людина сприймає ***акустичні коливання*** у ***діапазоні частот*** від 20 до 20000 Гц (Герц). Цей діапазон зветься ***звуковим*** діапазоном частот. Нагадаємо, що частоті 1 Гц відповідає коливання, яке утворює повний період за 1 секунду, як показано на рис. 2.3. Отже частота сигналу, це кількість повних періодів коливання за 1 секунду.

Крім звукового, розділяють ***інфразвуковий*** (від 0 до 20 Гц) та ***ультразвуковий*** (вище 20000 Гц) діапазони частот. Ці частоти чує більшість тварин, але люди їх не чують.

Для того, щоб передати звук по каналах зв’язку або запам’ятати у приладах звукозапису, акустичний сигнал необхідно перетворити у адекватний

йому електричний сигнал. Для такого перетворення використовується спеціальний перетворювач – ***мікрофон***. Для зворотного перетворення використовується гучномовці. Принцип перетворення акустичного сигналу в електричний показано на прикладі вугільного мікрофону, приведеного на рис. 2.4.

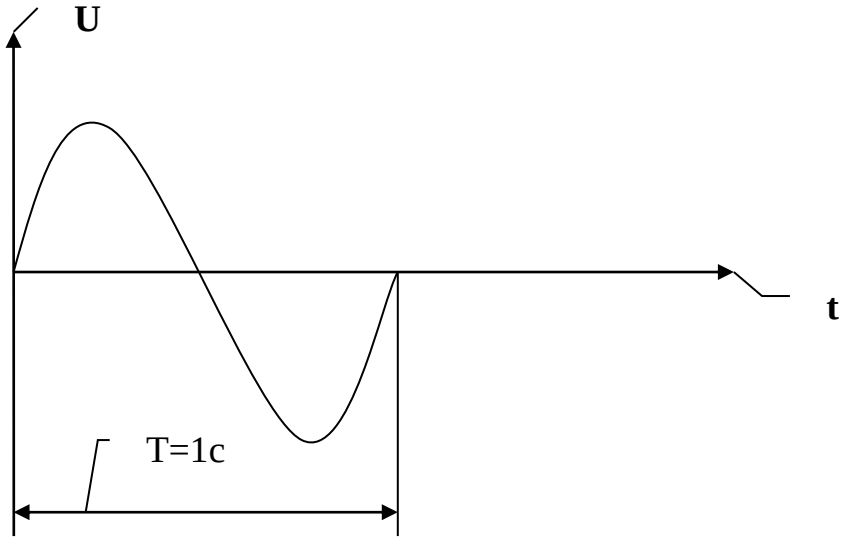

Рис. 2.3. Приклад гармонійного коливання з частотою 1 Гц.

Мікрофон побудований на ефекті зміни електричного опору вугільного порошку під дією механічного тиску акустичних коливань на мембрану мікрофону.

Конструктивно мікрофон являє собою круглу циліндричну металеву коробку із засипаним в неї вугільним порошком. На верхню частину циліндра накладено діелектричну пружну прокладку, на яку зверху кладеться металева мембрана. Конструкція затягується кришкою (на рис. 2.4 її не показано).

До циліндру з порошком та мембрани підключені два різних полюси джерела постійного току (батареї). Оскільки вугільний порошок проводить електричний струм, то через первинну обмотку трансформатору протікає постійний струм. Але під дією звукових коливань мембрана стискує порошок,

що призводить до зміни його опору. Завдяки цьому у струмі, що протікає у замкнутому ланцюгу, виникає змінна складова, яка передається через підвищувальний трансформатор. Частота і рівень сигналів змінної складової еквівалентні частоті та рівню звукових коливань, що потрапляють на мембрану мікрофона.

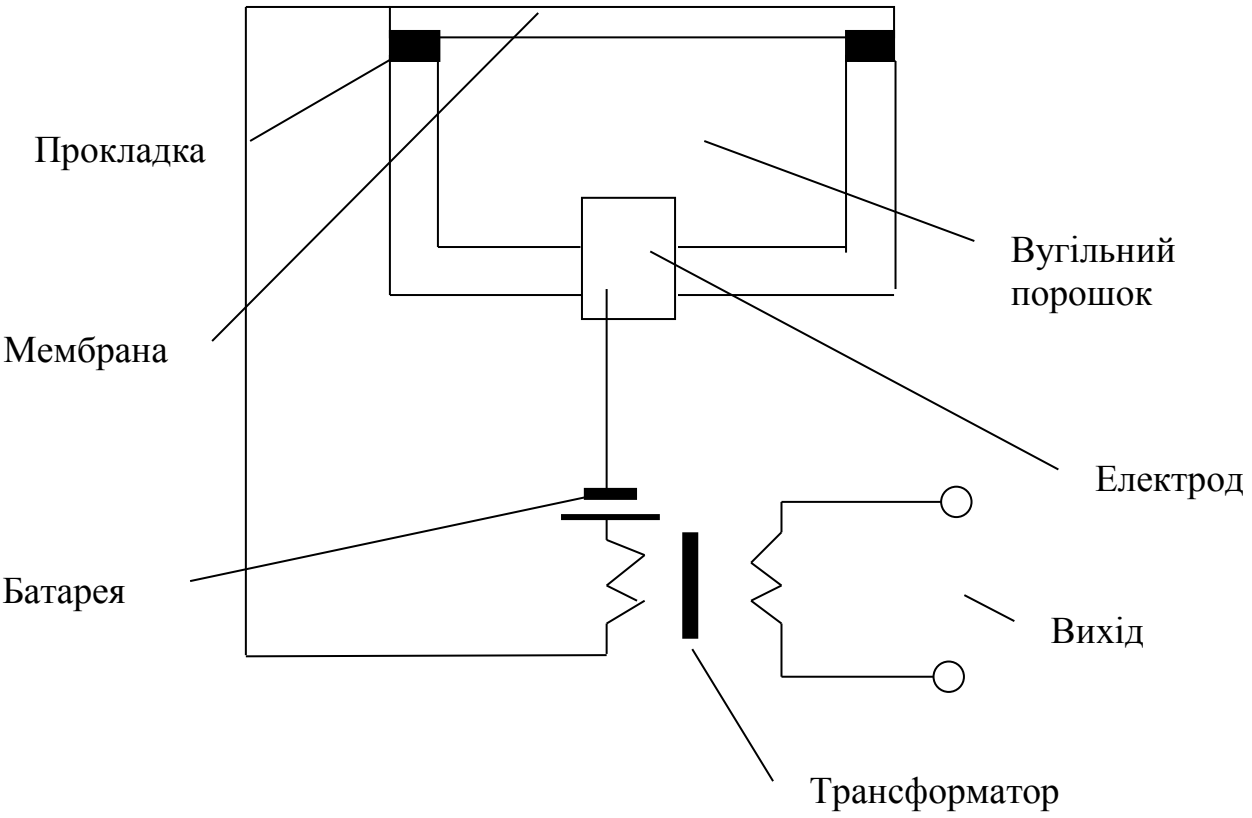

Рис. 2.4. Конструкція вугільного мікрофону

Вугільний мікрофон є найпростішим мікрофоном з найгіршими характеристиками перетворення. Він вносить найбільші спотворення у перетворювані сигнали. Та це й не дивно, адже цей мікрофон був першим типом мікрофонів, створених людством.

На теперішній час використовуються динамічні, конденсаторні та електретні мікрофони. Вони є обов’язковою складовою всіх засобів зняття акустичної інформації.

Але багато інших елементів різних електричних та електронних приладів можуть бути використані для зняття акустичної інформації за рахунок акустоелектричних перетворень, що виникають за рахунок так званого **"*мікрофонного ефекту*"**. Принцип його виникнення можна пояснити на прикладі звичайного телефону. Відомо, що на телефон від лінії подається постійний струм з напругою 45 В. Також відомо, що у вхідному каскаді телефону завжди є трансформатор, що підключається до цієї лінії. Сам телефон знаходиться у середовищі повітря, отже на трансформатор діє акустичні сигнали розмов, що ведуться у приміщенні, де цей телефон знаходиться. При цьому по телефону у цей час розмови не ведуться. Але акустичні хвилі тиснуть на феритовий сердечник трансформатора, що викликає у ньому появу змінного магнітного поля, яке виникає завдяки явищу ***магнітострикції.***

Поява змінного магнітного поля призводить до виникнення змінного струму в обмотках трансформатора за рахунок явища ***самоіндукції*** у відповідності до законів Фарадея та Ленца. А цей струм можна зняти безпосередньо з телефонної лінії, підключеної до телефонного апарату.

Крім того, акустичні хвилі тиснуть на обмотки трансформатора, що викликає у них зміну величини ***паразитної міжвиткової ємності***. Це, у свою чергу, призводять до зміни ***власної резонансної частоти*** обмоток трансформатора. Такі ж ефекти виникають при дії акустичного сигналу на будь-які котушки індуктивності.

Слід додати, що уникнути наявності паразитної міжвиткової ємності та власної резонансної частоти у індуктивностях неможливо, оскільки вони є фізичними властивостями таких елементів.

Всі ці зміни відбуваються з частотою акустичного сигналу, що діє на згадані елементи, та пропорційно рівню його тиску.

Отже, всі розмови у кімнаті можна зняти користуючись "мікрофонним ефектом" та ефектом зміни власної ***резонансної частоти***, що виникають на трансформаторах або котушках індуктивності будь-якого ДТЗС [9].

Виникнення змінного струму у обмотках трансформатора телефону проілюстровано на рис. 2.5.

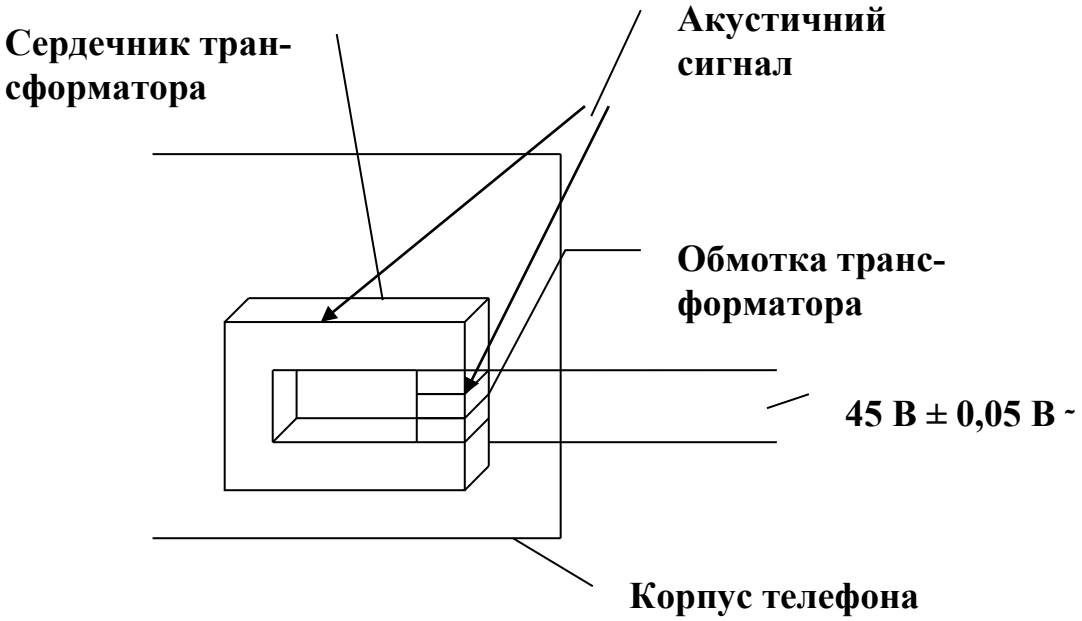

Рис. 2.5. Механічна дія акустичного сигналу на трансформатор телефону

Зрозуміло, що для зняття інформації з використанням цих ефектів необхідно користуватися спеціальною апаратурою технічної розвідки.

Розглянемо радіотехнічні канали витоку інформації. Почнемо з відкритих каналів радіозв'язку. Головною особливістю радіозв'язку є використання процесу ***модуляції*** для передавання інформаційних (корисних) сигналів. Його сутність полягає у тому, що для переносу на відстань корисного сигналу використовується ***сигнал-переносник***, на який "садять" інформаційний сигнал. Процес реалізується перемноженням цих двох сигналів. У результаті процесу модуляції утворюються ***модульовані*** сигнали, які й випромінюються у ефір. Процес модуляції застосовується для забезпечення передавання низькочастотних ***інформаційних сигналів*** з найменшими енергетичними затратами, оскільки високочастотні сигнали-переносники для свого ви-

промінювання та розповсюдження вимагають набагато менших енергетичних витрат, ніж низькочастотні.

Сигнал-переносник називають ***сигналом, що модулюється*** (інколи ***несучим*** сигналом або коливанням), а інформаційний сигнал – ***модулюючим сигналом***.

Зрозуміло, що частота несучого коливання завжди значно більша, ніж частота інформаційного сигналу.

Існують основні три види модуляції: ***амплітудна, частотна*** та ***фазова***. При амплітудній модуляції інформаційний сигнал у модульованому коливанні проявляється у зміні амплітуди несучого коливання, при частотній – у змінах частоти, при фазовій – у змінах фази [11].

З переходом на цифрові методи зв'язку використовується також ***амплітудноімпульсна*** модуляція, але вона застосовується лише при перетвореннях безперервних сигналів у цифрові та не використовується при випромінюванні радіосигналів у ефір.

Припустимо, що інформаційний сигнал визначається функцією $s_1(t) = A_m \sin\Omega t$, а сигнал-переносник функцією $s_2(t) = B_m \cos\omega t$. Тоді модульований сигнал слід записати як

$$s_M(t) = A_m \sin\Omega t \bullet B_m \cos\omega t = \frac{A_m B_m}{2}\left[\sin(\Omega+\omega)t + \sin(\Omega-\omega)t\right], \qquad (2.1)$$

де

Ω – частота інформаційного сигналу,

ω – частота сигнала-переносника,

A_m – амплітуда інформаційного сигналу,

B_m – амплітуда сигнала-переносника.

Таким чином, у модульованому коливанні присутні всі компоненти інформаційного сигналу, які можна виділити у процесі ***демодуляції*** **(*детектування*)**.

Розглянемо фізичні основи каналів витоку, що утворюються за рахунок *паразитних випромінювань та наводок*.

Будь-який електронний прилад генерує паразитне випромінювання на суто індивідуальній власній частоті.

Це явище викликається численними ***паразитними ємнісними зв'язками***, що обов'язково утворюються між дротами, друкованими струмопроводами, ніжками електрорадіоелементів та т. інше.

При цьому виникають нові ***паразитні ланцюги***, появу яких передбачити неможливо при проектуванні приладів та у процесі їх виробництва.

Ці паразитні ланцюги призводять до появи ***паразитних позитивних зворотних зв'язків***, що й перетворює будь-який (навіть низькочастотний) електронний прилад (наприклад, підсилювач) у передавач, що випромінює в ефір паразитні коливання на високих та зверхвисоких частотах [9].

При проектуванні та виробництві більшості побутових апаратів на ці випромінювання не звертають уваги, оскільки вони не впливають на виконання апаратурою своїх функцій. Лише при проектуванні та виробництві спеціальної та захищеної апаратури цим параметрам приділяється значна увага.

Оскільки такі коливання високочастотні, то вони, не зважаючи на їх малу потужність, можуть розповсюджуватися на сотні метрів. А у зв'язку з тим, що у будь-якій апаратурі присутні нелінійні елементи (транзистори та транзисторні мікросхеми), на них відбувається модуляція інформаційними сигналами, що обробляються в апаратурі, сигналу паразитного випромінювання [9].

Крім того, що такі сигнали можуть бути перехоплені з ефіру, вони ще гарантують утворення наводок.

Наводка *– це сигнал, що утворюється у будь-якій струмопровідній конструкції (наприклад, на трубах центрального опалення) через явище самоіндукції.* Тобто, змінне електромагнітне поле (електромагнітна хвиля), по-

падаючи на будь-який нерухомий провідник, викликає в останньому появу змінного струму.

А оскільки паразитне випромінювання несе на собі небезпечні сигнали, то їх можна зняти з будь-яких струмопровідних конструкцій та мереж.

Фізичні основи оптичних каналів витоку інформації розглядати не має сенсу, оскільки вони надаються у курсі спеціальної техніки.

2.4. Організаційно-технічні заходи щодо ТЗІ на об'єкті

Система захисту об'єктів від витоку інформації складається, в основному, із організаційних і технічних заходів, метою яких є ліквідація або суттєве зменшення можливості витоку конфіденційної інформації, а також контролю захищеності технічних засобів в період їх експлуатації.

Організаційний захід *– це захід по захисту інформації, проведення якого не потребує застосування спеціально розроблених технічних засобів.*

До основних організаційних і режимних заходів відносяться:

- проведення робіт із захисту інформації організаціями, які мають ліцензію на діяльність в сфері захисту інформації, виданою відповідними органами;
- ***категоріювання*** та ***атестація*** об'єктів ТЗПІ і виділених для проведення закритих заходів приміщень по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеню таємності;
- використання на об'єкті сертифікованих ТЗПІ та ДТЗС;
- встановлення ***контрольованої зони*** біля об'єкта;
- залучення до робіт з будівництва, реконструкції об'єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в сфері захисту інформації по відповідним пунктам;
- організація ***контролю*** і ***обмеження доступу*** на об'єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, що підлягають захисту;

- відключення на період закритих заходів технічних засобів, що мають елементи, які виконують роль ***електроакустичних перетворювачів*** (лінії зв'язку тощо) [4,8,9].

Технічний захід *– це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.*

Технічні заходи включають:

- встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

- перевірку техніки, яка використовується, на відповідність величини ***паразитних випромінювань*** допустимим рівням;

- ***екранування*** приміщень або техніки, яка використовується;

- перемонтаж окремих мереж, кабелів та ліній зв'язку;

- застосування спеціальних пристроїв і засобів захисту;

- використання засобів активного захисту;

- перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз [4,8,9].

На початку робіт з ТЗІ необхідно визначити види інформації та від якого роду загроз треба захищатися. Для цього в першу чергу визначають ***категорію приміщення***. При цьому з'ясовують види та ступень таємності інформації, що може циркулювати у приміщенні. Далі розглядаються конструктивні особливості приміщення та умови його розташування, наявність побутової техніки та апаратури для обробки інформації, її типи та технічні характеристики. З'ясовується та враховується наявність біля об'єкту, що треба захищати, іноземних установ, автостоянок, приватних фірм (тобто місць, з яких можна організувати стаціонарне та мобільне зняття інформації). Заміряється відстань до таких місць і визначається ***охоронна зона***, в межах якої несанкціоноване зняття інформації вважається неможливим. Це надає змогу з'ясувати

типи та ступень можливих загроз та встановити відповідну ***категорію захисту інформації.***

Якщо поряд з об'єктом є іноземні установи чи фірми, де можна організувати стаціонарне зняття інформації, категорійність приміщення підвищується на один ступень.

Складається акт про встановлення категорійності приміщення, в якому відбиваються всі питання, що перераховані вище. Такий акт складається представниками підрозділу з ТЗІ та членами комісії, яка призначається керівником установи, де проводяться такі роботи [9].

Встановлення категорійності приміщення надає змогу скласти план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об'єкті. Ці роботи повинен проводити ***ліцензіант***, тобто установа, яка має державну ліцензію на проведення таких робіт. Надалі всі роботи з ТЗІ проводяться ліцензіантом. Якщо в установі є підрозділ з ТЗІ, який має ліцензію на виконання всього потрібного обсягу робіт, то ці роботи можуть проводитися таким підрозділом.

При проведенні робіт з ТЗІ необхідно провести ряд заходів, зокрема:

- визначити та змонтувати необхідні технічні засоби, що потрібні для захисту інформації на об'єкті;

- провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Після проведення всього комплексу технічних робіт ліцензіант разом з замовником складають акт про надання об'єкту певної категорії із захисту інформації. Лише після одержання та затвердження такого акту на об'єкті можна обробляти інформацію з обмеженим доступом [9].

Технічний захист інформації від її несанкціонованого зняття полягає в застосуванні спеціальних технічних методів її захисту, які блокують поте-

нційні канали витоку інформації, тобто заважають спробам її незаконного отримання.

Для того, щоб захищати інформацію від витоку необхідно знати потенційні канали витоку та методи їх ***блокування.***

Починаючи вивчення методів та засобів технічного захисту інформації, слід зазначити, що при викладенні матеріалу обмежимося мінімумом тих фізичних і технічних даних, які необхідні для розуміння цього курсу.

Отже, спочатку розглянемо класифікацію каналів витоку та методів несанкціонованого зняття інформації. Такий порядок надання матеріалу пояснюється тим, що для того, щоб захищатися від якоїсь загрози, потрібно знати, що вона собою уявляє.

При цьому значну увагу приділимо сучасним способам беззаходового зняття інформації, зокрема, способу ***високочастотного нав'язування.***

2.5. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав'язування

Вперше зняття акустичної інформації способом високочастотного нав'язування (ВЧН) було проведено у 1945 р., коли делегація піонерів подарувала американському послу у СРСР зроблений власноруч у Палаці піонерів гіпсовий герб США, а розчулений посол повісив його у власному робочому кабінеті над своїм столом.

В "подарунок" був вмонтований пасивний акустичний резонатор, який опромінювався зовнішнім радіосигналом стабільної частоти, що відповідала власній резонансній частоті резонатора.

Під дією акустичних хвиль, що виникали при розмовах у кабінеті, резонансна частота резонатора змінювалася. Відповідно відбитий радіосигнал ставав модульованим сигналами від розмов, які велися у кабінеті.

Таким чином до 1951 р., коли спецслужби США нарешті виявили цю першу у світі ***пасивну радіозакладку***, керівництво СРСР знало зміст всіх ро-

змов, що велися у кабінеті посла США. Цей спосіб зняття інформації отримав назву ВЧН [12].

Надалі цей спосіб набув подальшого розвитку. Спеціалісти зрозуміли, що він може використовуватися для зняття інформації з будь-якого елемента, що має власну резонансну частоту.

Для того, щоб з'ясувати принцип ВЧН, необхідно розглянути явище резонансу у резонансному контурі.

На рис. 2.6 показано паралельний резонансний контур. Він складається з котушки з індуктивністю *L*, конденсатора з ємністю *C* та резистора з опором *R*.

Згадаємо з курсу фізики середньої школи, що індуктивний опір котушки $R_L = j\omega L$, ємнісний опір конденсатора $R_C = \frac{1}{j\omega C}$, кругова частота $\omega = 2\pi f$,

де L – індуктивність котушки, C – ємність конденсатора, f – частота гармонійного сигналу, що подається на котушку та конденсатор, $j = \sqrt{-1}$.

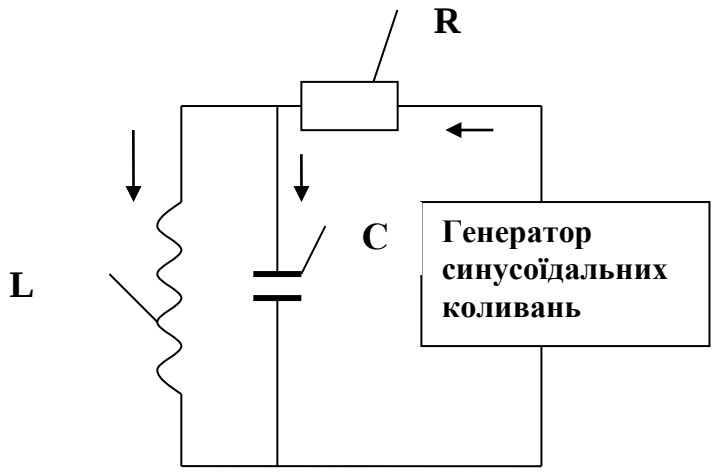

Рис. 2.6. Паралельний резонансний контур

З рис. 2.6 видно, що максимальний рівень напруги сигналу на котушці та конденсаторі у місці їх з'єднання з резистором буде тоді, коли струм у котушці та конденсаторі буде однаковим за своєю силою. Це й є умовою резонансу. Тобто, опір котушки та конденсатора на частоті резонансу рівні. Отже,

$$j\omega L = \frac{1}{j\omega C},$$

звідки резонансна частота

$$f = \frac{1}{2\pi\sqrt{LC}}.$$

Розглянемо ***частотну характеристику*** резонансного контуру (тобто залежність рівня напруги у точці з'єднання елементів L,C і R від частоти, що подається від генератора синусоїдальних коливань змінної частоти). З ростом частоти опір котушки зростає, а опір конденсатора падає. Тому, зліва від резонансу струм у контурі має індуктивний характер, справа – ємнісний, що і показано на рис. 2.7.

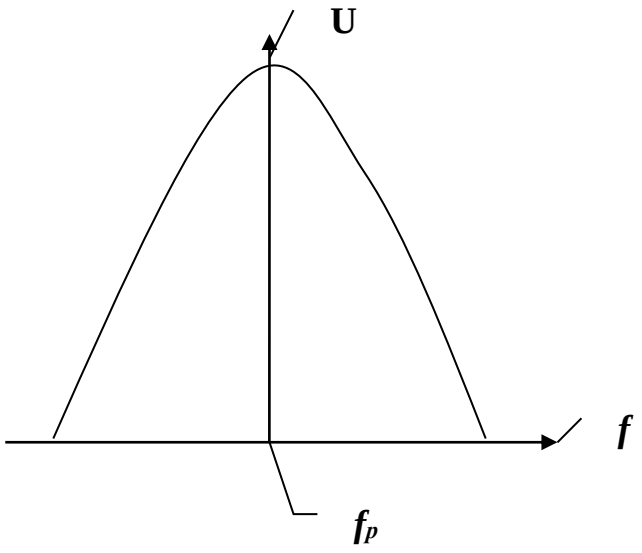

Рис. 2.7. Резонансна крива

При ВЧН на резонансний контур із зовні подається синусоїдальний сигнал резонансної частоти. Тиск акустичної хвилі змінює резонансну частоту контуру. При цьому резонансна крива і точка резонансу зміщується вліво або вправо від точки власної резонансної частоти, що була без дії акустичного сигналу. Частота зовнішнього сигналу при цьому не змінюється, отже він припадає на лівий або правий скат резонансної кривої, а відбитий сигнал стає модульованим мовним сигналом.

2.6. Класифікація каналів витоку інформації

Повторимо, що під технічним каналом витоку інформації розуміють сукупність об'єкта розвідки, ***технічного засобу розвідки*** (ТЗР), за допомогою якого збирається інформація про об'єкт, і фізичного середовища, де розповсюджується інформаційний сигнал.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР більш детально технічні канали витоку інформації можна поділити на:

- радіоканали (електромагнітне випромінювання радіодіапазону);
- електричні (засоби провідникового зв'язку та різні струмопровідні комунікації);
- акустичні (розповсюдження звукових коливань);
- оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектру).

На рис. 2.8 надано загальну характеристику каналів витоку оптичної, акустичної, електронної та електромагнітної інформації. Деякі з цих каналів можуть бути комбінованими, тобто бути каналами витоку для декількох видів інформації.

Так, скляні конструкції та вікна можуть бути каналами витоку для акустичної та оптичної інформації, але через них можна зняти також електронну

та друковану інформацію (зокрема, текст з екрану ПЕОМ). З телефонного апарату можна зняти акустичну інформацію, а також електронну та електромагнітну і т. п.

Отже, для розуміння принципів технічного захисту інформації треба знати способи і засоби її зняття, оцінити реальність загроз використання для цього різних каналів.

Способи та засоби зняття акустичної інформації, що використовуються нині, наведено на рис. 2.8 – 2.11 [9].

На рис. 2.9 наведено практично всі методи та засоби комбінованого зняття акустичної інформації: спочатку вказано канал витоку, а потім можливі способи та засоби зняття інформації. Відповідно до розташування та облаштування об'єкту, що охороняється, можливо використання різних каналів витоку. При цьому можуть використовуватися різні види перетворення та способи і засоби перенесення інформації. Наприклад, акустичну інформацію можна зняти в приміщенні за допомогою радіомікрофону, який живиться від струму електромережі, а можна виконати цю операцію за допомогою дротового мікрофону, який також підключено до електромережі. В цьому випадку інформація буде передаватися електромережею і її можна зняти навіть на трансформаторній підстанції.

Для зняття акустичної інформації з закритого приміщення дедалі частіше використовується так зване ВЧ-нав'язування, коли для зняття інформації використовується будь-який "цінний" подарунок (наприклад, картина або естамп), виконаний так, що він стає резонансним елементом модуляційної системи. При ВЧ опромінюванні цього елементу відбувається модуляція мовними сигналами спрямованого на цей елемент високочастотного радіовипромінювання. Таким самим чином, розрахувавши або експериментально з'ясувавши резонансні характеристики дзвінкового кола телефонного апарату чи, наприклад, трансформаторного кола радіоточки, можна зняти мовну інформацію за допомогою ВЧ-нав'язування (див. рис. 2.8).

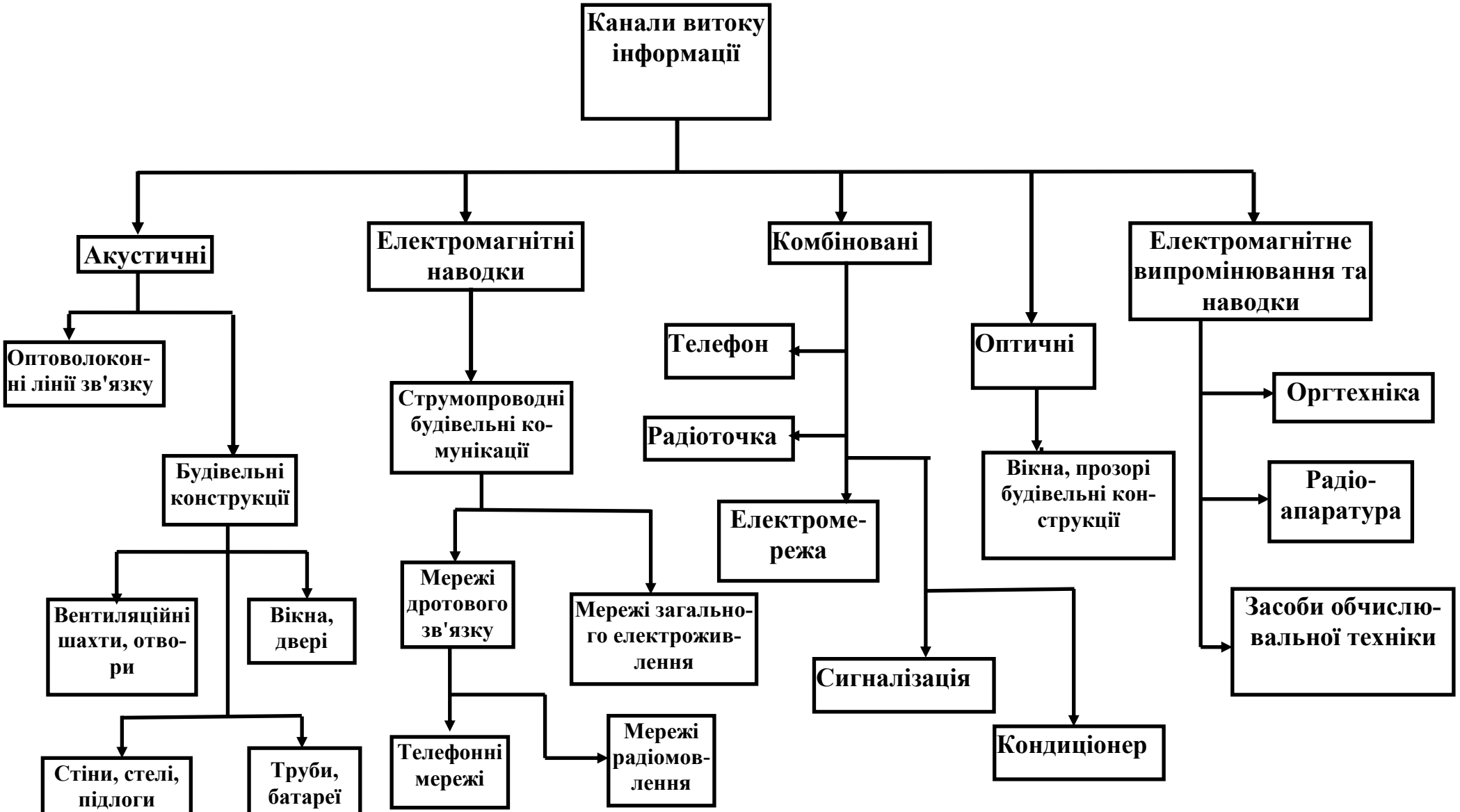

Рис. 2.8. Загальна характеристика каналів витоку інформації

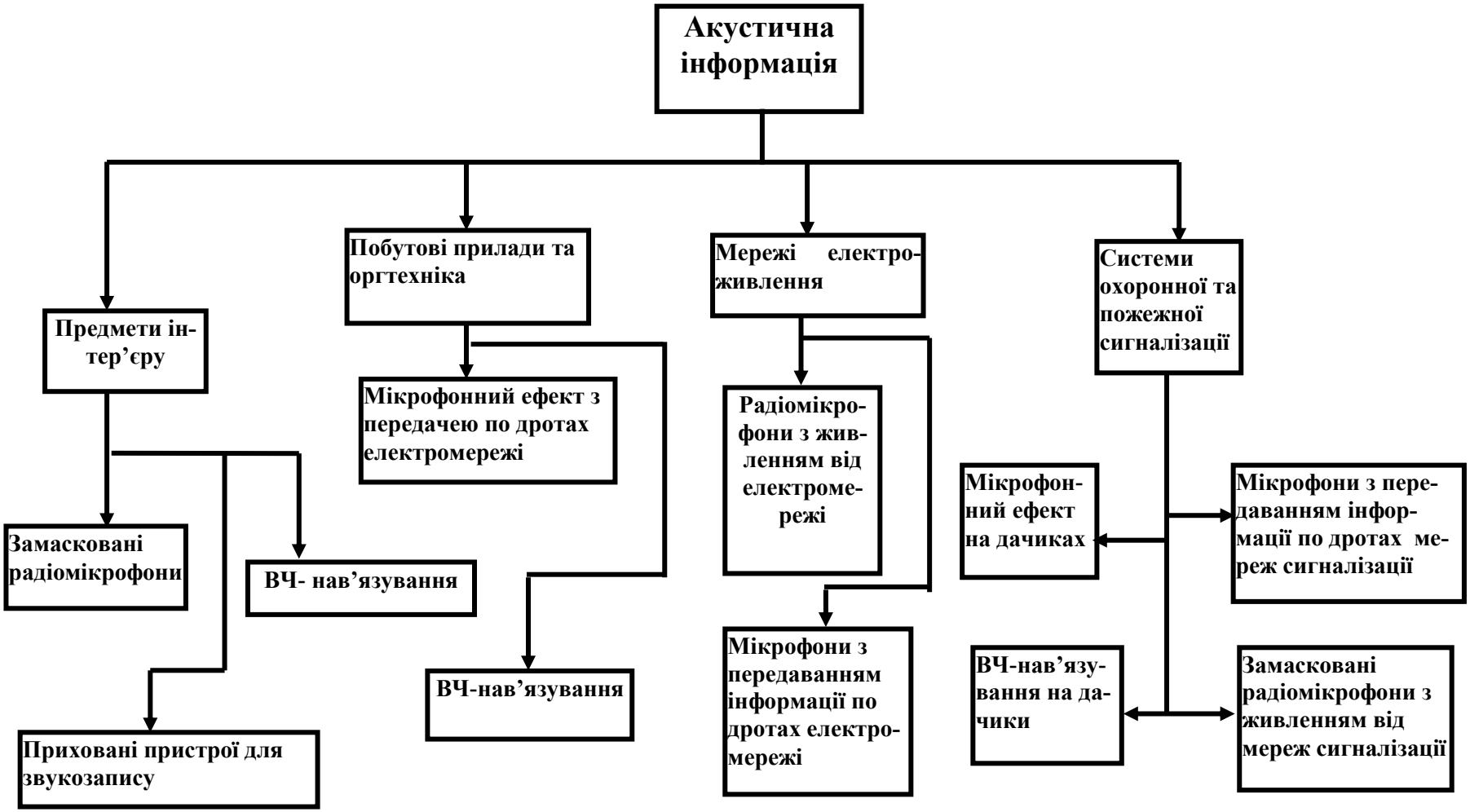

Рис. 2.9. Комбіновані методи та засоби зняття акустичної інформації

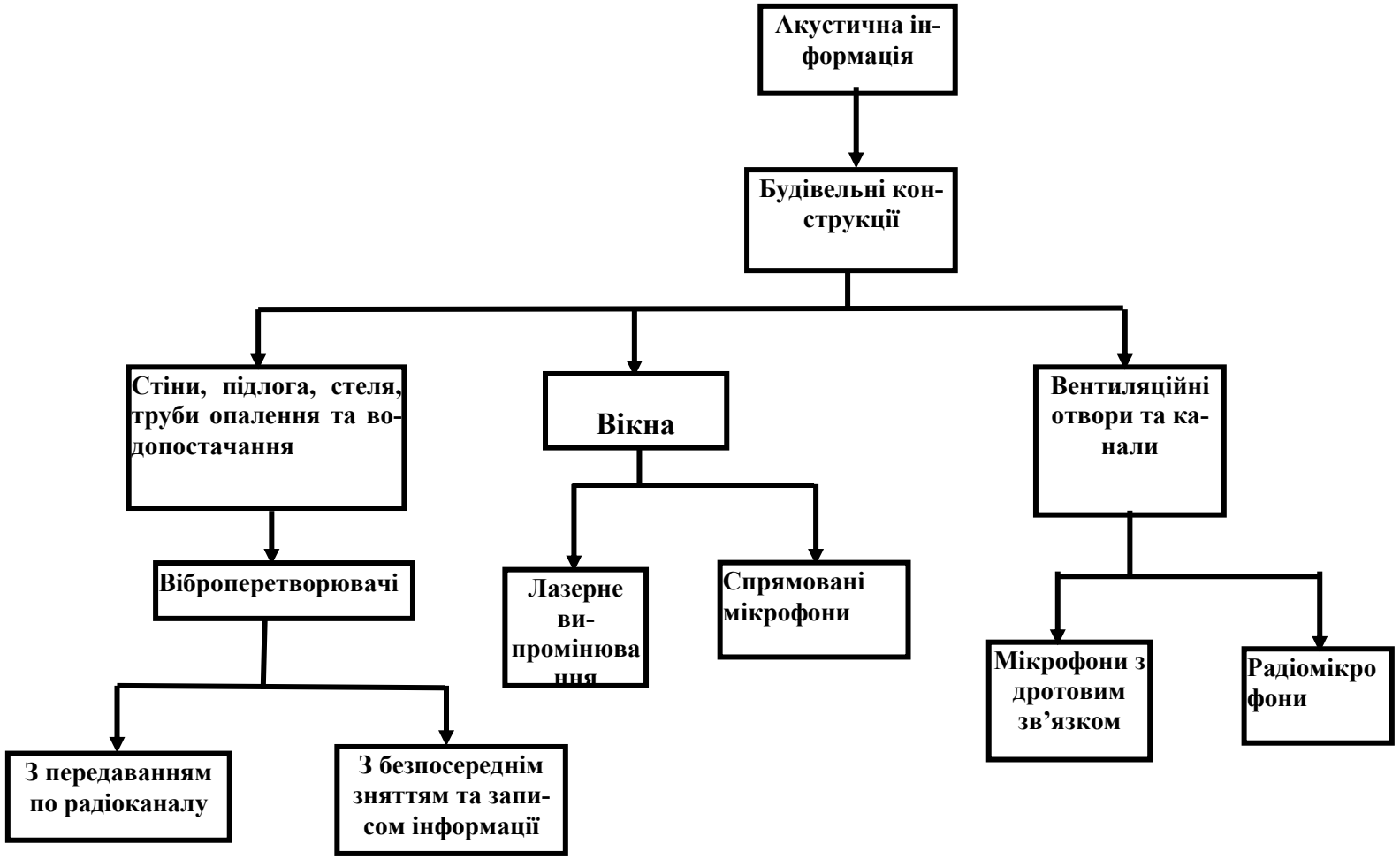

Рис. 2.10. Методи та засоби зняття акустичної інформації з будівельних конструкцій

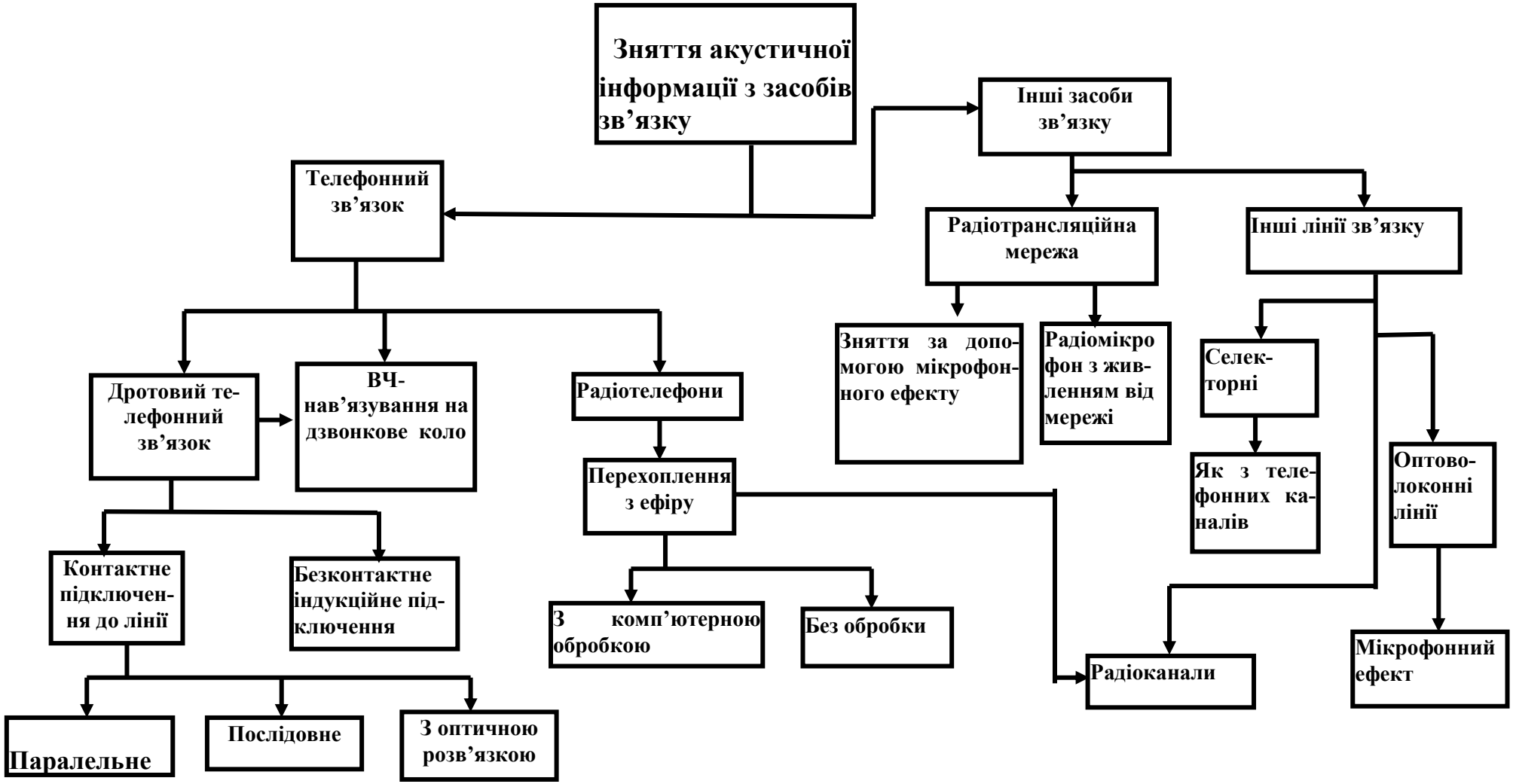

Рис. 2.11. Методи та засоби зняття акустичної інформації з засобів та ліній зв'язку

В закритих приміщеннях (див. рис. 2.10) акустичну інформацію можна знімати за рахунок того, що будівельні конструкції (стіни, підлоги, стелі, вікна, труби, зачинені двері) є по суті акустичними мембранами та чудово передають звукові коливання.

Таким чином, за допомогою віброперетворювача та підсилювача можна знімати акустичний сигнал з будь-якого приміщення через стіну, підлогу або стелю.

На відстані акустичний сигнал можна зняти з зачинених вікон, спрямувавши випромінювання лазеру на скло чи скористувавшись спрямованим мікрофоном.

Акустичну інформацію можна знімати також з побутових приладів та апаратури зв'язку (див. рис.2.11).

Особливо небезпечним приладом є телефон. Наявність незахищеного телефонного апарату в режимному приміщенні дає змогу без зайвого клопоту прослухувати в ньому всю акустичну інформацію навіть не використовуючи радіомікрофони чи іншу дорогу спецтехніку. При чому це можна робити навіть тоді, коли трубка лежить на апараті, тобто телефон, здається, виключено. Але дзвінкове коло телефону має елементи, що створюють резонансний контур, який постійно підключений до телефонної мережі під напругу від 40 до 60 В. Частина з них ще й мають властивості мембрани, яка коливається під дією акустичного сигналу, тобто механічних коливань повітря. При коливаннях такої мембрани відбувається зміна резонансних характеристик контуру (мікрофонний ефект). При розмові у разі наявності такого "шпигуна" на резонансному контурі відбувається модуляційний процес звуковими коливаннями мови, тобто акустичний сигнал перетворюється в електричний. Цей сигнал надходить до дротів телефонної мережі, звідки його можна зняти за допомогою простого пристрою. Не говорячи вже про застосування ВЧ-нав'язування або зняття сигналів за допомогою індукційного датчика, чи датчика з високим вхідним опором, які можна підключити до лінії зв'язку за межами приміщення чи, навіть, об'єкту, які взагалі надзвичайно важко ви-

явити (практично неможливо без застосування спеціальних приладів, що вимірюють неоднорідність мережі).

Мають свої резонансні контури та мембранні елементи інші побутові прилади: кондиціонери, оргтехніка (наприклад, електрична друкарська машинка). В цьому випадку акустичну інформацію можна зняти з електричної мережі, до якої вони підключені.

Нарешті, завжди існує загроза встановлення радіомікрофону (інколи його звуть радіозакладним пристроєм чи радіозакладкою, або “жучком”).

На рис. 2.12 наведено сучасні варіанти виконання цих дуже шкідливих “комах” – від найпростішого та найдешевшого, які, всупереч законодавству, сьогодні можна придбати, до найскладнішого (з шумоподібною несучою частотою), який є майже “невидимкою” для сучасних приладів контролю за ефіром. На щастя, такі закладки дуже дорого коштують та виготовляються на спеціалізованих виробництвах лише для правоохоронних органів. Але не виключено, що подібними приладами можуть бути оснащені злочинні угруповання та служби безпеки окремих фінансово-промислових груп.

З розгляду способів та засобів зняття акустичної інформації видно, як багато загроз для викрадення цього виду інформації надає сучасна техніка. Але, нажаль, крім акустичної інформації, сучасна техніка перехоплення надає можливості знімати електронну чи електромагнітну інформацію, тобто фактично викрадати будь-які документи, що створюються, передаються та зберігаються у незахищених засобах електронної обробки інформації.

Наведені на рис. 2.8 канали витоку інформації дають наочне уявлення про такі можливості. Додамо, що для їх реалізації застосовуються всі найсучасніші математичні теорії, технічні засоби та способи. В першу чергу використовуються методи та засоби спектральної обробки сигналів, які, хоч і базуються на винайденій ще у XVIII сторіччі математичній теорії рядів Фур’є, знайшли свій науковий розвиток і технічне застосування та реалізацію лише у XX сторіччі. Нині ці методи отримали широке визнання та розвиток. Цей розвиток складається як з розробки нових засобів (що пов’язано, головним

чином, з розвитком технологій створення та виробництва нових виробів мікроелектроніки), так і розвитком прикладної математики, яка надає нові алгоритми обробки інформації та нові, більш точні та продуктивні методи перетворення сигналів (наприклад, вейвлет-перетворення).

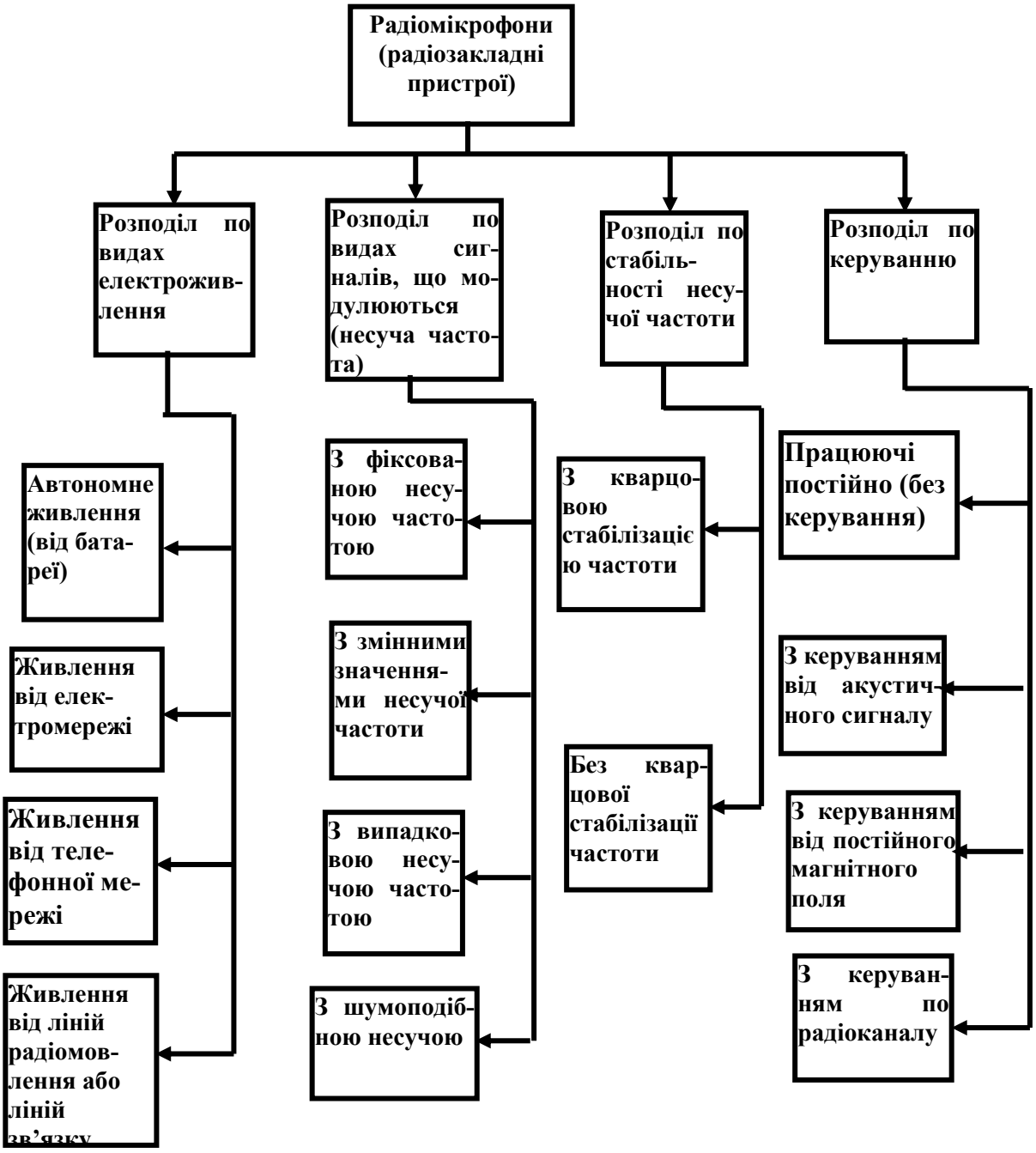

Рис. 2.12. Види радіомікрофонів (радіозакладних пристроїв) для зняття акустичної інформації

Слід відзначити, що всі ті методи мають універсальний характер, тобто вони можуть застосовуватися у медицині, військовій справі, керуванні технологічними процесами та у багатьох інших галузях життя та народного господарства. Ці методи, до речі, використовуються не лише для перехоплення, але й для захисту інформації.

Розглянемо спочатку методи зняття інформації, яку представлено в електронному вигляді. Канали витоку такої інформації можуть бути спільними з каналами витоку акустичної інформації (див. рис. 2.8). Знімання інформації, що представлена в електронному вигляді, проводиться за рахунок того, що всі електронні прилади (в тому числі – обчислювальна техніка та оргтехніка) мають паразитне електромагнітне випромінювання на високих частотах. Уникнути цього явища принципово неможливо, бо воно пов'язане з конструктивно-технологічними особливостями всіх радіокомпонентів, з яких виготовляється будь-яка електронна техніка. *Паразитне випромінювання* за рахунок ***нелінійності амплітудних характеристик***, яка також завжди присутня в електронному обладнанні, модулюється сигналами інформації, що обробляється, та у вигляді модульованих інформацією коливань випромінюється у ефір. Крім того, такі коливання, зважаючи на їх високочастотний характер, потрапляють через ланцюги вторинного електроживлення до електромережі. Вони також у вигляді електромагнітних наводок потрапляють на всі струмопровідні частини приміщення, де розміщено електронну апаратуру.

Зрозуміло, що рівень цих паразитних коливань малий. Взагалі він не перевищує рівня власних шумів апаратури, який завжди роблять як можна меншим, щоб розширити *динамічний діапазон* апаратури. Але навіть цього вкрай малого рівня ***паразитних сигналів*** вистачає для перехоплення інформації за допомогою сучасної чутливої апаратури для її несанкціонованого зняття.

Таку апаратуру може бути розміщено, наприклад, в легковому автомобілі, який поставлено на стоянку поряд з об’єктом. Перехоплення інформації з незахищених комп’ютерів нестаціонарними засобами може провадитись з відстані до 200 – 300 м. При перехопленні за допомогою стаціонарних потужних засобів, які розміщаються, як правило, у дипломатичних представництвах або інших стаціонарних об’єктах розвідки та контррозвідки, перехопленням може бути охоплено великий регіон.

Для глобального зняття інформації з розвідувальними цілями використовуються супутники Землі та стаціонарні пункти розвідки.

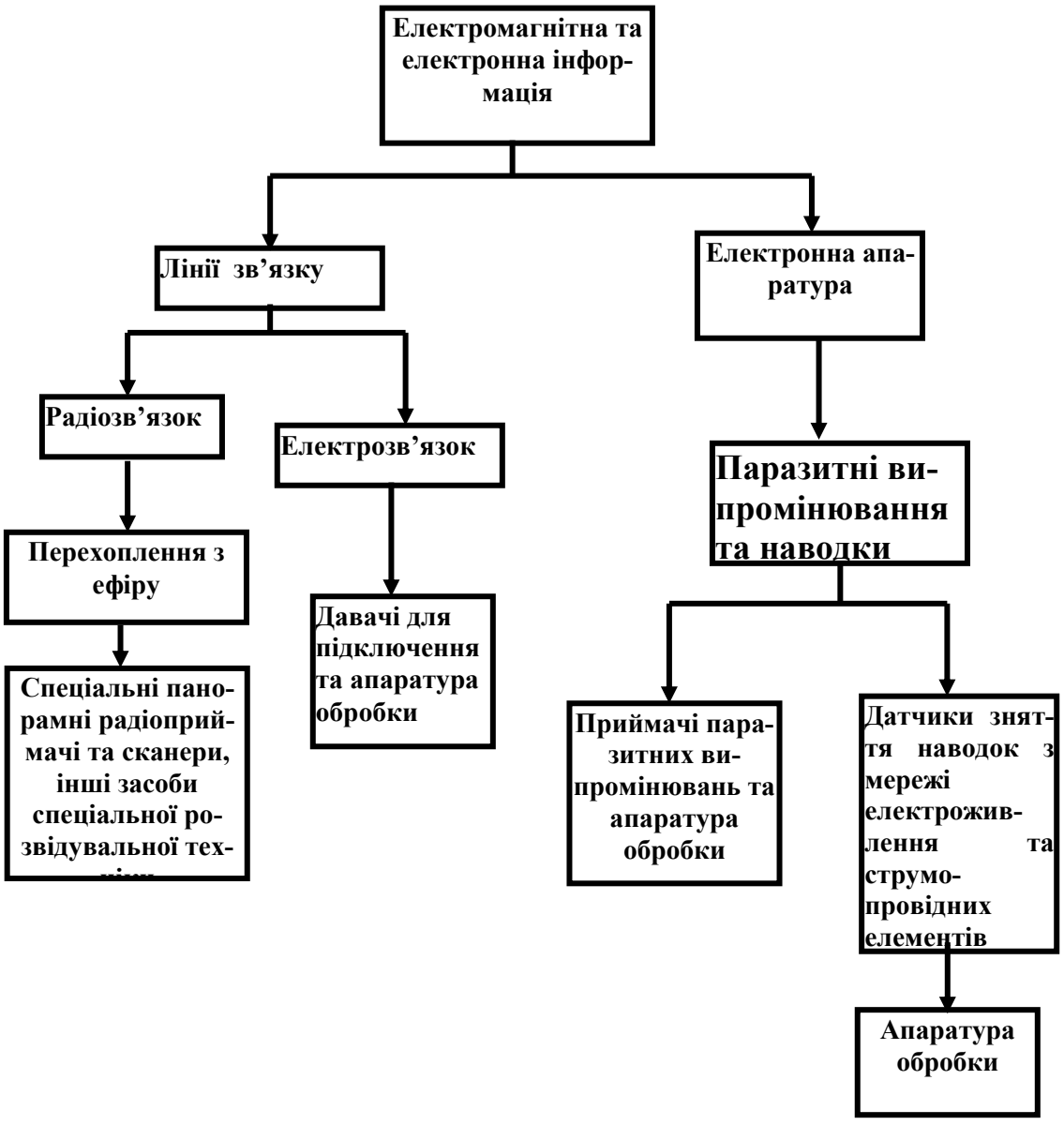

Рис. 2.13. Канали та засоби зняття електромагнітної та електронної інформації

На рис. 2.13 показано канали та засоби зняття електромагнітної інформації.

З рис. 2.13 видно, що інформацію в електронному та електромагнітному вигляді можна знімати з ліній зв'язку та з електронної апаратури обробки інформації.

Для перехоплення інформації з ефіру використовуються так звані панорамні радіоприймачі (в разі роботи на стаціонарному розвідувальному об'єкті) та малогабаритні ***сканери*** (для роботи на пересувному об'єкті). Ці прилади мають багато різних функцій та здатні приймати сигнали з різними видами модуляції, слідкувати за частотою станції, працювати під керуванням комп'ютера та т. інше.

Для зняття інформації з ліній зв'язку шляхом підключення використовуються *датчики з високим вхідним опором* для паралельного вмикання або *індукційні датчики* для безконтактного перехоплення сигналів. Визначити їх наявність на лінії зв'язку без складних спеціалізованих пристроїв практично неможливо.

Для зняття інформації, яка наводиться на струмопровідні конструкції приміщення використовуються спеціальні приймачі наводки, що побудовані за принципом частотно-селективного підсилювача з великим коефіцієнтом підсилення та, відповідно, значним динамічним діапазоном. При обробці отриманої таким чином інформації для підвищення співвідношення сигнал/завада використовують апаратуру спектральної обробки сигналів.

Так само провадиться зняття інформації, що надходить до електромережі у вигляді модульованого сигналу паразитного випромінювання чи у вигляді наводки.

Письмова інформація може бути отримана у двох видах: як оптична і як електронна.

Електронна інформація може бути отримана шляхом зняття з ліній зв'язку (факсимільний зв'язок чи електронна пошта), або перехопленням ка-

налами паразитних випромінювань та наводок (наприклад, дисплей комп'ютера, який, до речі, має найбільший рівень паразитного випромінювання).

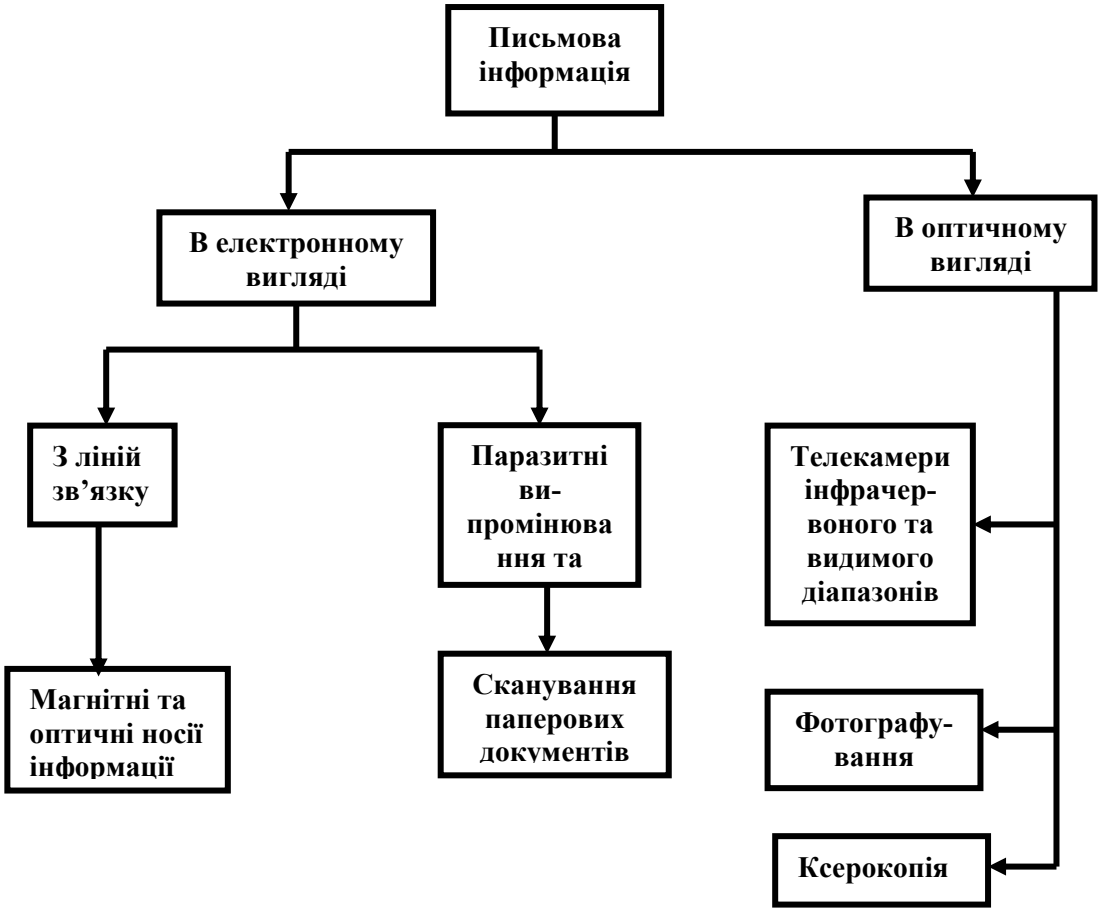

Рис. 2.14. Шляхи отримання письмової інформації

В електронному вигляді письмову інформацію можна також отримати шляхом копіювання магнітних чи оптичних носіїв, або копіювання шляхом зняття з паперового документа електронної копії на сканері. Оптична інформація може бути отримана шляхом використання прихованих телекамер, які можуть працювати або у інфрачервоному, або у діапазоні видимих хвиль. Крім того, можуть бути використані фотоапарати, копіювання шляхом зняття ксерокопій і звичайної крадіжки.

Шляхи отримання письмової інформації наведено на рис. 2.14.

Для зняття оптичної інформації використовуються оптичні та електронно-оптичні пристрої. Серед оптичних пристроїв слід відзначити біноклі, фотоапарати, підзорні труби, кінокамери, тобто засоби прямого оптичного спостереження та фіксації оптичної інформації без застосування електронних приладів. Серед оптично-електронних приладів слід відзначити відео- та телекамери, цифрові фотоапарати, прилади нічного бачення, інфрачервоні приціли, лазерні прилади спостереження та лазерні приціли.

Висновки до розділу 2

Розглянуті фізичні основи та різні аспекти технічного захисту інформації повинні вам пояснити важливість піднятих проблем для забезпечення надійності функціонування правоохоронних органів. У подальших главах будуть розглянуті класифікація способів та засобів несанкціонованого зняття інформації та методи і засоби захисту від таких протиправних посягань на інформацію. Отримані знання повинні допомогти Вам у виконанні своїх службових обов’язків.

Розглянуто основи зняття інформації способом та засобами високочастотного нав’язування.

Наведена класифікація каналів витоку інформації, способів та засобів зняття різних її видів та прикладів здійснення несанкціонованого зняття інформації дає можливість стверджувати, що сучасний стан розвитку науки і техніки дозволяє отримати практично будь-яку незахищену інформацію незаконним шляхом. Отже, інформація з обмеженим доступом потребує захисту.

Існує ще два аспекти інформаційної безпеки:

1. Захист інформації від знищення та спотворення; це питання відноситься до захисту інформації в автоматизованих інформаційних системах.

2. Захист інформації при її передаванню по відкритих каналах.

Ці аспекти інформаційної безпеки будуть розглянуті в наступних главах.

Перелік питань для самоконтролю до розділу 2

1. Які складові інформаційної безпеки держави відносяться до технічного аспекту інформаційної безпеки?
2. Яке призначення технічного захисту інформації?
3. Яке призначення криптографічного захисту інформації?
4. Надайте визначення поняття технічного каналу витоку інформації
5. Надайте визначення поняття небезпечного фізичного сигналу
6. Яка класифікація ТКВІ прийнята в Україні?
7. Що таке природні ТКВІ? Наведіть приклади таких каналів.
8. Що таке штучні ТКВІ? Наведіть приклади таких каналів. Яким шляхом утворюються штучні ТКВІ?
9. Намалюйте схему загальної класифікації видів інформації, яка може бути об’єктом злочинних посягань.
10. В чому полягає сутність та основні завдання ТЗІ?
11. Намалюйте класичну схему обробки, розповсюдження та захисту інформації.
12. Що є основними об’єктами захисту інформації?
13. Які технічні засоби і системи звуться додатковими технічними засобами і системами?
14. Яка фізична сутність акустичного сигналу?
15. Яка фізична сутність акустично-електричних перетворень?
16. Що є частотою та періодом коливань?
17. Які частоти коливань відносяться до звукового діапазону частот?
18. Які частоти коливань відносяться до інфразвукового діапазону частот?
19. Які частоти коливань відносяться до ультразвукового діапазону частот?
20. Яка фізична сутність мікрофону та гучномовця?

21. Як утворюється мікрофонний ефект та яка його фізична сутність?

22. Яка головна особливість радіозв’язку?

23. В чому полягає фізична сутність процесу модуляції?

24. Який сигнал має більшу частоту: сигнал-переносник, чи модулюючий сигнал?

25. Чому сигнал, що модулюється, звуть несучим коливанням?

26. Які види модуляції використовуються для передавання інформації по радіозв’язку?

27. В чому полягає процес демодуляції (детектування)?

28. Поясніть формулу 2.1.

29. Як і де утворюються паразитні випромінювання?

30. Який механізм утворення наводок? Де вони виникають?

31. В чому полягає небезпека паразитних випромінювань та наводок?

32. Дайте визначення організаційних заходів із захисту об’єкту.

33. Які основні організаційні та режимні заходи відносяться до основних?

34. Дайте визначення технічних заходів із захисту об’єкту.

35. Які основні складові технічних заходів?

36. Який порядок проведення робіт з ТЗІ?

37. В чому полягає особливість використання беззаходових способів зняття інформації?

38. В чому полягає фізична сутність способу високочастотного нав’язування для зняття інформації?

39. Чим визначається власна резонансна частота коливального контуру? Запишіть формулу визначення резонансної частоти.

40. За яким принципом побудовано детальний розподіл ТКВІ?

41. Що є комбінованими каналами витоку інформації?

42. Які є канали витоку акустичної інформації?

43. Які способи та засоби використовуються для зняття акустичної інформації?

44. Які є види радіозакладних пристроїв?

45. Які є канали витоку електромагнітної та електронної інформації?

46. Якими способами та засобами знімається електромагнітна та електронна інформація?

47. Які є канали зняття письмової інформації?

48. Якими способами та засобами знімається письмова інформація?

Перелік рекомендованої літератури до розділу 2

1. Наказ МВС України № 059 від 14.06.98 р. “Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”

2. Яворский Б.М. Справочник по физике для инженеров и студентов вузов / Яворский Б.М., Детлаф А.А. /. – М.: Наука. Гл. ред. физ.-мат.литер. – 1974. – 944 с.

3. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / Рибальський О.В., Хахановський В.Г., Шорошев В.В., Грищенко О.І., Сторожев С.В., Кобець М.В. /. – К.: НАВСУ, 2003. – 160 с.

4. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

5. Хорошко В.О. Основи інформаційної безпеки /Хорошко В.О., Чередниченко В.С., Шелест М.Є./ За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

6. Головань С.М. Нормативне забезпечення інформаційної безпеки / Головань С.М., Петров О.С., Хорошко В.О., Чирков Д.В., Щербак Л.М./ За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

7. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. /. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.

РОЗДІЛ 3. МЕТОДИ ТА ЗАСОБИ БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

3.1. Основні загальні положення технічного захисту інформації

Зараз, коли ми вже знаємо всі основні технічні канали витоку та класифікацію способів зняття інформації, можна починати вивчення методів та засобів технічної протидії протиправним намаганням її отримання.

Спочатку розглянемо основні загальні положення та визначення термінів захисту інформації [13]. Серед них особливе значення займає поняття об'єкту захисту.

Об'єкт технічного захисту інформації *– це будова, приміщення, окремий* ***основний технічний засіб*** *або їх група, об'єднана загальним призначенням, які підлягають захисту від* ***технічних розвідок.***

Розглянемо окремо всі складові поняття об'єкту захисту. Як видно з визначення, об'єкт може бути однією зі складових, але він може поєднувати у собі і всі зазначені складові.

Все залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, у яких приміщеннях об'єкту циркулює ця інформація. Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень.

Якщо треба захищати велику кількість приміщень (велику група, яка, наприклад, складається з підгруп), об'єкт захисту може складатися зі всієї будівлі.

Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об'єкту, то використовується ***комплексний*** захист інформації.

При цьому і сам об'єкт захисту може розміщуватися всередині іншого об'єкту, який не є в цілому об'єктом захисту інформації. Наприклад, виділені

приміщення з обмеженим доступом, розміщені на території будівлі з більш широким доступом, передбачені для роботи з певними видами інформації.

Основні технічні засоби – це технічні засоби, призначені для обробки, зберігання та передавання закритої інформації.

Існують і *допоміжні технічні засоби та системи*, призначені для обробки відкритої інформації. Але вони можуть утворювати технічні канали витоку закритої інформації.

Отже, приступаючи до захисту інформації на певному об'єкті, необхідно, в першу чергу, визначити, які види інформації підлягають захисту, а, по-друге, які приміщення у будівлі (або всю будівлю) необхідно захищати.

Також необхідно знати *ступень таємності* інформації, що підлягає захисту.

Крім того обов'язково необхідно знати *загрози для інформації*, які можуть виходити від потенційного супротивника.

Загроза для інформації – це виток, можливість блокування або порушення цілісності інформації, яка може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації.

Знаючі всі ці складові, можна розробляти систему захисту інформації на об'єкті.

При цьому слід пам'ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування, отже треба користуватися тими системами та засобами захисту, що найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об'єкті.

В разі комплексного захисту необхідно розробляти ***підсистеми*** захисту для кожного окремого виду інформації, обов'язково пов'язавши їх у комплексну систему.

При цьому необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з ***рівнем технічного захисту***, відповідним ступеню таємності інформації та рівню потенційних загроз.

Рівень технічного захисту інформації – це сукупність вимог, в тому числі і тих, що нормуються, які визначаються режимом доступу до інформації та загрозами для її безпеки.

Взагалі у технічному захисті інформації розрізняють два основні методи: ***пасивний*** та ***активний методи*** захисту інформації [9].

Активний захист побудовано на постановці перешкоди зняттю інформації шляхом випромінювання завад у канал витоку, рівень яких перевищує рівень небезпечних сигналів, які можна зняти з каналів витоку. До активного захисту також відносяться методи протидії, що засновані на постійному контролі середовища розповсюдження небезпечних сигналів необхідними для цього приладами та комплексами, які дозволяють виявляти спроби зняття інформації та активного пошуку і знешкодження засобів зняття інформації.

Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, наприклад, шляхом екранування електромагнітного випромінювання.

Для ТЗІ використовуються обидва напрямки захисту. Але слід відзначити, що пасивні методи захисту не використовують фізичних процесів, які шкідливі для здоров’я оточуючих та заважають повсякденній діяльності людей. Однак у більшості випадків застосування активних методів захисту є необхідним, які разом з пасивними методами захисту забезпечують потрібний ступень рівня технічного захисту інформації.

Таким чином, ми розглянули основні загальні положення технічного захисту інформації та можемо перейти до розгляду методів та засобів блокування технічних каналів витоку окремих видів інформації. Почнемо з каналів витоку акустичної інформації.

3.2. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації

Першочерговим завданням при розробці проекту та обладнанні об'єкту для його захисту від витоку інформації є встановлення технічних каналів витоку інформації для кожного конкретного приміщення.

Зокрема, серед акустичних каналів витоку можуть бути як такі, що зумовлені конструктивними особливостями приміщення, так і ті, що створені навмисно (наприклад, замасковані отвори у стінах, ***звуководні канали***). Особливо це стосується старих споруд, та блочних бетонних споруд – в останніх звуководні канали утворюються на стиках блоків.

Для проведення робіт із захисту акустичної інформації використовуються прилади для загальних акустичних вимірювань та спеціалізована апаратура, яка побудована на тих самих принципах, що й апаратура для зняття інформації. Крім того, органолептично перевіряються всі приміщення, які можуть бути пов'язані з об'єктом захисту створеними навмисно звуководними каналами. При цьому, за правило, користуються повними будівельними планами всієї будівлі, де розміщено об'єкт захисту. Одночасно перевіряють відсутність (чи наявність) засобів зняття інформації на виявлених каналах витоку. При проведенні цих робіт особливу увагу слід звертати на можливість несанкціонованого зняття акустичної інформації з металевих трубопроводів опалення, вентиляції та водопостачання. Після проведення обстеження на базі отриманих результатів вимірювань та розрахунків складається ***паспорт об'єкту*** та проектується система його захисту (обираються типи та кількість необхідної апаратури, місця розміщення випромінювачів та інше).

Захиститися від витоку акустичної інформації через зачинені вікна та через стіни, стелю й підлогу можна при застосуванні спеціальних ***генераторів випадкових*** або ***псевдовипадкових*** електричних коливань, яких навантажено на ***перетворювачі електричного сигналу в механічні коливання***. Такі генератори створюють маскуючий механічний сигнал, який заважає прийма-

ти мовні сигнали на перетворювачі, що використовуються при знятті акустичної інформації. Перетворювачі генераторів розміщують на склі та на стінах, підлозі й стелях. Зрозуміло, що спочатку з'ясовують можливість такого зняття інформації з суміжних приміщень (тобто можливість проникнення в суміжні приміщення сторонніх осіб). Захищати вікна в приміщеннях, де циркулює інформація з обмеженим доступом, необхідно в тих випадках, коли вони виходять на незахищений простір, якщо охоронна зона (відстань від вікна до периметру охорони) не перевищує 200 м. Такий захист ефективно діє також проти зняття акустичної інформації з вікон за допомогою лазерного випромінювання та спрямованого мікрофону.

Нині широко відомі та часто використовуються як зарубіжні, так і вітчизняні генератори випадкових вібрацій. Серед них можна відзначити генератори таких типів: генератор ANG-2000 з перетворювачами TRN-2000 та випромінювачами OMS-2000 (виробництво США, мінімальна вартість 1450 у.о.), "Барон" (виробництва РФ).

Серед найсучасніших генераторів слід відзначити генератори фірми PIAC, м. Київ.

Вони мають дві модифікації – стаціонарний генератор "PIAC-2ГС" та його мобільний варіант "PIAC-2M".

Генератори призначені для захисту об'єктів від витоку інформації по акустичним та віброакустичним (будівельні конструкції) каналам шляхом генерації шумового сигналу. Вони мають високі тактико-технічні характеристики забезпечують придушення (маскування) акустичних сигналів у смузі частот від 180 Гц до 5,6 кГц. Вихідна середньоквадратична напруга акустичного каналу приладу при навантаженні 4 Ом – не менше 8 В. Вихідна середньоквадратична напруга п'єзоелектричного каналу приладу при ємності навантаження 0,5 мкФ – не менше 20В. Генератор забезпечує глибину регулювання рівня шумового сигналу у робочому діапазоні частот не менше 20 дБ.

Важливою особливістю приладу є те, що він здатен працювати як для захисту будівельних конструкцій, так і випромінювати у повітря шумові акустичні сигнали.

У комплект входять випромінювачі обох типів. При цьому вартість приладу та випромінювачів значно нижча, ніж у імпортних, а технічні характеристики не гірше (а деякі кращі) ніж у іноземних генераторів.

Ці прилади та випромінювачі для них показано на рис. 3.1 – 3.5.

Рис. 3.1. Генератор PIAC-2ГС

Рис. 3.2. Генератор PIAC-2М. Генератор розміщено у кейсі разом з комплектом випромінювачів та з'єднуючих шнурів для підключення. На фото генератор разом з комплектом розміщено на кришці кейса

Рис. 3.3. Перетворювач електромагнітного типу електричного сигналу звукового діапазону у механічні коливання “РІАС -2ЕМ”

Рис. 3.4. П’єзоелектричний перетворювач електричного сигналу звукового діапазону у механічні коливання “РІАС -2ВП”

За цінами фірми-виробника РІАС (станом на червень 2010 р.) вартість генератора РІАС-2ГС складає 5700 грн., генератора РІАС-2М – 10900 грн., випромінювачів РІАС -2ЕМ – 690 грн., випромінювачів РІАС -2ВП – 670 грн., випромінювачів РІАС -2ВА – 498 грн.

Рис. 3.5. Перетворювач електричного сигналу звукового діапазону в акустичні коливання “PIAC -2BA”

Генератори вібрацій можна віднести до активних методів захисту, бо ці вібрації є активною завадою для акустичних сигналів та діє на середовища, з поверхні яких їх намагаються знімати.

Також до активних методів захисту як від прослуховування через будівельні конструкції мембранного типу, так і від прослуховування за допомогою різних типів мікрофонів, можна віднести генератори ***акустичного шуму***, який випромінюється у повітря приміщення, що захищається. Саме такі коливання випромінюють розглянуті нами генератори PIAC-2ГС та PIAC-2M. Зрозуміло, що при роботі таких генераторів вести розмову дуже неприємно, бо шум, що випромінюється, заважає розмовляти.

Тому з’явилися ***комбіновані*** генератори, які побудовані на принципі: завада не повинна заважати тому, хто її використовує.

Існує три загальні тенденції розробки таких генераторів. Перша тенденція – використання зворотного зв’язку для регулювання спектру шумового сигналу та його рівня залежно від рівня акустичного сигналу, який треба маскувати. Друга тенденція – створення закритого ланцюга зв’язку для розмов між учасниками переговорів. Вона реалізується або за рахунок шифрування

розмов, що передаються в ізольованому від навколишнього акустичного середовища колі, або шляхом використання поза цього кола спеціальної завади, що не дозволяє зняття розбірливої акустичної інформації за межами цього кола.

Третя тенденція – використання ***змішаної*** завади, яка складається з тихої музики, шуму та голосових сигналів декількох учасників розмови, які зсунуті у часі та інвертовані по спектру. Така суміш сигналів не дозволяє зняти розбірливі сигнали розмови. Навіть якщо записати розмову, що замасковано таким чином, та очистити її відомими нині методами, неможливо отримати розбірливих сигналів. При цьому методі маскування рівень завади, що випромінюється у повітря приміщення, значно нижчий від рівня шуму, який випромінюється при застосуванні звичайного генератору. Такий шум не заважає розмові та не є шкідливим для здоров'я оточуючих.

Такого типу генератори виготовляються Центром захисту інформації "Бар'єр" м. Київ.

Крім того виробляють подібні генератори "Базальт" у НДІ "Квант" м. Київ.

Захист від будь-яких (радіо- чи звичайних, з дротовим зв'язком) мікрофонів, що встановлені в приміщенні, може бути виконаний також ***методом "завантаження"*** його ***мембрани***. При застосуванні цього методу у повітря випромінюється акустична завада у вигляді модульованих ультразвукових сигналів високого рівня, які діють на мембрану мікрофону з таким тиском, що інші акустичні коливання меншого рівня мікрофонами не сприймаються.

До недоліків такого методу захисту слід віднести шкідливий вплив на людину та зовнішнє середовище ультразвукових коливань високого рівня та дуже швидке затухання таких коливань у повітрі.

Використовується також ще один метод захисту акустичної інформації, пов'язаний з встановленням електромагнітної завади від генераторів ***радіочастотного випромінювання***.

Він також дозволяє нав’язати шумову або, навіть, будь-яку іншу акустичну інформацію на нелінійні елементи апаратури звукозапису та з’єднуючі дроти мікрофонів. Метод засновано на випромінюванні у навколишнє середовище широкосмугової модульованої радіохвилі з енергією, що достатня для наведення на елементи апаратури зняття інформації сигналів завади, що повністю блокують її функціонування. Апаратура, що використовується при реалізації всіх цих методів, буде наведена нижче.

Серед генераторів вібраційних та шумових коливань сьогодні знайшли широке застосування генератори “Барон”, які призначено для захисту інформації, яка обговорюється в службових приміщеннях, методом вібраційного та акустичного зашумлення. Генератор створює на поверхнях конструкцій, які огороджують приміщення, та у відкритому просторі завади з рівнями, що виключають можливість виділення конфіденційної інформації з суміші сигналу з завадою.

Генератор має 4 канали формування завад, до кожного з яких можуть підключатися до 30 – 40 вібраторів п’єзоелектричного типу, до 10 вібраторів електромагнітного типу або акустичних систем, що забезпечують перетворення електричного сигналу в механічні коливання в конструкціях, що огороджують приміщення, а також в акустичні коливання повітря.

Разом із створенням традиційної шумової завади для підвищення ступеню маскування мовної інформації генератор може формувати нестаціонарну заваду у вигляді суміші трьох сигналів від станцій радіомовлення, для чого є три вбудовані радіоприймачі. В ході роботи здійснюється автоматичне перестроювання робочої частоти кожного з приймачів. Перестроювання робочої частоти здійснюється за випадковим законом як у часі, так і по радіостанціях за рядом встановлених заздалегідь частот.

Для корекції ***амплітудно-частотної характеристики*** (АЧХ) приміщення кожний з каналів має вбудований еквалайзер (корегувач частотної характеристики під акустичні особливості приміщення) на п’ять смуг.

Кількість каналів завади – 4; вихідна потужність кожного каналу – не менш ніж 20 Вт; діапазон частот від 175 до 5600 Гц; кількість вібраторів, що підключаються до одного каналу: п'єзоелектричних – до 40, електромагнітних – до 10.

Для захисту телефонного каналу використовуються декілька пристроїв, що виробляються в Україні та країнах СНД, які виконують різні функції.

Для захисту від витоку інформації з приміщення, де розташовано телефонний апарат, використовуються прилади типу "Рікас", "РІАС", та "Базальт", які забезпечують блокування зняття інформації при покладеній трубці за рахунок *мікрофонного ефекту* дзвінкового ланцюга. Залежно від типу АТС, до якої підключено телефон, використовуються різні моделі приладу: для аналогової або квазіелектронної АТС використовуються прилади "Рікас-2", РІАС-4РА, а для цифрової АТС – "Рікас-9".

Прилад "Рікас-2" є вітчизняним варіантом приладу "Граніт IV", розробленому ще за часів СРСР. Він утримує чотири напівпровідникових діоди та ***фільтр нижніх частот*** (ФНЧ). Вмикається у розрив ланцюга між телефонним апаратом та телефонною розеткою на кожний дріт мережі. В основу роботи приладу покладено нелінійність характеристики напівпровідникових діодів, що надає змогу не перепускати через прилад електричні сигнали малої амплітуди до 0,4 В, які виникають у дзвінковому ланцюзі за рахунок мікрофонного ефекту. ФНЧ дозволяє захистити телефон від зняття інформації методом ВЧ-нав'язування на дзвінковий ланцюг. Прилад "Рікас-9" побудовано за приблизно тими самими принципами, але з урахуванням особливостей цифрових АТС.

Ці прилади дозволяють ефективно захистити акустичну інформацію в приміщенні від витоку телефонними каналами при покладеній трубці.

Виробляються прилади підприємством МВС України "Рікас" (м. Київ), РІАС та НДІ "Квант".

Значно складніше захистити від зняття інформацію під час розмови по телефону. Існує декілька видів приладів, які спроможні визначати підклю-

чення до телефонної мережі приладів, що живляться від цієї мережі. Це найпростіші прилади виявлення підслуховуючи пристроїв та несанкціонованого підключення до телефонної мережі, таких приладів багато. Хоча вони і відрізняються один від одного, але використовують однакові принципи, тобто реагують на падіння напруги у мережі (дуже незначні), що виникають при підключенні додаткових споживачів електричного струму. До таких приладів можна віднести “Рікас-16”, "Телефонний страж ЛСТ-1007" ("Лабораторія ППШ", РФ, м. С.-Петербург) та інші. Більш складні прилади такого типу можуть “придушувати” виявлені підслуховуючи пристрої, блокувати несанкціоновані паралельні телефони та інше. Прикладами таких приладів можуть бути "УЗТ-01" (московська фірма "НЕЛК"), "Фантмастер ФСМ-6" (фірма "Фантазія), ряд виробів фірми "МініТех" і т.д. (всі виробники з РФ). Інколи такі пристрої потребують окремого підключення до мережі 220 В, мають додаткові регулятори та індикатори.

Однак треба враховувати, що всі вироби подібного класу можуть контролювати телефонну мережу лише від апарату до АТС. Підключення на АТС можливо лише у одному випадку – з відповідного дозволу суду технічними службами правоохоронних органів. Але у цьому випадку підключення не може бути виявлено жодним приладом. Саме тому необхідні реально працюючі прилади, які б надійно виявляли “інтелігентні” способи зняття інформації з телефонних ліній, наприклад, способом індукційного зняття або пристроями з надвисокими вхідними опорами та відповідно малими ємностями.

Такий прилад існує. Він побудований на принципі рефлектометра та визначає ***неоднорідності лінії***. Це єдиний відомий нині ***локатор-рефлектометр*** "Бор".

Він здатний витримувати напругу сигналу виклику АТС (до 150 В) та забезпечує перевірку та визначення місця неоднорідності у лінії на відстані до 400 м.

Вартість приладів цього класу набагато вища, ніж всіх інших, більш простих, проте ця вартість компенсується вирішенням завдання, що ставить-

ся. Можливість виявлення засобів зняття інформації за допомогою локатора-рефлектометра не менше 95%, тоді як всі інші нічого не гарантують щодо можливостей виявлення.

Максимальна дальність виявлення у локатора “Бор” – 400 м. Всю дистанцію розбито на три діапазони: 0 – 40 м, 40 – 200 м, 200 – 400 м. Точність виміру дальності по діапазонах відповідно 1м, 2м, 3м. Є два режими роботи: ручний, автоматичний. Конструктивно виконаний у стандартному портфелі типу “Кейс”, вага – 4,8 кг.

При роботі приладу не потрібно відключення лінії від АТС. Вихід приладу вмикається в телефонну розетку замість телефонного апарата. При надходженні виклику на даний номер під час роботи локатора відбувається його автоматичне відключення на момент проходження сигналу виклику. Результати виявлення видаються на цифровий індикатор у метрах, послідовно від кожного наступного об'єкта. Також видається номер об'єкта.

Деякі “фахівці” вважають, що для рефлектометра характерна “...низька достовірність отриманих результатів виміру (найчастіше за неоднорідність приймаються контактні з'єднання)...”. Але саме цей “недолік” і є гідністю. Дійсно, якщо виявлено і локалізоване максимально можлива кількість штучних неоднорідностей лінії, то це є її “паспорт”, тому що ці неоднорідності стабільні та постійні. Крім того, число таких з'єднань на реальному абонентському шлейфі обмежене і може складати не більш трьох: зовнішній розподільний щит, вхідний розподільний щит у будинку, розподільна коробка (при необхідності). У цій ситуації не складно виявити і ліквідувати засіб зняття інформації.

Це говорить про високу чутливість ***рефлектометрії***, що дозволяє виявляти ємнісне підключенні від 25 пФ, індуктивне – від 10 мкГн. Визначення іншими засобами подібної зміни параметрів лінії є достатньо проблематичним. Більш того, вказується дальність до місця зміни параметра, що і потрібно при пошуку.

Простота в обслуговуванні дозволяє дуже швидко провести ***паспортизацію лінії*** з одночасним виявленням і знищенням всіх, вже наявних засобів зняття інформації. Після паспортизації лінії прилад дозволяє швидко здійснювати контроль, виявлення і ліквідацію об'єктів, що з'явилися та не відповідають паспорту лінії.

Сьогодні (якщо б не було приладу “Бор”) не уразливим із погляду виявлення залишається один клас засобів несанкціонованого зняття інформації – засоби знімання інформації з безконтактним вмиканням у лінію – індуктивні датчики та датчики типу “телефонне вухо”. Це викликано тим, що ці пристрої не вносять змін у динамічні параметри лінії, а внесена ними неоднорідність настільки незначна, що рефлектометр може виявити її тільки при зондуванні надкоротким імпульсом, але при цьому різко обмежується дальність його дії. Так, при тривалості імпульсу, що зондує, 500 пс максимальна дальність виявлення з можливістю 90% складатиме не більш ніж 20 – 25 м. Для порівняння: мінімальна тривалість імпульсу серійних рефлектометрів: Р5-11 – пікосекундний діапазон, працює тільки по коаксіальних лініях із Z_B = 50 Ом; Р5-12 – 5 нс, працює тільки по коаксіальних кабелях із Z_B = 50 Ом; Р5-13 – 50 нс, працює в кабелях зв'язку до 10 км; Р5-14 – 50 нс, працює по коаксіальних парах до 10.5 км. В час як “Бор” при генеруванні імпульсу тривалістю 30 нс працює і по коаксіальних лініях, і по лініях зв'язку до 500 м. Серійне виробництво локатора “Бор” розпочате з 1996 р. За ций час конструкція приладу значно удосконалена.

Але ніякі прилади, що використовуються з одного боку лінії, не можуть виявити наявність засобів зняття інформації на протилежному полюсі зв’язку, тобто у абонента, з яким ведеться розмова (якщо він, звичайно, сам не потурбувався про захист своєї частини лінії). Тому для надійного захисту телефонних розмов слід використовувати “закриті” телефонні канали, де застосовується криптографічний захист інформації (***скремблери***).

Існує декілька принципів криптографічного захисту акустичної інформації. Відповідно до цього є й різні прилади захисту, які відрізняються різною вартістю та надійністю.

Найбільш надійними є прилади та методи, що використовують ***вокодери*** та ***лінідери*** з подальшим шифруванням. Принцип роботи таких пристроїв полягає у цифровій обробці аналогових сигналів, виявленні та розкладенні слів та звуків на окремі форманти та передачі мови у вигляді попередньо зашифрованому набору формант. При цьому ключове слово до шифру може сягати довжини до 512 знаків, а інколи і ще більше. Це системи надвисокої надійності, наприклад, урядовий зв'язок. На розшифрування такої перехопленої розмови за правило потрібно багато часу, інколи мільйони років.

Зараз прилади на цих принципах для широкого вжитку виготовляються різними фірмами як у нашій країні, так і за її межами. Прикладом таких пристроїв може бути прилад Voice Coder-2400, який придатний працювати як у відкритому, так і в закритому режимах. Передача у закритому режимі провадиться з гарантованою стійкістю.

Характеристики апарату Voice Coder-2400 в захищеному режимі роботи:

- алгоритм стискання мови на швидкості 2400 біт/с – на основі моделі с лінійним передбаченням (LPC-10) та табличним сигналом збудження;
- алгоритм стискання мови на швидкості 4800 біт/с – CELP;
- спеціалізовані алгоритми захисту інформації;
- дуплексний зв'язок з швидкостями передачі мови 2400 і 4800 біт/с в синхронному режимі;
- складова розбірливість синтезованої мови:

на швидкості 2400 біт/с - не нижче 86 %;

на швидкості 4800 біт/с - не нижче 94%;

- габарити апарату – 240х230х90 мм, вага – 1,2 кг.

Існують менш складні системи, які засновано на цифровій обробці спектру сигналів та передачі сигналів з іншим спектром. На приймальному кінці

у відповідності з завданими правилами приймання відбувається зворотне перетворення сигналів.

Прикладом таких пристроїв може бути скремблер "Орех-А" (Зеленоградська фірма “АНКАД”, РФ, Московська обл.). Це елегантна підставка під телефонний апарат, яка має лише одну кнопку керування.

Зрозуміло, що всі ***апарати криптографічного захисту*** інформації працюють у закритому режимі лише тоді, коли вони встановлені з обох кінців лінії зв’язку, тобто наявні у обох абонентів, що розмовляють між собою.

На останнє слід додати, що всі наведені вище методи та засоби захисту інформації як у провідних каналах, так і у каналах радіозв’язку застосовуються (або можуть бути застосовані) для захисту повідомлень у системах оперативного зв’язку ОВС.

3.3. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв

При вивченні методів та пристроїв для зняття інформації ми бачили велике різноманіття радіозакладок. Це пояснюється, з одного боку простотою та ефективністю використання таких пристроїв, а, з другого боку, постійним удосконаленням методів їх знешкодження.

Зрозуміло, що в попередньому розділі, присвяченого захисту від витоку інформації через будівельні конструкції, нами було розглянуто методи, що заважають знімати акустичну інформацію з використанням мікрофонів. Оскільки радіозакладки мають мікрофон, то всі методи захисту від зняття за його допомогою діють також і на радіозакладні пристрої.

Тому в цьому розділі звернемо увагу на методи виявлення та знешкодження таких пристроїв (інколи їх звуть “жучки”, “комахи”, “клопи”). Всі методи можна поділити на два підвиди, які доповнюють один одного.

Перший, найбільш ефективний – це постійний ***радіомоніторинг ефіру***. Метод полягає у постійній перевірці радіовипромінювань та виявленні нових

складових у рисунку спектру (тобто, нових частот випромінювання), шляхом порівняння з попереднім. При появі у контрольованій області спектру нових частотних складових проводять пошук передавача. Для цього використовують спеціальні прилади та методи пошуку, які складають сутність другого підвиду.

Але якщо перший підвид вимагає, в разі появи нових спектральних складових, застосувати інший, то останній може бути використаний автономно. Це метод періодичних оглядів, який застосовується на об’єктах, де відсутня апаратура для постійного контролю.

Виконувати цю роботу повинні фахівці, що добре розуміються у радіотехнічних вимірюваннях та володіють методикою виявлення та знешкодження радіозакладок.

Розглянемо деяку апаратуру для радіомоніторингу ефіру та методи її застосування. Головним приладом, що входить до такої системи, є скануючий приймач (сканер), наприклад, AR-2700, AR-3000A, AR-8000, AR-8200 або відповідні їм за технічними характеристиками, наприклад, приймачі серії "Тантал" (московська фірмою "Anna Design".) Найбільш досконалі серед них – сканери “AR-8200” та “AR-8600”. Такі приймачі мають вихід на персональний комп’ютер (другий елемент системи), з якого за допомогою спеціальної програми (третій елемент системи) провадиться керування режимами роботи сканера. Сканер може перенастроюватися із заданим шагом дискретності по частоті. Крім того, він може працювати з сигналами, які мають різний вид модуляції та в різній смузі частот прослуховування (широкій та вузькій), має зменшувач шуму, індикацію режиму. Взагалі, сканер може працювати автономно від ПЕОМ, що і використовується при пошуку радіозакладок.

Є й більш досконала апаратура, яка використовується у професійній радіорозвідці.

Програма моніторінгу побудована таким чином, що запам’ятовує спектр просканованої ділянки ефіру та використовує його як еталон при порівнянні з наступними вимірюваннями. Результати пошуку виводяться на

монітор. В разі виявлення нових частотних складових у контрольованій зоні ПЕОМ видає сигнал тривоги. Система може працювати і в автоматичному режимі.

Зараз багатьма фірмами розроблено декілька таких програм. Принцип їх побудови однаковий, хоча вони можуть бути різними за вартістю і точністю роботи.

Як приклад наведемо програми “Sedif” (фірма "НЕЛК", Москва), Arcon (фірми “Дивекон” і “Аист”, Москва), “RS-8000” (фірма "RS - Радиоэлектронная служба безопасности", Москва).

Зараз подібні програми розроблені й в Україні. Це програма “DigiScoun”, яку слід відмітити серед багатьох програм, розроблених для автоматичного сканування ефіру.

Робота комплексу з цією програмою побудована за принципом порівняння параметрів акустичних сигналів та працює таким чином:

1. На першому етапі вимірюється та запам’ятовується спектр радіосигналів по всьому діапазону роботи сканера. Одночасно встановлюється вид модуляції для кожного сигналу, випромінювання якого зафіксовано.

2. На другому етапі на кожній з виявлених частот комплекс випромінює у повітря декілька складних акустичних сигналів, які сприймаються ним через ланцюг зворотного зв’язку, а саме – через радіоканал (приймач сканеру) на тій частоті, що перевіряється. Якщо в приміщенні є радіозакладка, то параметри сигналу, який продетектовано з ефіру, співпадуть з параметрами сигналу, що випромінювався у повітря приміщення. Для забезпечення однозначності сигналів, що сприймаються радіозакладкою, в сигнал, що випромінюється комплексом, додається акустичний сигнал з приміщення (шум, розмови та т. інше) через другий *ланцюг зворотного зв’язку* (мікрофон, підсилювач та змішувач сигналів).

Серед сучасних вітчизняних автоматизованих комплексів виявлення електромагнітних випромінювань слід відзначити комплекси “АКОР” та

РІАС-РДм “DigiScan EX”. Обидва комплекси розроблені головним конструктором, к.т.н. О.В. Шпитою.

Особливість цих комплексів полягає у тому, що вони, по-перше, здатні виявляти наявність радіозакладних пристроїв з шумоподібною та випадковою несучою і, по-друге, локалізувати місце знаходження радіозакладок. Для цього у комплекси введено ряд додаткових пристроїв та програм. Крім того, такі комплекси використовуються для перевірки відповідності рівня захисту об’єкту технічним вимогам та надійності блокування каналів витоку акустичної інформації. Ці комплекси розроблені в Україні та пройшли відповідну атестацію. Вони є офіційними приладами захисту інформації у нашій країні.

На рис. 3.6 показано зовнішній вигляд та інтерфейс апаратно-програмного комплексу РІАС-РДм “DigiScan EX”, на рис. 3.7 – “АКОР”.

Рис. 3.6. Зовнішній вигляд та інтерфейс апаратно-програмного комплексу РІАС-РДм “DigiScan EX”

Рис 3.7. Зовнішній вигляд та інтерфейс апаратно-програмного комплексу “АКОР”

Крім того, при використанні додаткового конвертору зверхнизьких частот DS-LINE програма може виявляти підслуховувальні пристрої, що використовують кабельні комунікації для передавання ***звукової інформації*** з приміщення у діапазоні частот від 5 кГц до 2 МГц (мережа 220 В, телефонні кабелі, дроти сигналізації).

Розглянемо методику та засоби пошуку та знешкодження радіозакладних пристроїв. При наявності комплексу радіомоніторингу при проведенні таких робіт необхідно провести моніторинг ефіру. В разі відсутності такого комплексу можна проводити контроль за допомогою сканера.

Такі роботи проводяться двома – трьома особами і завжди починаються з розпитувань хазяїв приміщення, що перевіряється: чи дарували їм якісь сувеніри, якщо так, то коли, й які з них знаходяться у приміщенні?

Далі завжди проводять візуальний огляд приміщення, звертаючи особливу увагу на зручні (для розміщення закладки) місця. У цих роботах слід користуватися ліхтариком. Крім меблів, слід оглянути електричні та телефонні розетки, вентиляційні отвори, ніші для батарей опалювання і т. п. Також особливу увагу слід звернути на рамки від різних картин, естампів, портретів, фотографій. При огляді цих предметів треба детально проаналізувати

їх конструкцію та перевірити, чи не виконані вони так, що утворюють резонансний контур для ВЧ-нав'язування.

Далі сканером перевіряється ефір. При цьому для активації закладок, що спрацьовують від акустичного сигналу, застосовується спеціальні сигнали, записані на магнітофон. Така фонограма записується з суміші мовних та синусоїдальних сигналів з частотою 400 Гц та 1 кГц.

Одночасно можна починати перевірку у близькому полі. Для цього використовуються індикатори (або детектори) поля. Такі прилади фіксують наявність джерела випромінювання, що розміщено на відстані до 25 см від антени апарата. Це портативний широкосмуговий радіоприймач, що реагує на електромагнітне поле (джерело радіовипромінювання).

Як правило, такі прилади забезпечені світовою та звуковою індикацією, яка сигналізує про наближення до джерела випромінювання. Часто вони мають вбудований частотомір з індикацією частоти випромінювання. Такі прилади є незамінними там, де неможливо провести візуальний контроль.

Серед таких приладів можна назвати детектор марки "D-006" фірми "СмерШ Техникс" (м. С.-Петербург) та пошуковий прилад "РТ-2" московської фірми "НОВО", що поєднує у собі функції детектора поля та частотоміра. Найбільш досконалими є прилади фірми "Optoelectronics", наприклад, "РТ-/025". Деякі з цих приладів наведено на рис. 3.8 та рис. 3.9.

Крім того, необхідно провести комплексну перевірку електромережі, телефонної мережі на відсутність закладних пристроїв, що від них живляться, та інфрачервоних джерел випромінювання (зокрема, телевізійних камер). Таку перевірку дозволяє провести прилад комплексного контролю "Акула" (прилад СРМ – 700, виробництва США) – рис. 3.10.

Рис. 3.8. Сканер AR-8600

Рис. 3.9. Індикатор-частотомір електромагнітного випромінювання для пошуку у ближньому полі фірми “Optoelectronics”

Рис. 3.10. Прилад універсальний СРМ-700, "Акула", виробництва США

Аналогічний прилад розроблено та серійно виробляється у РФ. Це прилад “Піранья”. Оскільки він розроблений пізніше “Акули”, то розробники забезпечили кращі параметри та експлуатаційні характеристики у своєму виробі. Прилад “Піранья” показаний а рис. 3.11.

Рис. 3.11. Прилад універсальний "Піранья", виробництва РФ

І, нарешті, для виявлення закладок, що керуються дистанційно і можуть бути відключені від джерела живлення на час перевірки, слід застосувати так званий ***нелінійний локатор***, тобто апарат, який виявляє напівпровідникові прилади навіть якщо вони не працюють.

За допомогою такого апарату слід перевірити всі предмети інтер'єру, стіни, стелю (особливо, якщо вона підвісна), підлогу (особливо паркетну).

Апаратура цього типу побудована на властивій всім напівпровідникам нелінійності характеристик, отже на обов'язковому процесу нелінійного перетворення сигналів (модуляції), що на них подаються у будь-який спосіб. Тому такі апарати випромінюють імпульси (або змінне електромагнітне поле достатньої потужності) та приймають і аналізують сигнал відгуку на наявність у ньому нових частотних складових, що відповідають другій та третій гармонікам контрольного сигналу. Це прилад фірми "Энвис" NR-900EM, «Циклон» (РФ), Armashield (Англія). Це найбільш точні та надійні (з точки зору виявлення закладок) апарати. На жаль, їх вартість сягає десятків тисяч доларів.

Приклад таких приладів наведено на рис. 3.12.

Рис. 3.12. Нелінійний локатор фірми "Энвис" NR-900EM, виробництва РФ

Крім виявлення радіозакладних пристроїв їх можна придушити шляхом встановлення активної радіотехнічної ***широкосмугової*** або ***прицільної*** (***вузькосмугової***) завади. Вузькосмугова завада ставиться в тому випадку, коли точно відома частота, на якій працює радіозакладка. Але цей спосіб захисту використовується рідко та лише в разі, коли передавач закладки має дуже велику потужність.

Серед таких приладів слід виділити ряд вітчизняних сучасних генераторів завади, побудованих на принципі випромінювання в ефір шумових електромагнітних коливань. Серед найсучасніших приладів такого типу можна назвати прилад “Завада”, м. Київ, та ряд приладів фірми PIAC.

В таких приладах використовуються генератор випадкового сигналу, підсилювачі потужності та випромінювачі. Але прилад “Завада” має значну перевагу над зарубіжними аналогами. По-перше, він має високу потужність, що дозволяє перекрити велику площу захисту, і, по-друге, його генератор побудовано на генерації “білого” шуму у широкій смузі частот, значно ширше, ніж у всіх інших приладів такого типу.

Слід додати, що прилади постановки радіотехнічної завади мають ще одне важливе призначення. Їх застосовують для блокування радіовибухових пристроїв під час розмінування. І в цьому випадку пристрій “Завада” має незаперечну перевагу, оскільки його генератор побудований на принципі генерації шуму, а не псевдовипадкових послідовностей, що використовуються у більшості інших аналогічних приладів.

Саме тому при його застосуванні виключається можливість випадкового співпадіння сигналу завади з кодом підриву вибухового пристрою.

3.4. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами

При розгляді методів та засобів зняття інформації ми побачили, скільки можливих каналів витоку виникає на різноманітних технічних засобах, які використовуються у робочих приміщеннях та побуті.

Зрозуміло, що при проектуванні системи захисту інформації слід потурбуватися про блокування цих каналів.

Найбільш імовірне їх використання – це зняття акустичної та електромагнітної інформації. Найчастіше використовуються механізми перетворень акустичних сигналів у електричні та паразитні випромінювання і наводки.

Також ніколи не виключається можливість використання супротивником ВЧ-нав'язування.

Для блокування таких каналів витоку використовуються активні методи протидії. Блокувати такі канали витоку можна застосуванням активної завади у радіотехнічному та звуковому діапазоні частот. При цьому слід забезпечити можливість виконання технічними засобами, які треба захистити, своїх основних функцій без перешкод для їх роботи з боку засобів захисту інформації.

Для цього у різних країнах на різних етапах розвитку методів та засобів технічного захисту інформації розроблялися окремі прилади, використання яких вимагало узгодження їх різних характеристик та можливостей для отримання цілісного комплексу захисту інформації.

На теперішній час вітчизняною фірмою РІАС створено та атестовано цілісний комплекс РІАС–ЛЗ, що виробляється за технічними умовами ТУ У 31.6-33694400-002:2009 та призначений для захисту інформації від витоку по провідних лініях електроживлення, пожежної та охоронної сигналізації, радіо- та телефонної мереж і т.п.

До комплексу входить ряд приладів, зокрема:

- низка роздільних трансформаторів різної потужності РІАС-4ТР;

- прилади захисту інформації у електромережі з придушенням небезпечних сигналів у смузі частот від 180 Гц до 30 МГц РІАС-4 ЗМ/1 та РІАС-4 ЗМ/2;

- генератор шуму у звуковому діапазоні частот РІАС-4 ШМ;

- генератор шумоподібного сигналу для електромережі у діапазоні частот від 20 кГц до 1 ГГц РІАС-4 НМ;

- фільтр загороджувальний високих частот в слабкострумових лініях РІАС-4 ФС, призначений для захисту таких ліній від проходження сигналів ВЧ-нав'язування;

- генератор шумоподібного сигналу у мовному діапазоні у слабкострумових лініях РІАС-4 ШС, що забезпечує активне маскування сигналу парази-

тного акустоелектричного перетворення у мовному частотному діапазоні у слабкострумових лініях;

- генератори шумоподібного радіочастотного сигналу у лініях аналогового телефонного зв'язку та у слабкострумових лініях PIAC–4 НС.

Всі прилади, що входять у комплекс, побудовані на одній елементній базі та на одному загальному принципі. У більшості з них є вбудовані пристрої автоматизованого контролю працездатності.

Для активного захисту інформації від ВЧ-нав'язування можна використати новий метод, запропонований О.В. Рибальським.

Його застосування змінює властивості сигналу ВЧ-нав'язування, що робить його непридатним для отримання акустичної інформації.

Цей ефект виникає тому, що випромінюється спеціальний сигнал протидії з частотою, близькою до частоти сигналу зондування ВЧ-нав'язування. Це призводить до виникнення явища биття між цими сигналами, а при наближенні частоти випромінюваного сигналу протидії до частоти сигналу ВЧ-нав'язування відбувається навіть захоплення частоти сигналу протидії генератором сигналу зондування ВЧ-нав'язування.

В результаті взаємодії двох таких коливань виникає нове коливання з частотою

$$\omega = \frac{\omega_1 + \omega_2}{2}, \tag{3.1}$$

де

ω_1 – частота сигналу протидії,

ω_2 – частота сигналу зондування,

та змінною амплітудою, максимальні значення якої повторюються з частотою

$$\Omega = \omega_1 - \omega_2 . \tag{3.2}$$

При цьому, при переході амплітуди цих коливань через нуль відбувається змінювання їх фази.

При використанні ВЧ-нав'язування зняття інформації може відбуватися методами амплітудної, частотної та фазової модуляції.

Сам факт виникнення нового коливання з іншою частотою вже перешкоджає зняттю інформації, оскільки не відбувається перевипромінювання модульованих інформацією сигналів, або їх рівень значно послаблюється.

Змінювання фази нового коливання перешкоджає зняттю інформації методом фазової модуляції. Але цей ефект підвищується для фазової та частотної модуляції за рахунок змінювання частоти генерації випромінюваного сигналу вліво та вправо від її середнього значення сигналом керування, складеним з ***випадковим*** сигналом. Крім того, виникає паразитна амплітудна модуляція перевипромінюваних сигналів.

А складання генерованого сигналу з іншим випадковим сигналом призводить до ще більшого рівня завади для амплітудної модуляції, що додатково перешкоджає зняттю інформації.

3.5. Захист інформації від несанкціонованого запису звукозаписувальними пристроями

Захист інформації від такого виду несанкціонованого зняття стає дедалі актуальнішим. При цьому слід виділити два напрямки захисту:

1. Виявлення у відвідувача або в приміщенні диктофона;

2. Придушення можливості запису на аналоговий апарат або на апарат цифрового звукозапису.

Виявлення звукозаписувального приладу у відвідувача може бути проведено звичайним детектором металу, але для цього його треба піддати явному контролю.

Якщо така дія є небажаною, то можна скористатися індикаторним приладом наявності диктофону. Такий прилад розташовується у одязі на тілі

особи, що проводить перевірку. При наближенні на відстань до 0,5 – 1 м до працюючого диктофону прилад починає вібрувати. Промисловість багатьох країн випускає подібну апаратуру, наприклад, “ST-041” (РФ, С.-Петербург).

Для придушення можливості ***несанкціонованого запису інформації*** використовуються як прилади з випромінюванням акустичної завади, так і прилади з застосуванням електромагнітної завади. Серед такої апаратури можна відзначити прилад ЛГШ-103 “РаМЗес-Дубль”, призначений для захисту від несанкціонованої роботи апаратури магнітного звукозапису (магнітофони, диктофони). Серед апаратури для загального придушення будь-яких пристроїв з мікрофоном та радіоелектронною схемою слід виділити прилад “Завада” (Київ) та пристрій “Шторм” (С.-Петербург). Розробка подібних пристроїв проводиться і в НАВС, на них отримані патенти України на винаходи.

При користуванні такими приладами слід пам’ятати, що вони випромінюють електромагнітне поле великої інтенсивності. Тому час роботи з такою апаратурою повинен бути обмежений та не перевищувати 1 – 2 години на добу.

3.6. Захист електронної інформації

Проблемам захисту електронної інформації присвячено дуже багато робіт як відкритого, так і спеціального характеру. Проведення робіт з такого виду захисту інформації вимагає застосування спеціального обладнання та засобів вимірювальної техніки, які є лише на крупних спеціалізованих підприємствах радіоелектронного профілю (великі науково-дослідні інститути, заводи). Як правило, вони мають ліцензії на виконання таких робіт та виконують їх на замовлення інших установ.

Основні методи, що використовуються для захисту від витоку інформації з електронної, офісної та обчислювальної техніки:

- екранування паразитних випромінювань та наводок;
- маскування сигналів від паразитних випромінювань та наводок;

- застосування спеціальних ланцюгів заземлення;

- використання спеціальних джерел електроживлення;

- використання спеціальних фільтрів у мережах електроживлення;

- програмне шифрування інформації при її запису на жорсткий диск.

Всі ці роботи вимагають складного технологічного обладнання. Наприклад, екранування комп'ютерної техніки проводиться напиленням тонких захисних шарів металу шляхом осадження у вакуумі. Захищаються таким чином корпуси системного блоку, монітору, магнітних та оптичних накопичувачів та інші блоки. Для маскування використовуються генератори широкосмугового шуму з спеціальним спектральним складом, який адаптується під кожний конкретний виріб.

Крім того, захищені засоби обробки інформації розміщуються у спеціальних приміщеннях з обмеженим доступом, а в самому приміщені встановлюється спеціальний додатковий пристрій – генератор випадкових електромагнітних коливань, які випромінюють їх у ефір та перешкоджають зняттю інформації з використанням паразитних випромінювань та наводок.

Найбільш часто для цього використовуються прилади "Волна" (виробництво РФ) та "Базальт" (Україна, м. Київ).

3.7. Захист письмової інформації від оптичного зняття

Зрозуміло, що отримати чужу письмову інформацію можна способом перлюстрації або звичайної крадіжки, але питання боротьби з такими правопорушеннями є предметом розгляду інших курсів.

Тому розглянемо захист від оптичного зняття письмової інформації, яку можна зняти як з паперового носія, так і з екрану монітора комп'ютера.

Основними засобами захисту в такому разі будуть захист від зняття через вікна за допомогою фотографуючих та телевізійних пристроїв (відеокамер) із спеціальними довгофокусними об'єктивами, так і за допомогою телекамер (відеокамер), розміщених у приміщенні. Захист від оптичного зняття

через вікна досягається або використанням спеціального скла (матового чи з нерівностями, що неуможливлюють перегляд приміщення), або застосуванням штор та спеціальних плівок, які наклеюють на скло.

Захист від телевізійних (відео) камер, які несанкціоновано встановлені всередині приміщення, досягається використанням приладів, що ставлять активну заваду роботі електронних приладів (що не завжди можливо), або пошуком, виявленням та знешкодженням таких пристроїв.

Пошук телевізійних камер здійснюється тими самими приладами та за тією ж самою методикою, що і пошук радіозакладних пристроїв.

Висновки до розділу 3

Розглянуті у попередній главі класифікація способів та засобів несанкціонованого зняття інформації та методи і засоби протидії протиправним посяганням на інформацію дають підстави зробити висновок, що процес такої боротьби є безперервним. Це так звана боротьба “калібру та броні”. По мірі розвитку засобів захисту набувають подальшого розвитку засоби нападу. Далі удосконалюються засоби захисту і т. д.

Отже, слід завжди пам’ятати, що в цій боротьбі нападник завжди попереду і весь час не втрачати пильності.

Зрозуміло, що як розробкою засобів нападу, так і розробкою засобів захисту займаються фахівці у цих напрямках науки і техніки. Але для забезпечення інформаційної безпеки Вам треба завжди бути обізнаними з тим новим, що з’являється у цих галузях.

Питання для самоконтролю до розділу 3

1. Дайте визначення об’єкту технічного захисту інформації.
2. Коли використовується комплексний захист інформації?
3. Дайте визначення основних технічних засобів.

4. Дайте визначення допоміжних технічних засобів.

5. Дайте визначення поняття загрози для інформації.

6. Дайте визначення поняття рівня технічного захисту інформації.

7. Дайте визначення поняття активний захист інформації.

8. Дайте визначення поняття пасивний захист інформації.

9. Чим відрізняється пасивний захист від активного захисту інформації?

10. Який порядок проведення робіт з технічного захисту інформації на об'єкті?

11. Які фізичні явища покладені у методи та засоби захисту акустичної інформації від витоку по вібраційних каналах?

12. В чому полягає метод "завантаження мембрани", що використовується для придушення мікрофонів?

13. Які прилади використовуються для захисту акустичної інформації, що циркулює у приміщенні, від зняття з телефону?

14. Які засоби захисту акустичної інформації використовуються для її захисту при передаванні по телефонних мережах у проміжку від телефону до АТС?

15. Які прилади використовуються для виявлення засобів зняття акустичної інформації з телефонних мереж у проміжку від телефону до АТС?

16. Які засоби захисту акустичної інформації використовують для її захисту по всьому ланцюгу передавання у телефонній мережі між двома телефонами?

17. На що потрібно звертати увагу при візуальному пошуку радіозакладних пристроїв?

18. Які методи використовують для виявлення радіозакладних пристроїв?

19. Які функції виконують програми моніторингу ефіру?

20. Який алгоритм виявлення радіозакладних пристроїв з використанням методу моніторингу ефіру?

21. Які функції виконують сканери?

22. Які функції виконують індикатори електромагнітного поля?

23. Які функції виконують нелінійні локатори?

24. Які багатофункціональні прилади використовують для виявлення засобів зняття інформації?

25. Які методи пошуку радіозакладних пристроїв, побудованих на використанні способу ВЧ-нав'язування?

26. Як використовуються генератори шуму для захисту акустичної інформації?

27. На яких принципах будуються генератори шуму?

28. Які методи та засоби використовуються для виявлення та захисту акустичної інформації від несанкціонованого запису звукозаписувальними пристроями?

29. Які методи та засоби використовуються для захисту електронної та електромагнітної інформації?

30. Які технічні методи та засоби використовуються для захисту письмової інформації?

Перелік рекомендованої літератури до розділу 3

1. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / Рибальський О.В., Хахановський В.Г., Шорошев В.В., Грищенко О.І., Сторожев С.В., Кобець М.В. – К.: НАВСУ, 2003. – 160 с.

2. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

3. Хорошко В.О. Основи інформаційної безпеки /Хорошко В.О., Чередниченко В.С., Шелест М.Є./ За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

4. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.

5. Максименко Г.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств / Максименко Г.А., Хорошко В.А. – К.: ООО «ПолиграфКонсалтинг», 2004. – 317 с.

Перелік умовних скорочень

АІС – автоматизована інформаційна система

АНБ – Агентство національної безпеки США

АС – автоматизована система

АТС – автоматична телефонна станція

АЧХ – амплітудно-частотна характеристика

ВЧ – висока частота

ВЧН – високочастотне нав’язування

ДСТУ – державний стандарт України

ДТЗС - додаткові технічні засоби і системи

ДССЗіТЗІ – Державна служба спеціального зв’язку і технічного захисту інформації

ЗМІ – засоби масової інформації

НСД – несанкціонований доступ

ОС – охоронна сигналізація

ПЕМВН – паразитні електромагнітні випромінювання та наводки

ПЕОМ – персональна електронно-обчислювальна машина

ТЗІ – технічний захист інформації

ТЗПІ – технічні засоби прийому, переробки, зберігання і передачі інформації

ТЗР - технічний засіб розвідки

ТКВІ – технічний канал витоку інформації

ТУУ – технічні умови, Україна

УКХ – ультракороткохвильовий діапазон радіозв’язку

ФНЧ – фільтр нижніх частот

Перелік умовних позначень одиниць вимірювання фізичних величин, що використовуються в посібнику

А (Ампер) - одиниця вимірювання сили електричного струму

Гн (Генрі) - одиниця вимірювання індуктивності

Гц (Герц)- одиниця вимірювання частоти

В (Вольт) - одиниця вимірювання напруги електричного струму

Ф (Фарада) - одиниця вимірювання електричної ємності

Головні приставки до одиниць вимірювання, на які вони помножуються

10^{-12} - піко

10^{-9} - нано

10^{-6} - мікро

10^{-3} - мілі

10^{3} - кіло

10^{6} - мега

10^{9} - гіга

але,

1 байт = 8 біт

1кбіт = 2^{10} біт

1 кбайт = 2^{10} байт = 8×2^{10} біт

1 Мбіт = 2^{10} кбіт = 2^{20} біт

1 Мбайт = 2^{10} кбайт = 2^{20} байт = 8×2^{20} біт

1 Гбіт = 2^{10} Мбіт = 2^{20} кбіт = 2^{30} біт

1 Гбайт = 2^{10} Мбайт = 2^{20} кбайт = 8×2^{30} біт

Загальний список літературних джерел, на які є посилання у тексті посібника

1. Конституція України. – Урядовий кур'єр. – 13 липня 1996 р.

2. Закон України "Про інформацію" // Відомості Верховної Ради, 1992, № 48, с. 650 – 651.

3. Закон України "Про державну таємницю" від 21.01.1994 // Відомості Верховної Ради України. – 1994. – № 16. – с. 93.

4. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

5. Закон України "Про основи національної безпеки України"// Урядовий кур'єр, 30 липня 2003 р.

6. Постанова Верховної Ради України від 16 січня 1997 року N 3/97-ВР "Про затвердження Концепції національної безпеки України"

7. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 р.

8. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест /За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

9. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / О.В. Рибальський, В.Г. Хахановський, В.В. Шорошев, О.І. Грищенко, С.В. Сторожев, М.В. Кобець. – К.: НАВСУ, 2003. – 160 с.

10. Иофе В.К. Справочник по акустике / В.К. Иофе, В.Г. Корольков, М.А. Сапожков / Под ред. М.А. Сапожкова. – М.: Связь, 1979. – 312 с.

11. Гоноровский И.С. Радиотехнические цепи и сигналы, ч. 1 / И.С. Гоноровский. – М.: Соврадио, 1967. – 439 с.

12. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф.Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.

13. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

Навчальне видання

Олег Володимирович Рибальський, Валерій Георгійович Хахановський,
Вадим Анатолійович Куднов, В’ячеслав Михайлович Смаглюк

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Посібник