

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»
Кафедра радіотехніки та телекомунікацій

ТЕКСТИ (конспект) лекцій з дисципліни

Методи і засоби захисту інформації.
(Частина 1)
для студентів спеціальності 172 " Телекомунікації та радіотехніка"
усіх форм навчання

Тексти (конспект) лекцій з дисципліни «Методи і засоби захисту інформації» (Частина 1) для студентів спеціальності 172 "Телекомунікації та радіотехніка" усіх форм навчання / Укл.: В.О. Костенко, І.М. Сметанін. - Запоріжжя: НУ «Запорізька політехніка», 2019. – 66 с.

Укладачі: В.О. Костенко, доцент, канд.техн.наук;
І.М. Сметанін, старший викладач

Рецензент: В.П. Дмитренко, доцент, канд.техн.наук

Відповідальний
за випуск: І.М. Сметанін, старший викладач

Затверджено
на засіданні кафедри
радіотехніки і телекомунікацій.
Протокол № 3 від 16.10.2019 р.

Рекомендовано до видання НМК
факультету радіоелектроніки та
телекомунікацій
Протокол № 3 від 24.10.2019 р.

ЗМІСТ

ЗМІСТ	3
ВСТУП.....	5
1 ЗАГРОЗИ БЕЗПЕКИ ІНФОРМАЦІЇ І ОБ'ЄКТИ ЗАХИСТУ	6
1.1 Загрози безпеки інформації	6
1.2 Об'єкти захисту	8
1.3. Відомості, що охороняються, і демаскуючі ознаки.....	10
2 ХАРАКТЕРИСТИКИ ТЕХНІЧНИХ КАНАЛІВ ПРОСОЧУВАННЯ ІНФОРМАЦІЇ.....	14
2.1 Канали просочування інформації, яка оброблюється технічними засобами прийому, обробки, зберігання і передачі інформації	14
2.1.1 Електричні канали	15
2.1.2 Електромагнітні канали	17
2.1.3 Параметричні канали.....	18
2.1.4 Вібраційні канали	18
2.2 Канали просочування мовної інформації	18
2.2.1 Акустичні канали.....	19
2.2.2 Віброакустичні канали	19
2.2.3 Акустоелектричний канал	20
2.2.4 Оптиелектронний (лазерний) канал	21
2.2.5 Параметричні канали.....	21
2.3. Канали просочування інформації при її передачі по каналах зв'язку	21
2.3.1 Електромагнітні канали	22
2.3.2 Електричні канали	22
2.3.3 Індукційний канал	22
2.4 Технічні канали витоку відеоінформації.....	23
2.4.1 Спостереження за об'єктами.....	23
2.4.2 Зйомка об'єктів.....	24
2.4.3 Зйомка документів.....	24
2.5 Несанкціонований доступ до інформації, що обробляється засобами обчислювальної техніки	24
2.5.1 Атаки на рівні систем управління базами даних	24
2.5.2 Атаки на рівні операційної системи	25
2.5.3 Атаки на рівні мережевого програмного забезпечення	25
2.5.4 Програмні закладки	26

2.6. Технічні канали просочування інформації, що виникає при роботі обчислювальної техніки за рахунок ПЕМВН	26
2.6.1 Класифікація каналів витоку інформаційних сигналів за рахунок ПЕМВН.....	27
2.6.2 Критерії захищеності ЗОТ	30
3 АКУСТИЧНІ І ВІБРОАКУСТИЧНІ КАНАЛИ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ З ОБ'ЄМІВ ВИДІЛЕНИХ ПРИМІЩЕНЬ.....	32
3.1 Основні поняття, визначення і одиниці вимірювань в акустиці	32
3.2 Основні акустичні параметри мовних сигналів.....	34
3.2.1 Частотний діапазон мови	34
3.2.2 Рівні мовних сигналів.....	34
3.2.3 Динамічний діапазон	35
3.2.4 Сприйняття мови	35
3.2.5 Розбірливість і зрозумілість мови.....	37
3.3 Поширення акустичних сигналів в приміщеннях і будівельних конструкціях	39
3.4 Канали просочування мовної інформації	41
3.5 Віброакустичні канали	42
3.6. Акустичне підслуховування – пасивний спосіб добування інформації.....	44
4 ЗНІМАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЗАКЛАДНИХ ПРИСТРОЇВ.....	49
4.1 Побудова і загальні характеристики закладних пристроїв.....	49
4.1.1 Загальні характеристики закладних пристроїв	50
4.1.2 Радіозакладні пристрої.....	51
4.1.3 Радіозакладні пристрої, що перевипромінюють.....	57
4.1.4 Закладні облаштування типу «довге вухо».....	59
4.1.5 Мережеві закладні пристрої	60
ЛІТЕРАТУРА.....	604

ВСТУП

Інформація є категорією економічною, оскільки вона може бути оцінена з урахуванням витрат на її створення і втрат у разі її витоку. Втрата закритої державної інформації може нанести державі непоправний ущерб - як економічний, так і політичний.

Знання конфіденційної інформації завжди допомагає швидше і ефективніше вирішувати проблеми, що стоять перед державою, фірмою або людиною.

Інформація може або накопичуватися в місці її створення, або передаватися адресатам каналами поштової, електро- чи радіозв'язку. Найбільша кількість інформації передається у вигляді повідомлень по технічних каналах спеціальними технічними засобами. Інформація шифрується і передається за допомогою сигналів. Сигнали можуть бути звукові, електромагнітні, світлові та ін.

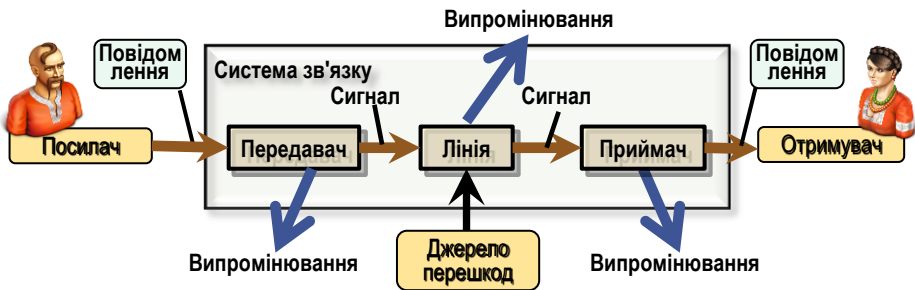


Рисунок 1.1 – Структурна схема каналу зв'язку

Передавач і приймач пов'язані між собою лінією зв'язку. Лінія може бути, наприклад, парою дротів або обмеженою зоною простору, по якій електромагнітні хвилі поширюються від передавача до приймача.

У основі утворення каналу передачі інформації і в основі появи каналів просочування інформації лежать фізичні процеси, які протікають в технічних системах передачі інформації.

1 ЗАГРОЗИ БЕЗПЕКИ ІНФОРМАЦІЇ І ОБ'ЄКТИ ЗАХИСТУ

1.1 Загрози безпеки інформації

Під безпекою інформації прийнято розуміти стан захищеності інформації, носіїв і засобів, що забезпечують її отримання, обробку, зберігання, передачу і використання, від різного виду загроз.

Основні джерела загроз безпеки інформації можна розділити на дві групи:

1. Неумисні джерела.
2. Умисні джерела.

До групи **неумисних** джерел відносяться:

- недостатня кваліфікація (некомпетентність) обслуговуючого технічні засоби обробки інформації (ТЗОІ) персоналу і керівного складу;
- недосконалість програмного забезпечення засобів і систем інформатизації і АСУ;
- недосконалість технічних рішень, реалізованих при розробці, створенні і монтажі ТЗОІ;
- природне старіння технічних засобів і систем в процесі експлуатації, що призводить до зміни їх властивостей і характеристик;
- екстремальні навантаження, випробовувані ТЗОІ в процесі експлуатації;
- несправності ТЗОІ і допоміжного устаткування;
- дії власників або законних користувачів інформації, не переслідуючи корисних цілей, але що призводять до непередбачених наслідків;
- стихійні лиха і катастрофи.

Процес прояви неумисних джерел носить, як правило, випадковий характер і не переслідує мети порушення безпеки інформації. Проте наслідки таких процесів можуть бути дуже серйозними.

До групи **умисних** джерел загроз безпеки інформації можна віднести:

- дії іноземних розвідок і спецслужб;
- дії конкурентів (промислове шпигунство);

– дії зловмисників (терористів, злодіїв, шантажистів, хуліганів і тому подібне).

Процеси прояви умисних джерел загроз безпеки інформації (дії супротивника) мають цілеспрямований характер.

Інтереси розвідок і спецслужб охоплюють усі сфери діяльності супротивної держави (економічну, політичну, науково-технічну, військову і так далі). Для держави порушення безпеки інформації може обернутися значним політичним, економічним, військовим збитком і привести до зниження рівня національної безпеки.

Інтереси конкуруючих підприємств в умовах ринкової економіки спрямовані на добування інформації, що відноситься до сфери комерційної, фінансової, виробничої таємниці, тобто інформації про комерційні плани, фінансовий стан фірм, технічні і технологічні досягнення, про картотеки клієнтів, про програмне забезпечення і так далі. Отримання і використання, а також знищення або спотворення такої інформації конкурентами може заподіяти істотний збиток підприємству – власникові інформації.

До цього ж виду джерел загроз слід віднести і можливі дії вітчизняних підприємств і організацій з добування інформації про технічні і технологічні досягнення в космічній промисловості, інші передові галузі науки і техніки, оскільки ці досягнення частенько можуть бути застосовані в інших сферах людської діяльності.

Дії різного роду зловмисників пов'язані в основному з комп'ютерними злочинами. Такі злочини скоюються організованими злочинними групами або злочинцями-одинаками в цілях розкрадання великих грошових сум, незаконного користування різними послугами, посягання на державну, комерційну і особисту таємницю, шантажу, тероризму, втручання в роботу систем управління і тому подібне. Мотиви скоєння комп'ютерних злочинів можуть і не переслідувати матеріальних вигід. У цих випадках на перше місце висуваються інші цілі: затвердження свого «я», помста за образу, бажання «пожартувати».

Загрози безпеки інформації реалізуються через небезпечні дії з боку перелічених вище джерел загроз на певні інформаційні об'єкти: інформаційні ресурси, інформаційні системи і технології, засоби забезпечення автоматизованих інформаційних систем і технологій. При цьому залежно від мети дії розрізняють декілька основних видів загроз.

1. Знищення. При знищенні інформаційних об'єктів або їх елементів вони втрачаються, тобто або переходять в руки сторонніх осіб (наприклад, при розкраданні), або знищуються або руйнуються (наприклад, в результаті стихійного лиха або озброєного конфлікту, безграмотних дій законних користувачів, умисного введення в програмне забезпечення певного типу вірусів і тому подібне).

2. Витік. При витіку інформаційні об'єкти не втрачаються, проте стають доступними стороннім особам (наприклад, випадкове або умисне підслуховування конфіденційної розмови, перехоплення випромінювань РЕЗ технічними засобами розвідки, незаконне копіювання інформації в комп'ютерних системах, аналіз і узагальнення безлічі джерел відкритої інформації і тому подібне).

3. Спотворення. Результатом спотворення є несанкціонована зміна змісту (структури) інформаційного об'єкту (наприклад, введення неправдивої інформації в систему обробки, зміну елементів програмного забезпечення, зміну змісту банку даних і тому подібне).

4. Блокування. В результаті блокування інформаційний об'єкт не втрачається, але стає недоступним для його власника або користувача (споживача) в результаті фізичного або логічного блокування цього елементу.

Кожна з розглянутих загроз при її реалізації може привести до серйозних наслідків з точки зору безпеки інформації.

1.2 Об'єкти захисту

Відповідно до законів України захисту підлягає інформація, віднесена до державної таємниці, конфіденційна інформація, у тому числі персональні дані, неправомірне поводження з якими може завдати збитку її власникові, користувачеві або іншій особі.

Власниками, користувачами (споживачами) інформації можуть бути державні і недержавні підприємства, організації, фізичні особи.

Основні об'єкти захисту можна об'єднати в наступні групи:

- власники, користувачі (споживачі) інформації;
- носії і технічні засоби передачі і обробки інформації;
- системи інформатизації, зв'язку і управління;
- озброєння і військова техніка;
- об'єкти органів управління, військові і промислові об'єкти.

В цілях інформаційної безпеки необхідно забезпечити захист прав власників, а також визначити їх обов'язки і відповідальність за порушення режиму захисту.

У групі носіїв і технічних засобів передачі і обробки інформації захисту підлягають:

- власне носії інформації у вигляді інформаційних фізичних полів і хімічних середовищ, сигналів, документів на паперовій, магнітній, оптичній і інших основах;
- засоби електронно-обчислювальної техніки (ЕОТ);
- засоби зв'язку (ТЛФ, ТЛГ, ГМЗ, телефакси, телетайпи);
- засоби перетворення мовної інформації (засоби звукозапису, звукопідсилення, звуковідтворення, звукового супроводу кінофільмів);
- засоби візуального відображення (телевізори, дисплеї, засоби внутрішнього телебачення);
- засоби виготовлення і розмноження документів (принтери, ксерокси, плоттери і так далі);
- допоміжні технічні засоби (засоби, які безпосередньо не оброблюють інформацію, що захищається, але розміщені в приміщеннях, де вона обробляється);
- приміщення, виділені для проведення закритих заходів.

У системах інформатизації, зв'язку і управління необхідно забезпечити захист:

- інформаційних ресурсів (архівів, банків даних і так далі);
- інформаційних технологій;
- засобів забезпечення інформаційних систем і їх технологій (програмних, технічних, експлуатаційних, лінгвістичних та ін.).

В інтересах захисту інформації про озброєння і військову техніку захисту підлягають:

- характеристики і параметри конкретних зразків озброєння і військової техніки на усіх етапах їх життєвого циклу (проектування, розробки, створення, випробувань, виробництва, зберігання, експлуатації, знищення);
- вживані на етапах життєвого циклу технології;
- науково-дослідні, дослідно-конструкторські і пошуково-експериментальні роботи військово-прикладної спрямованості.

Для об'єктів органів управління, військових і промислових об'єктів захисту підлягає інформація:

- про місце розташування об'єкту;
- про призначення, профіль діяльності, структуру об'єкту і режими його функціонування;
- циркулююча в технічних засобах, використовуваних на об'єкті;
- про ті, що розробляються (вироблюваних, випробовуваних) або експлуатованих зразках озброєння, військової техніки або про виробництва і технології;
- про науково-дослідні і дослідно-конструкторські роботи.

1.3. Відомості, що охороняються, і демаскуючі ознаки

Технічні засоби, системи і інші об'єкти захисту мають визначені характерні для них властивості, а їх функціонування супроводжується різними процесами. Виявлення і аналіз таких властивостей і процесів дозволяє отримати уявлення про сам об'єкт захисту і про інформацію, циркулюючу в його елементах. Серед відомостей, що отримуються про об'єкт захисту при веденні розвідки, можуть бути так звані відомості, що охороняються, тобто відомості, які містять державну таємницю або віднесені до іншої категорії конфіденційних відомостей.

Відповідно до закону про державну таємницю до тих, що охороняються можуть бути віднесені наступні відомості:

- у військовій області про зміст стратегічних і оперативних планів, про напрями розвитку озброєння і військової техніки, про кількість, устрій і технологію виробництва ядерної і спеціальної зброї, про тактико-технічні характеристики і можливості бойового застосування зразків озброєння і військової техніки, про дислокацію, призначення, міру готовності і захищеності режимних і особливо важливих об'єктів і так далі;
- в області економіки, науки і техніки про зміст планів підготовки держави і окремих регіонів до можливих військових дій, про сили і засоби цивільної оборони, про об'єм, плани державного оборонного замовлення, про науково-дослідні, дослідно-конструкторські і проектні роботи, технології, що мають важливе оборонне і економічне значення;
- у сфері зовнішньої політики і економіки;
- в області розвідувальній, контррозвідувальній і оперативно-

розшукової діяльності.

Джерелами інформації про відомості, що охороняються, можуть бути різноманітні характеристики об'єктів захисту, їх елементів і створюваних ними фізичних полів. З урахуванням розвіддоступності цих характеристик вводять поняття демаскуючих ознак.

Демаскуючі ознаки (ДО) — це характеристики будь-якого роду, що піддаються виявленню і аналізу за допомогою розвідувальної апаратури і що є джерелами інформації для розвідки супротивника про відомості, які охороняються.

Демаскуючі ознаки можуть бути розподілені на первинні і вторинні.

Первинні ДО є фізичними характеристиками об'єктів і середовища, що безпосередньо зареєстровані спеціальною апаратурою і містять інформацію про відомості, що охороняються. Прикладом первинних ДО можуть служити напруженість і поляризація електромагнітного поля, амплітуда, частота і фаза змінного електричного струму, рівень радіаційного випромінювання, відсотковий вміст хімічної речовини в середовищі, сила і частота звукових коливань, яскравість і довжина хвилі світлового випромінювання об'єкту і тому подібне. Зрозуміло, що саме первинні ДО є джерелами розвідувальної інформації, що отримується за допомогою технічних засобів розвідки (ТЗР). Для деяких об'єктів первинні ДО містять усю інформацію про відомості, що охороняються. Тому знання первинних ДО має первинне самостійне значення для протидії технічним розвідкам.

Вторинні ДО — це ознаки, які можуть бути отримані шляхом накопичення і обробки первинних ДО. Прикладами вторинних ДО можуть служити різного роду зразки (зображення споруд і військової техніки, діаграми первинного і вторинного випромінювання об'єкту, амплітудно-частотні спектри випромінювань, хімічний склад речовини і так далі), процеси (радіосигнал, акустичний сигнал, залежність якого-небудь первинного ДО від часу і так далі) і ситуації, тобто поєднання різних зразків і процесів, пов'язаних з відомостями, що охороняються, про об'єкт розвідки.

Відомо, що для розробки і реалізації ефективних заходів по захисту інформації потрібен облік усіх без виключення можливостей ТЗР, а це припускає наявність максимально достовірних переліків відомостей, що охороняються, і їх демаскуючих ознак.

Нині скласти початковий перелік демаскуючих ознак (відомостей, що охороняються) формальними методами не вдається. Зазвичай це здійснюється на основі методу експертних оцінок.

Коротко основний зміст методики полягає в наступному:

1. Визначається генеральна сукупність фахівців (експертів), компетентних в області фізичних властивостей об'єкту, що захищається, шляхом їх послідовного опитування до стабілізації поповнюваного списку експертів.

2. Розраховується об'єм робочої групи експертів, виходячи з умови її репрезентативності (показності).

3. Кожен експерт незалежно від інших складає свій відранжирований по мірі важливості перелік ознак: їх число не повинне перевищувати заданої величини.

4. На підставі пропозицій експертів формується таблиця, що містить перелік усіх ознак, які не повторюються, приватні коефіцієнти ваги ознак, сумарні і середні ваги кожної ознаки. Ця таблиця дозволяє визначити думки експертів відносно необхідності включення в загальний перелік кожної з ознак.

Після того, як буде складено початковий перелік демаскуючих ознак, необхідно виявити, які з них дійсно піддаються виявленню і виміру в конкретних умовах існування об'єкту, що захищається, тобто є реально доступними для ТЗР. Актуальність рішення цієї задачі обумовлена тим, що у разі невиявлення якої-небудь реально доступної ДО вона залишається незахищеною від розвідки, а у разі прийняття реально недоступної ДО за доступну будуть марно витрачені сили, засоби і ресурси на її захист.

Очевидно також, що ознаку слід вважати доступною для ТЗР, якщо ці засоби в змозі виявити її і виміряти з необхідною точністю, якщо ДО не володіє енергетичною і параметричною скритністю.

Найбільш достовірним способом виявлення реально доступних ДО є натурні випробування, при яких енергетична і параметрична скритність визначається експериментально в заданих умовах, або за допомогою своїх ТЗР (аналогів апаратури розвідки супротивника), а також за допомогою спеціальних засобів комплексного технічного контролю. Проте разом з натурними випробуваннями широко застосовуються розрахункові методи оцінки можливостей різних видів розвідки по виявленню, вимірюванню і розпізнаванню ДО, а також методи, засновані на машинному моделюванні усіх основних

процесів технічної розвідки, що мають місце в даній обстановці.

В процесі моделювання на ЕОМ узагальнена модель процесу технічної розвідки повинна враховувати усі основні чинники, що впливають на ефективність останньої, тобто вміщувати в себе приватні моделі об'єктів, що захищаються, навколишнє оточення (фону), заходи пасивного і активного захисту, канали поширення енергії, що сприймається апаратурою розвідки, а також моделі функціонування апаратури розвідки і оцінки ефективності технічної розвідки.

2 ХАРАКТЕРИСТИКИ ТЕХНІЧНИХ КАНАЛІВ ПРОСОЧУВАННЯ ІНФОРМАЦІЇ

Під **технічним каналом просочування інформації** розуміють сукупність джерела інформації, середовища або системи, по якій поширюється інформаційний сигнал, шумів, що перешкоджають передачі сигналу, і технічних засобів перехоплення інформації.

Джерелами інформації можуть бути безпосередньо голос людини, комп'ютерні мережі, системи звукопідсилення, телефонні лінії, друкарський текст, радіопередавальні пристрої і тому подібне.

Матеріальними носіями інформації є сигнали. Сигналами є електричні, електромагнітні, акустичні і інші види коливань або хвиль, причому інформація міститься в змінах їх параметрів.

Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути повітряні, рідкі і тверді середовища. До них відносяться: повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, ґрунтові породи і тому подібне.

Шуми супроводжують усі фізичні процеси і є присутніми на вході засобів перехоплення інформації.

Засоби перехоплення інформації служать для прийому і перетворення сигналів з метою отримання інформації.

2.1 Канали просочування інформації, яка оброблюється технічними засобами прийому, обробки, зберігання і передачі інформації

До *технічних засобів прийому інформації (ТЗПІ)*, а так само її обробки, зберігання і передачі відносять технічні засоби, які безпосередньо оброблюють і передають конфіденційну інформацію. До їх числа входять електронно-обчислювальна техніка, телефонні станції, системи оперативно-командного і гучномовного зв'язку, системи звукопідсилення, звукового супроводу і звукозапису, телевізійні системи і так далі.

При виявленні технічних каналів просочування інформації технічні засоби необхідно розглядати як систему, що включає основне устаткування, кінцеві пристрої, з'єднувальні лінії у вигляді сукупності дротів і кабелів, які прокладаються між окремими ТЗПІ, розподільні і

комутаційні пристрої, системи електроживлення, системи заземлення.

Усі ТЗП відносяться до *основних технічних засобів*.

Разом з ТЗП в приміщеннях встановлюються технічні засоби і системи, що безпосередньо не беруть участь в обробці конфіденційної інформації, але які використовуються спільно з ТЗП і знаходяться в зоні електромагнітного поля, створюваного ТЗП. Такі технічні засоби і системи називаються *допоміжними технічними засобами і системами (ДТЗС)*. Це технічні засоби відкритого телефонного, гучномовного зв'язку, системи пожежної і охоронної сигналізації, засоби і системи кондиціонування, електрифікації, радіофікації, часофікації, електропобутові прилади і так далі.

В якості каналу просочування інформації найбільший інтерес представляють ДТЗС, що мають вихід за межі контрольованої зони.

Контрольована зона – територія (або будівля, група приміщень, приміщення), на якій виключено неконтрольоване перебування осіб і транспортних засобів, що не мають постійного або разового допуску. У контрольованій зоні за допомогою проведення технічних і режимних заходів мають бути створені умови, що запобігають можливості витоку, з неї конфіденційної інформації. Контрольована зона визначається керівництвом організації, виходячи з конкретної обстановки в місці розташування об'єкту і можливостей використання технічних засобів перехоплення.

Окрім з'єднувальних ліній основних і допоміжних засобів за межі контрольованої зони можуть виходити дроти і кабелі, що не відносяться до них, але які проходять через приміщення, де встановлені ці технічні засоби, а також металеві труби систем опалювання, водопостачання і інші струмопровідні металоконструкції. Такі дроти, кабелі і струмопровідні елементи називаються *сторонніми провідниками*.

Будь-який вид сигналу, з якого може бути виділена закрита інформація, називається *інформаційним*.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення, технічні канали просочування інформації можна розподілити на *електричні, електромагнітні, параметричні і вібраційні*.

2.1.1 Електричні канали

Електричні канали просочування інформації виникають за

рахунок:

- наведень електромагнітних випромінювань ТЗПІ на з'єднувальні лінії ДТЗС і сторонні провідники, що виходять за межі контрольованої зони;
- просочування інформаційних сигналів в лінії електроживлення і ланцюга заземлення ТЗПІ;
- використання закладних пристроїв.

Наведення електромагнітних випромінювань ТЗПІ виникають при випромінюванні елементами ТЗПІ інформаційних сигналів, а також за наявності гальванічного зв'язку сполучних ліній ТЗПІ і сторонніх провідників або ліній ДТЗС. Рівень сигналів, що наводяться, значною мірою залежить від потужності випромінюваних сигналів, відстані між провідниками, а також довжини спільного пробігу сполучних ліній ТЗПІ і сторонніх провідників.

Випадковою антеною є ланцюг ДТЗС або сторонні провідники, які здатні приймати побічні електромагнітні випромінювання.

Випадкові антени можуть бути зосередженими і розподіленими. Зосереджена випадкова антена є компактним технічним засобом (наприклад, телефонний апарат, ПК). До розподілених випадкових антен відносяться кабелі, дроти, металеві труби і інші струмопровідні комунікації.

Просочування інформаційних сигналів в лінії електроживлення можливо за наявності магнітного зв'язку між ланцюгами з інформаційними сигналами і блоком живлення. Крім того, струми посилюваних інформаційних сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі додаткову напругу, яка може бути виявлена в лінії електроживлення. Інформаційний сигнал може проникнути в лінію електроживлення також в результаті того, що середнє значення споживаного струму в кінцевих каскадах підсилювачів залежить від амплітуди інформаційного сигналу, що і призводить до зміни споживаного струму за законом зміни інформаційного сигналу.

Просочування інформаційних сигналів в ланцюзі заземлення. Окрім заземлюючих провідників, що служать для безпосереднього з'єднання ТЗПІ з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий дріт мережі електроживлення, екрани сполучних кабелів, металеві труби систем опалювання,

водопостачання, каналізації, металева арматура залізобетонних конструкцій і так далі. Усі ці провідники спільно із заземлюючим пристроєм утворюють розгалужену систему заземлення, в яку можуть просочуватися інформаційні сигнали.

2.1.2 Електромагнітні канали

До електромагнітних відносяться канали просочування інформації, що виникають за рахунок різного виду побічних електромагнітних випромінювань і наведень (ПЕМВН) ТЗПІ :

- випромінювань елементів ТЗПІ;
- випромінювань на частотах роботи високочастотних генераторів ТЗПІ;
- випромінювань на частотах самозбудження підсилювачів низької частоти ТЗПІ.

Електромагнітні випромінювання елементів ТЗПІ. У ТЗПІ носієм інформації є електричний струм, параметри якого (амплітуда, частота або фаза) змінюються згідно із законом зміни інформаційного сигналу. При проходженні електричного струму по струмоведучих елементах ТЗПІ навколо них виникає електричне і магнітне поля. В силу цього елементи ТЗПІ можна розглядати як випромінювачі електромагнітного поля, що несе інформацію.

Електромагнітні випромінювання на частотах роботи ВЧ-генераторів ТЗПІ і ДТЗС. До складу ТЗПІ і ДТЗС можуть входити різного роду високочастотні генератори. До таких пристроїв можна віднести: задаючі генератори, генератори тактової частоти, генератори стирання і подмагнічivanja магнітофонів, гетеродини радіоприймальних і телевізійних пристроїв і так далі.

В результаті зовнішніх дій інформаційного сигналу на елементах ВЧ-генераторів наводяться електричні сигнали, які можуть викликати паразитну модуляцію власних ВЧ-коливань генераторів. Ці модульовані ВЧ- коливання випромінюються в навколишній простір.

Електромагнітні випромінювання на частотах самозбудження ПНЧ ТЗПІ. Самозбудження ПНЧ ТЗПІ (наприклад, підсилювачів систем звукопідсилення і звукового супроводу, магнітофонів, систем гучномовного зв'язку і тому подібне) можливо за рахунок утворення випадкових паразитних позитивних зворотних зв'язків, що призводить до переведення підсилювача в режим автогенерації. Сигнал на частотах самозбудження, як правило, виявляється промодульованим

інформаційним сигналом.

Перехоплення побічних електромагнітних випромінювань ТЗПІ здійснюється засобами радіотехнічної розвідки, розташованими поза контрольованою зоною.

2.1.3 Параметричні канали

Перехоплення інформації можливе шляхом «високочастотного опромінювання» ТЗПІ. При взаємодії опромінюючого електромагнітного поля з елементами ТЗПІ відбувається перевипромінювання електромагнітного поля. У ряді випадків це вторинне випромінювання має модуляцію, обумовлену дією інформаційного сигналу.

Оскільки перевипромінюване електромагнітне поле має параметри, відмінні від опромінюючого поля, цей канал витоку інформації часто називають *параметричним*.

Для перехоплення інформації по цьому каналу потрібні спеціальні високочастотні генератори з антенами, які мають вузькі діаграми спрямованості, і спеціальні радіоприймальні пристрої.

2.1.4 Вібраційні канали

Деякі ТЗПІ мають у своєму складі друкуючі пристрої, для яких можна знайти відповідність між роздруковуваним символом і його акустичним зразком. Цей принцип лежить в основі каналу просочування інформації по вібраційному каналу.

2.2 Канали просочування мовної інформації

У разі, коли джерелом інформації є голосовий апарат людини, інформація називається *мовною*.

Мовний сигнал – складний акустичний сигнал, основна енергія якого зосереджена в діапазоні частот від 300 до 4000 Гц.

Голосовий апарат людини є *первинним* джерелом акустичних коливань, які є зміною повітряного середовища у вигляді хвиль стискування і розтягування – подовжніх хвиль.

Під дією акустичних коливань в будівельних конструкціях і інженерних комунікаціях приміщення, в якому знаходиться мовне джерело, виникають вібраційні коливання. Таким чином, у своєму первинному стані мовний сигнал в приміщенні є присутнім у вигляді

акустичних і вібраційних коливань.

Різного роду перетворювачі акустичних і вібраційних коливань є *вторинними* джерелами. До останніх відносяться: гучномовці, телефони, мікрофони, акселерометри і інші пристрої.

Залежно від середовища поширення мовних сигналів і способів їх перехоплення технічні канали просочування інформації можна розподілити на: *акустичні, вібраційні, акустоелектричні, оптоелектронні і параметричні*.

2.2.1 Акустичні канали

В акустичних каналах просочування інформації середовищем поширення мовних сигналів є повітря, і для їх перехоплення використовуються високочутливі мікрофони і спеціальні спрямовані мікрофони, які з'єднуються з портативними звукозаписними пристроями або із спеціальними мініатюрними передавачами.

Автономні пристрої, які конструктивно об'єднують мікрофони і передавачі, називають *закладними пристроями*. Перехоплена мовна інформація може передаватися по радіоканалу, мережі електроживлення, оптичному каналу, з'єднувальним лініям, стороннім провідникам, інженерним комунікаціям в ультразвуковому діапазоні частот, телефонної лінії.

Прийом інформації, що передається закладними пристроями, здійснюється на спеціальні приймальні пристрої. Виняток становить система «Довге вухо», в якій прослуховування здійснюється звичайним телефонним апаратом.

Використання портативних диктофонів і закладних пристроїв вимагає проникнення в контрольоване приміщення. У тому випадку, коли це не вдається, для перехоплення мовної інформації використовуються спрямовані мікрофони.

2.2.2 Віброакустичні канали

У віброакустичних каналах просочування інформації середовищем поширення мовних сигналів є будівельні конструкції приміщень (стіни, стелі, пол) і інженерні комунікації (труби водопостачання, опалювання, вентиляція і тому подібне). Для перехоплення мовних сигналів в цьому випадку використовуються вібродатчики (акселерометри).

Вібродатчик, сполучений з електронним підсилювачем

називають електронним стетоскопом. Електронний стетоскоп дозволяє здійснювати прослуховування мови за допомогою головних телефонів і записувати її.

По віброакустичному каналу також можливе перехоплення інформації з використанням закладних пристроїв. В основному для передачі інформації використовується радіоканал, тому такі пристрої часто називають радіостетоскопами. Можливо використання закладних пристроїв з передачею інформації по оптичному каналу в інфрачервоному діапазоні довжин хвиль, а також по ультразвуковому каналу з використанням інженерних комунікацій.

2.2.3 Акустоелектричний канал

Акустоелектричні канали просочування інформації виникають за рахунок перетворень акустичних сигналів в електричні. За фізичним принципом дії цей канал аналогічний параметричному.

Деякі елементи ДТЗС, у тому числі трансформатори, котушки індуктивності, електромагніти вторинного електромагнітного, дзвінків телефонних апаратів і тому подібне, мають властивість змінювати свої параметри (місткість, індуктивність, опір) під дією акустичного поля, що створюється джерелом мовного сигналу. Зміна параметрів призводить або до появи на цих елементах електрорушійної сили, або до модуляції струмів, що протікають по цих елементах відповідно до змін впливаючого акустичного поля.

Крім того технічні засоби можуть містити безпосередньо акустоелектричні перетворювачі. До таких відносяться деякі типи датчиків охоронної і пожежної сигналізації, гучномовці в ланцюгах трансляції і звукопідсилення і так далі. Ефект акустоелектричного перетворення іноді називають «мікрофонним ефектом».

Технічний канал просочування інформації з використанням **«високочастотного нав'язування»** може бути здійснений шляхом несанкціонованого контактного введення струмів високої частоти від генератора в лінію, яка має функціональний зв'язок з нелінійними або параметричними елементами технічних систем, на яких і відбувається модуляція високочастотного сигналу інформаційним. Інформаційний сигнал в даних елементах ДТЗС з'являється внаслідок акустоелектричного перетворення акустичних сигналів в електричні.

Найчастіше такий канал використовується для перехоплення розмов, що ведуться в приміщенні, через телефонний апарат, який має

вихід за межі контрольованої зони.

2.2.4 Оптикоелектронний (лазерний) канал

Оптико-електронний канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих під дією акустичного мовного сигналу відзеркалювальних поверхонь приміщень (шибок, дзеркал, люстр і так далі). Відбите лазерне випромінювання модулюється голосом по амплітуді і фазі і приймається приймачем оптичного або лазерного випромінювання, при демодуляції якого виділяється мовна інформація.

Для організації такого каналу переважним є використання дзеркального відображення лазерного променя. Проте при відстанях до відзеркалювальних поверхонь близько декількох десятків метрів, може бути використане дифузне відображення лазерного випромінювання.

Такі системи мають назву «Лазерних мікрофонів». Працюють вони, як правило, в довгохвильовому інфрачервоному діапазоні хвиль або на частотах роботи лазерів.

2.2.5 Параметричні канали

В результаті дії акустичного поля на усіх елементах технічних засобів змінюється взаємна дія елементів схем, дротів в котушках індуктивності, дроселів, трансформаторів і тому подібне, що може привести до змін параметрів високочастотного сигналу, наприклад, за рахунок модуляції його інформаційним сигналом. Тому цей канал просочування інформації називається параметричним. Найчастіше спостерігається паразитна модуляція інформаційним або акустичним сигналом випромінювань гетеродинів.

Параметричний канал просочування інформації може бути реалізований і шляхом «високочастотного опромінення» приміщення, де встановлені спеціальні закладні пристрої, що мають елементи, параметри яких (наприклад, добротність і резонансна частота об'ємного резонатора) змінюються під дією акустичного сигналу.

2.3. Канали просочування інформації при її передачі по каналах зв'язку

Нині для передачі інформації використовуються в основному КХ, УКХ, радіорелейні, тропосферні і космічні канали зв'язку, різні

види телефонного радіозв'язку (наприклад, стільникова), а також кабельні і волоконо-оптичні лінії зв'язку. Залежно від виду каналу зв'язку технічні канали перехоплення інформації можна розділити на *електромагнітні, електричні і індукційні*.

2.3.1 Електромагнітні канали

Електромагнітні випромінювання передавачів засобів зв'язку, модульовані інформаційним сигналом, можуть перехоплюватися портативними засобами радіорозвідки.

Цей канал найширше використовується для прослуховування телефонних розмов, що ведуться по радіотелефонах, стільниковим телефонам або по радіорелейних і супутникових лініях зв'язку.

2.3.2 Електричні канали

Електричний канал перехоплення інформації, що передається по кабельних лініях зв'язку, припускає контактне підключення апаратури перехоплення до кабельних ліній зв'язку. Найпростіший спосіб – це безпосереднє паралельне підключення до лінії зв'язку. Але цей факт легко виявляється, оскільки призводить до зміни характеристик лінії зв'язку і до падіння напруги. Тому засоби перехоплення підключаються до лінії зв'язку або через пристрої, які погоджують, що трохи знижують падіння напруги, або через пристрої компенсації падіння напруги.

Контактний спосіб використовується в основному для зняття інформації з коаксіальних і низькочастотних кабелів зв'язку. Для кабелів, усередині яких підтримується підвищений тиск повітря, застосовуються пристрої, які виключають його зниження, що запобігає спрацюванню спеціальної сигналізації.

Електричний канал найчастіше використовується для перехоплення телефонних розмов. Пристрої, що підключаються до телефонних ліній зв'язку і поєднані з пристроями передачі інформації по радіоканалу, називають телефонними радіозакладками.

2.3.3 Індукційний канал

Існуючі системи контролю дротяних ліній дозволяють строго контролювати факт несанкціонованого підключення прослуховуючих пристроїв. Тому найчастіше використовується спосіб контролю таких ліній зв'язку, який не вимагає контактного підключення –

індукційний. У індукційному каналі використовується ефект виникнення навколо кабелю зв'язку електромагнітного поля. При виникненні такого поля електричні сигнали перехоплюються спеціальними індукційними датчиками.

Сучасні індукційні датчики здатні знімати інформацію з кабелів, захищених не лише ізоляцією, але і подвійною бронею із сталевих стрічки і сталевих дроту, що обвивають кабель.

Для безконтактного знімання інформації з незахищених телефонних ліній зв'язку можуть використовуватися спеціальні високочутливі низькочастотні підсилювачі, які забезпечені магнітними антенами.

Засоби безконтактного знімання інформації можуть поєднуватися з радіопередавачами для передачі її на пункт перехоплення.

2.4 Технічні канали витоку відеоінформації

Дуже важливу роль грає *візуальна інформація*, що отримується технічними засобами перехоплення у вигляді зображень об'єктів або документів.

Залежно від характеру інформації можна виділити наступні способи її отримання :

- спостереження за об'єктами;
- зйомка об'єктів;
- зняття копій документів.

2.4.1 Спостереження за об'єктами

Залежно від умов спостереження і освітлення для спостереження за об'єктами можуть використовуватися різні технічні засоби. Для спостереження вдень – оптичні прилади у виді монокулярів, підзорних труб, біноклів, телескопів, телевізійних камер, а для спостережень вночі – прилади нічного бачення, телевізійні камери, тепловізори.

Для спостереження з великих відстаней використовуються засоби з довгофокусними оптичними системами, а при спостереженні зблизька – телевізійні камери з ширококутними об'єктивами. При цьому зображення з телевізійних камер може передаватися на монітори як по кабелю, так і по радіоканалу.

2.4.2 Зйомка об'єктів

Зйомка об'єктів проводиться для документування результатів спостереження і детальнішого вивчення об'єктів. Для зйомки об'єктів використовуються телевізійні і фотографічні засоби.

При зйомці об'єктів, також як і при спостереженні за ними, застосування тих або інших технічних засобів обумовлене умовами зйомки і часом доби.

Для зйомки об'єктів застосовуються портативні закамouflьовані фотоапарати і телекамери, які поєднані з облаштуваннями відеозапису або передачі зображень по радіоканалу.

Зйомка об'єктів вночі проводиться, як правило, зблизька. Для цих цілей використовуються портативні фотоапарати і телевізійні камери, поєднані з приладами нічного бачення, або тепловізори, а також телевізійні камери високої чутливості, які поєднані з облаштуваннями передачі інформації по радіоканалу.

2.4.3 Зйомка документів

Зйомка документів здійснюється, як правило, з використанням портативних фотоапаратів.

2.5 Несанкціонований доступ до інформації, що обробляється засобами обчислювальної техніки

У загальному випадку програмне забезпечення будь-якої універсальної комп'ютерної системи складається з трьох основних компонентів: операційної системи, мережевого програмного забезпечення і системи управління базами даних (СУБД). Тому усі спроби злому захисту комп'ютерних систем можна розподілити на чотири групи:

- атаки на рівні систем управління базами даних;
- атаки на рівні операційної системи;
- атаки на рівні мережевого програмного забезпечення;
- програмні закладки.

2.5.1 Атаки на рівні систем управління базами даних

Захист СУБД є одним з найпростіших завдань. Це пов'язано з тим, що СУБД мають строго певну внутрішню структуру, і операції

над елементами СУБД задана досить чітко. У більшості випадків несанкціонований доступ здійснюється подоланням захисту комп'ютерної системи на рівні операційної системи, що дозволяє отримати доступ до файлів СУБД за допомогою засобів операційної системи. Проте у разі, якщо використовується СУБД, що не має досить надійних захисних механізмів, то стає цілком вірогідним подолання захисту, що реалізовується на рівні СУБД.

2.5.2 Атаки на рівні операційної системи

Захищати операційну систему, на відміну від СУБД, набагато складніше. Річ у тому, що внутрішня структура сучасних операційних систем надзвичайно складна, і тому дотримання адекватної політики безпеки є значно важчим завданням.

Можливості несанкціонованого доступу на практиці значною мірою залежать від архітектури і конфігурації конкретної операційної системи.

Проте є методи несанкціонованого доступу, які застосовні практично до будь-яких операційних систем:

- крадіжка пароля шляхом підглядання за користувачем, коли той вводить пароль;
- отримання пароля з файлу, в якому пароль був збережений користувачем;
- крадіжка зовнішнього носія пароліної інформації;
- сканування жорстких дисків комп'ютера;
- зборка комп'ютерного «сміття» в цілях відновлення раніше видалені об'єктів;
- перевищення повноважень шляхом використання помилок в програмному забезпеченні або в адмініструванні операційної системи;
- часткове або повне виведення із ладу операційної системи.

2.5.3 Атаки на рівні мережевого програмного забезпечення

Мережеве програмне забезпечення є найуразливішим, тому що канал зв'язку, по якому передаються повідомлення, найчастіше не захищений, і всякий, хто може мати доступ до цього каналу, відповідно може перехоплювати повідомлення і відправляти свої власні. Тому на рівні мережевого програмного забезпечення можливі наступні методи несанкціонованого доступу:

- прослуховування сегменту локальної мережі;

- перехоплення повідомлень на маршрутизаторі;
- створення неправдивого маршрутизатора;
- нав'язування повідомлень, коли відправляючи в мережу сполучення з неправдивою зворотною мережевою адресою, зломисник перемикає на свій комп'ютер вже встановлені мережеві з'єднання і в результаті отримує права користувачів;
- відмова в обслуговуванні, коли при відправленні в мережу повідомлення спеціального виду комп'ютерні системи, які підключені до мережі, повністю або частково виходять з ладу.

Для протидії вказаним методам доступу слідують максимально захистити канали зв'язку і тим самим ускладнити обмін інформацією по мережі для тих, хто не є легальним користувачем.

2.5.4 Програмні закладки

Програмна закладка – недокументований модуль, що впроваджується в загальносистемні програмні засоби, застосовні програми і апаратні засоби інформаційних і телекомунікаційних систем.

Існують три основні групи деструктивних дій, які можуть здійснюватися програмними закладками:

- копіювання інформації користувача комп'ютерної системи (паролів, криптографічних ключів, кодів доступу, конфіденційних електронних документів), що знаходяться в оперативній або зовнішній пам'яті цієї системи або в пам'яті іншої комп'ютерної системи;
- зміна алгоритмів функціонування системних, прикладних і службових програм;
- нав'язування певних режимів роботи, наприклад, блокування запису на диск при видаленні інформації, коли інформація, яку вимагається видалити, не знищується і може бути згодом скопійована.

2.6. Технічні канали просочування інформації, що виникає при роботі обчислювальної техніки за рахунок ПЕМВН

Стабільність надходження відомостей, неявна, прихована від власника, форма знімання інформації, що обробляється технічними засобами, зумовили неослабний інтерес до каналу витoku, який виникає за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН), супроводжуючих роботу цієї апаратури.

При виявленні технічних каналів просочування інформації засіб обчислювальної техніки необхідно розглядати як систему, що включає основне устаткування, кінцеві пристрої, з'єднувальні лінії, систему електроживлення, систему заземлення.

Технічні засоби, призначені для обробки конфіденційної інформації, разом з приміщеннями, в яких вони розміщуються, складають *захисний абонентський пункт (ЗАП)*.

Разом із ЗАП в приміщеннях встановлюються технічні засоби і системи, що безпосередньо не беруть участь в обробці конфіденційної інформації, але використовуються спільно із ЗАП і такі, що знаходяться в зоні його електромагнітного поля.

В якості каналу просочування інформації найбільший інтерес представляють допоміжні технічні засоби, що мають вихід за межі контрольованої зони. Такі дроти, кабелі і струмопровідні елементи можуть виявитися носіями закритої інформації.

Розглянемо характеристики каналів витоку, за рахунок ПЕМВН.

2.6.1 Класифікація каналів витоку інформаційних сигналів за рахунок ПЕМВН

Частотний діапазон побічних електромагнітних випромінювань, супроводжуваних інформативні сигнали, тягнеться від одиниць кГц до ГГц і вище і визначається тактовою частотою використовуваного засобу обробки інформації (ЗОІ). Так, для стандартного комп'ютерного монітора з електронно-променевою трубкою перехоплення інформації можливий на частотах аж до 50 гармоніки тактової частоти, а рівень випромінювання, що становить у ближній зоні величину до десятків дБ, дозволяє приймати сигнали на видаленні до декількох сотень метрів.

Залежно від середовища поширення інформативних сигналів розглядають два можливі канали витоку: *власне за рахунок ПЕМВН і комунікаційний*.

За способом утворення класифікують чотири типи каналів витоку:

- канал електромагнітного випромінювання (ЕМВ), що утворюється полями, які виникають при проходженні інформації по ланцюгах ЗОІ;

- канал випадкових антен (ВА), що виникає за рахунок наведених ЕРС в струмопровідних комунікаціях, гальванічно не

пов'язаних з ЗОІ і що мають вихід за межі контрольованої зони (КЗ);

- канал комунікацій, що відходять, гальванічно пов'язаних з ЗОІ;

- канал нерівномірного споживання струму (НСС), що утворюється за рахунок амплітудної модуляції струму спрацюванням елементів ЗОІ при обробці інформації.

Канал ЕМВ характеризується розміром ЕМВ – відстанню між ЗОІ і антенної апаратури перехоплення, за межами якої неможливий ефективний прийом внаслідок природного зниження рівня випромінюваного сигналу.

Канал випадкових антен характеризується розмірами їх зони для зосереджених випадкових антен (ЗВА) і розподілених випадкових антен (РВА). До зосереджених випадкових антен відносяться будь-які технічні засоби, що мають вихід за межі контрольованої зони. До розподілених випадкових антен відносять дроти, кабелі, елементи конструкцій будівлі і тому подібне. Відстань між ЗОІ і ВА, на якому неможливе ефективне перехоплення, визначає розмір зони ВА.

Канал комунікацій, що відходять, характеризується гранично допустимим значенням відношення потужностей інформативного сигналу і нормованої перешкоди, при якому неможливий ефективний прийом.

Канал нерівномірного споживання струму (НСС) характеризується гранично допустимим значенням відношення величини зміни струму, що поступає від джерела при обробці інформації, до середньої величини струму споживання. Якщо вказане відношення не перевищує граничного значення, ефективний прийом по каналу НСС неможливий. У сьогодення, з урахуванням практичної відсутності у складі засобів обчислювальної техніки (ЗОТ) низькошвидкісних пристроїв (діапазон частот цього каналу приймається 0...30 Гц), цей канал мало актуальний.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення, технічні канали просочування інформації можна розподілити на *електромагнітні* і *електричні*.

Окрім електромагнітних випромінювань навколо засобів обробки інформації є присутніми квазістатичні інформаційні електричні і магнітні поля, що викликають певні наведення на близько розташовані кабелі, телефонні дроти, лінії охоронно-пожежної

сигналізації, електромережі і тому подібне. Інтенсивність полів в діапазоні частот від одиниць кГц до десятків МГц така, що прийом сигналів може вестися за межами контрольованої зони (КЗ) при безпосередньому підключенні до цих ліній передачі.

До електромагнітних каналів просочування інформації відносяться:

- випромінювання елементів засобів обчислювальної техніки;
- випромінювання на частотах роботи високочастотних генераторів обчислювальної техніки, що модулюються інформаційними сигналами;
- випромінювання на частотах самозбудження засобів обчислювальної техніки.

Основні закономірності і властивості електромагнітного поля описуються системою рівнянь Максвелла. Фізична суть цієї системи рівнянь полягає в тому, що змінний струм в провіднику породжує змінне електромагнітне поле в навколишньому просторі. І навпаки – змінне електромагнітне поле наводить в провідниках, що знаходяться в цьому полі, змінний струм тієї ж частоти.

Тому усі провідники, що сполучають між собою складові частини комп'ютера і мережі, система електроживлення і заземлення являють собою антени, здатні випромінювати або перевипромінювати електромагнітні хвилі.

Рівень наведеного в провідниках сигналу залежить від таких чинників:

- інтенсивності випромінювання технічного засобу, відстані від нього до межі контрольованої зони, а також від довжини струмоведучого ланцюга і частоти;
- просочування інформаційних сигналів в ланцюзі електроживлення і заземлення. Ці сигнали обумовлені як власним електромагнітним полем обчислювальної техніки, так і просочуванням інформаційних сигналів через блок живлення;
- нерівномірності споживання струму в мережі електроживлення.

Простір навколо засобу обчислювальної техніки, в межах якого на випадкових антенах наводиться інформаційний сигнал вище за допустимий рівень, називається *зоною r1*. А випадкові антени можуть бути як зосередженими, так і розподіленими.

Просочування інформаційних сигналів в мережу

електроживлення можливе за наявності реакції блоку живлення на роботу пристроїв з інформаційними сигналами.

Просочування інформаційних сигналів в ланцюзі заземлення об'єкту можливо при роботі локальної обчислювальної мережі по кабелях при значній їх протяжності.

З урахуванням викладеного можна сформулювати критерій захищеності ЗОІ від витоку через ПЕМВН: ЗОІ вважається захищеним, якщо:

- радіус зони електромагнітних випромінювань не перевищує мінімально допустимої відстані від ЗОІ до межі КЗ;
- відношення потужностей інформативного сигналу нормованої перешкоди в усіх ВА не перевищує на межі КЗ гранично допустиму величину;
- відношення потужностей інформативного сигналу нормованої перешкоди в усіх комунікаціях, що відходять, на межі КЗ не перевищує гранично допустиму величину;
- відношення величини зміни струму «обробки» до середньої величини струму споживання від електромережі на межі КЗ не перевищує граничне допустиме значення m .

2.6.2 Критерії захищеності ЗОТ

Критерієм оцінки захищеності об'єкту обчислювальної техніки є умова: якщо для облаштування ЗОТ відношення сигнал/перешкода (Δ) на виході приймального облаштування перехоплення секретної інформації не перевищує гранично допустимого значення δ в усіх можливих каналах витоку, тобто

$$\delta \geq \Delta = U_{c.nik} / U_{пш.эф} , \quad (2.1)$$

то пристрій захищений від витоку. Об'єкт вважається захищеним в цілому, якщо захищений кожен пристрій.

Виміряне відношення небезпечний сигнал/перешкода (Δ) – відношення амплітуди імпульсного сигналу до середньоквадратичної напруги перешкоди на виході приймального пристрою.

Для об'єктів категорії 1 - це оптимальний приймач імпульсних сигналів з повністю відомими параметрами на прийомі, що забезпечує мінімальну вірогідність помилки. Для об'єктів категорії 2 і 3 –

перебудований погоджений фільтр з оптимальною смугою пропускання Δf , що лежить в межах

$$f_T < \Delta f < \frac{1}{\tau}, \quad (2.2)$$

де f_T – тактова частота сигналу, τ – тривалість імпульсу.

Норми на відношення небезпечного сигналу до шуму (перешкоді) (відносяться до послідовних і паралельних кодам, а також враховують багатократне повторення інформації. Випромінювання одного розряду – це таке випромінювання, яке характерне для цього розряду у відсутності випромінювань інших розрядів машинного осередку і яких-небудь інших випромінювань. Якщо виміряно сумарне випромінювання великого числа розрядів (але не більше 8), то необхідно зробити розрахунок енергії на один розряд. Паралельні коди розрядністю більше 8 вважаються безпечними.

Якщо виміряно сумарне випромінювання декількох розрядів (але не більше 8), то необхідно зробити нормування цього випромінювання на один розряд шляхом ділення його на експериментально визначений коефіцієнт, еквівалентний умовному числу розрядів в кодї, або на $n/2$, де n - число розрядів.

При регулярних повтореннях сигналу норма гранично допустимого відношення сигнал/перешкода (δ_{Π}) визначається за формулою:

$$\delta_{\Pi} = \delta / \sqrt{K_{\Pi}}, \quad (2.3)$$

де K_{Π} - число повторень.

Граничне допустиме відношення сигнал/перешкода (δ_H) для каналу просочування інформації за рахунок нерівномірності споживання струму мережі електроживлення визначається по формулі:

$$\delta_H = \delta \cdot K_H, \quad (2.4)$$

де K_H - коефіцієнт, що враховує обмеження пропускної спроможності цього каналу витоку по відношенню до швидкості роботи $S_{\text{Бод}}$ джерела небезпечного сигналу і змінюється від 1 до 10 при зміні $S_{\text{Бод}}$ від 50 до 1200. Для швидкості понад 1200 бод вказаний параметр не нормується.

З АКУСТИЧНІ І ВІБРОАКУСТИЧНІ КАНАЛИ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ З ОБ'ЄМІВ ВИДІЛЕНИХ ПРИМІЩЕНЬ

3.1 Основні поняття, визначення і одиниці вимірювань в акустиці

Звукові хвилі являють собою малі механічні коливання в твердих, рідких і газоподібних середовищах з частотами від 20 Гц до 20 кГц. Частоти, нижче 20 Гц називаються інфразвуковими, а вище 20 кГц - ультразвуковими.

Процес поширення коливального руху в середовищі називається звуковою хвилею. За один повний період коливання T звуковий процес поширюється в середовищі на відстань, рівну довжині хвилі λ (рис. 3.1).

$$f = \frac{1}{T} \text{ (Гц)}, \quad \lambda = c \cdot T \text{ (м)}, \quad (3.1)$$

де c – швидкість поширення звуку в середовищі.

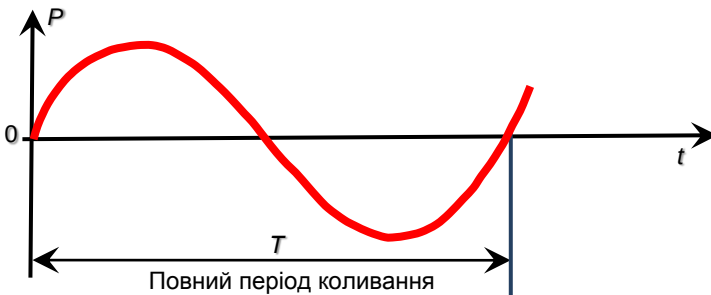


Рисунок 3.1 – Повний період коливання

Швидкість пружних хвиль в рідинах і подовжніх хвиль в твердих тілах перевищує швидкість звуку в газах і залежить від пружності (стисливості) і щільності середовища (табл.3.1).

Зміни тиску в звуковій хвилі відносно середнього значення називається звуковим тиском P і вимірюється в Паскалях. Один

Паскаль цей тиск, що створюється силою в один Ньютон, діючою на площу один квадратний метр.

$$P = \frac{1\text{Н}}{1\text{м}^2} = 1 \text{ (Па)} = \frac{1}{100000} \text{ (АТМ)}. \quad (3.2)$$

Таблиця 3.1. Швидкість поширення звуку в середовищі залежить від її щільності ρ .

Середовище поширення	$\rho, \text{кг}/\text{м}^3$	$c, \text{м}/\text{сек}$
Повітря	1.3	331
Спирт	790	1440
Алюміній	2650	6220
Мідь	8930	4620
Стекло	2500	4900...5900
Вода	1000	1450
Сталь	7800	6110
Цеглина	2 100	2 250
Бетон	2 400	3 600

У акустиці прийнято використання відносних одиниць вимірювання рівня звукового тиску - децибел.

$$L_{\text{дБ}} = 20 \lg \frac{P}{P_0} \quad (3.3)$$

У якості P_0 вибрана величина $P=P_0=2 \cdot 10^{-5}$ Па, що відповідає мінімальному звуковому тиску, що сприймається людським слухом. Зміна рівня звукового тиску на 1 дБ є мінімальною, розрізною людським слухом величиною зміни гучності.

Слід зазначити, що в акустиці при частотному аналізі сигналів використовують стандартизовані частотні смуги шириною в 1 октаву, 1/3 октави, 1/12 октав. Октава – це смуга частот, у якій верхня гранична частота в два рази більше нижньої граничної частоти

$$\Delta f = (f_{\text{В}} - f_{\text{Н}}) = 1 \text{ окт, якщо } f_{\text{В}} = 2 f_{\text{Н}}. \quad (3.4)$$

Центральні частоти стандартних октавних смуг відповідають наступному ряду:

2, 4, 8, 16, 31,5, 63, 125, 250, 500 (Гц); 1, 2, 4, 8, 16 (кГц).

3.2 Основні акустичні параметри мовних сигналів

В силу різних механізмів утворення гласних і приголосних звуків мовний сигнал є складним частотно-амплітудним модульованим шумовим процесом, який характеризується наступними основними статистичними параметрами: *частотний діапазон*; *рівень мовних сигналів*; *динамічний діапазон*.

3.2.1 Частотний діапазон мови

Основна енергія акустичних коливань мовного сигналу знаходиться в діапазоні 70 Гц ÷ 7 кГц, причому більше 95% смислової інформації розміщується у вузкому діапазоні – 200 Гц ÷ 5 кГц. Акустичні коливання вище і нижче цих частот несуть інформацію про емоції і особу того, хто говорить (усний почерк), сприяє впізнаності і декілька підвищують розбірливість мови в умовах підвищених шумів.

На рис. 3.2, крива 1 характеризує вид середньостатистичного спектру української мови.

Важливо відмітити, що інформативна насиченість окремих ділянок спектру мови нерівномірна. Крива 2 на рис 3.2 показує вклад окремих ділянок спектру мови в сумарну розбірливість.

3.2.2 Рівні мовних сигналів

В різних умовах людина обмінюється усною інформацією з різним рівнем гучності, при цьому створюються наступні рівні звукового тиску :

- тихий шепіт 35 ... 40 дБ;
- спокійна бесіда 55 ... 60дБ;
- виступ в аудиторії
без засобів звукопідсилення 65 ... 70 дБ.

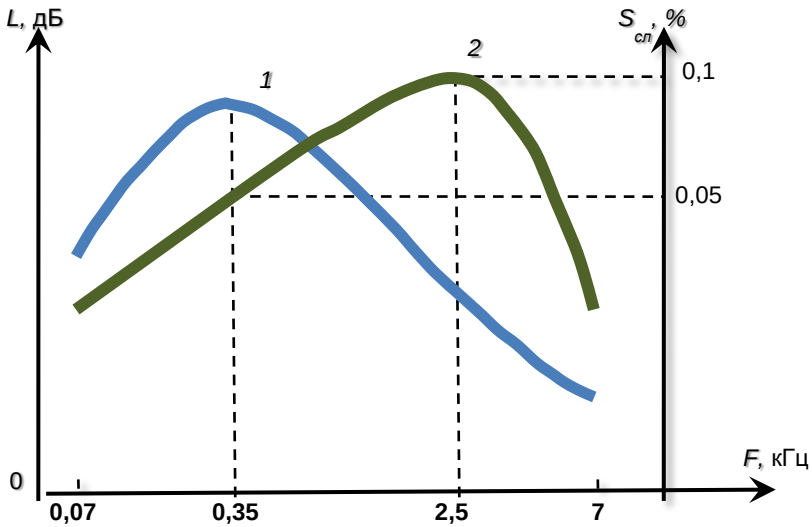


Рисунок 3.2 – Середньостатистичний спектр української мови

3.2.3 Динамічний діапазон

Динамічні характеристики розмовної мови дуже різні і багато в чому залежать від зовнішніх умов, в яких знаходиться той, хто говорить. Так, спокійна, довірча розмова, що ведеться співрозмовниками, які знаходяться поруч один з одним, відбувається зазвичай з рівнем близько 55 дБ (звуковий тиск); виступ в залі, а нерідко і розмова по телефону - близько 75 дБ. При цьому динамічний діапазон мови також міняється в досить широких межах 25÷45 дБ.

Рівень мови в процесі озвучування одного повідомлення може мінятися в значних межах. Різниця між квазімаксимальними і квазімінімальними рівнями для різних видів мови складає:

- дикторська мова 25 ... 35 дБ;
- телефонні переговори 35 ... 45 дБ;
- драматична мова 45 ... 55 дБ.

3.2.4 Сприйняття мови

При вимовленні звуків мови через мовний тракт, що є складним

акустичним фільтром з рядом резонаторів, які створюються порожнинами рота, носа і носоглотки, проходить або тональний імпульсний сигнал (дзвінки звуку), або шумовий (глухі звуки), або той і інший разом. Внаслідок цього рівномірний тональний або шумовий спектр перетворюється на спектр з рядом максимумів, що називаються *формантами*, і мінімумів, що називаються *антиформантами*. Оскільки найбільш інформативними є глухі приголосні, то при дії шумів розбірливість мови знижується, в першу чергу, із-за маскування глухих звуків. Вухом людини має властивості дискретного сприйняття по частотному і динамічному діапазонам. Слухове відчуття пропорційно логарифму дратівливої сили:

$$E = 10 \log \left(\frac{I}{I_{\text{п.ч}}} \right), \text{ (дБ)}. \quad (3.5)$$

де $I_{\text{п.ч}}$ - дратівлива сила на порозі чутності.

Величину E називають *рівнем відчуття*, причому $E = I_1 - I_{\text{п.ч.}}$, де $I_1 = 10 \lg I + 120$ - рівень інтенсивності звуку I , Вт/м². Рівень відчуття, представляючи собою рівень над порогом чутності, неточно характеризує суб'єктивне відчуття, тому в акустиці застосовується поняття рівня гучності звуку (або шуму), під яким розуміється рівень в децибелах рівногучного з ним чистого тону 1000 Гц.

Відповідно до кривих рівної гучності, рівень гучності на частоті 1000 Гц на 6 дБ вище за гучність в діапазоні частот 250...500 Гц, тому при прийомі елементів мови технічними засобами це зниження можна компенсувати частотною корекцією, що неможливо здійснити при прийомі мови людиною. Сприйняття мови значною мірою залежить від рівня акустичних шумів, які викликаються численними джерелами - як зовнішніми, що знаходяться за межами приміщень, так і внутрішніми.

Найбільший маскуючий ефект мають широкосмугові перешкоди з "гладким" спектром, але задовільна розбірливість мови може бути досягнута навіть у тому випадку, якщо рівень мови буде на декілька децибел нижче рівня шуму.

Вузькосмугові перешкоди навіть високого рівня не можуть забезпечити необхідній мірі зашумлення мови, оскільки вони, можуть бути істотно компенсовані за допомогою різних фільтрів.

3.2.5 Розбірливість і зрозумілість мови

Розбірливістю називають відносну або процентну кількість прийнятих спеціально тренованими слухачами (артикулянтами) елементів мови із загальної кількості переданих по тракту. Оскільки в якості елементів мови застосовують звуки, склади, слова і фрази, то має місце звукова, складова, словесна і фразова розбірливість. Усі вони при випробуванні однієї і тієї ж системи виражатимуться різними чисельними величинами, оскільки відсоток правильних оцінок для передбаченого правильного повідомлення завжди вищий, ніж для непередбаченого, міра ж передбачення при прослуховуванні фрази вища, ніж при слуханні окремих слів або складів. Проте усі види розбірливості пов'язані один з одним з однозначними функціональними залежностями, що представляються зазвичай у вигляді кривих або таблиць.

Об'єктивні вимірювальні оцінки розбірливості мови можуть робитися за допомогою обчислення розбірливості формант.

По формантній розбірливості визначають складову, словесну, фразову розбірливість і зрозумілість мови.

Зрозумілість мови, будучи фонетичною характеристикою розбірливості, визначається в процесі звичайних телефонних переговорів для не тренованих спеціально абонентів. При цьому зрозумілість вважається: *відмінною*, якщо переговори ведуться без перезапитувань; *доброю*, якщо бувають окремі перезапитування слів, які рідко зустрічаються, або невідомих прізвищ, назв і тому подібне, про яких не можна здогадатися за змістом; *задовільною*, якщо потрібні часті перезапитування і слухачі повідомляють, що важко розмовляти; *гранично допустимою*, якщо потрібні неодноразові перезапитування одного і того ж матеріалу, в передачі окремих слів по буквах з повною напругою слухачів.

Враховуючи, що сприйняття людиною формант має властивість аддитивності, тобто кожна ділянка мовного діапазону вносить свій вклад в загальну розбірливість мови, можна розрахувати вклади октавних смуг для формантної розбірливості.

Від якісного прийому кожної частотної смуги залежить сумарна розбірливість. Мінімальна формантна розбірливість, при якій ще можливе розуміння змісту мовного повідомлення (сумарна вірогідність прийому формант) рівна 15%, що відповідає 25% складовою і 75% словесної розбірливості.

Відомо, що на розбірливість мовних повідомлень робить вплив ефект реверберації, що характеризується часом зменшення рівня звукового тиску в приміщенні на 60 дБ після виключення джерела.

Розбірливість мови. Якість мови оцінюється її розбірливістю, що є статистичною характеристикою мови, що приймається на тлі шумів. Розбірливість – це відношення числа правильно зрозумілих елементів мови (звуків, складів, слів) до загального числа переданих по каналу елементів. Вона може характеризувати якість каналу тільки в середньому значенні, допускаючи флуктуації в той або інший бік. Розбірливість мови визначається експериментально за допомогою так званих *випробувань артикуляції*. Об'єктивні вимірювальні і розрахункові оцінки розбірливості мови можуть проводитися за допомогою обчислення розбірливості формант. Форманти – це максимуми поточного спектру розмови, які заповнюють увесь мовний діапазон. У акустичних вимірах використовуються октавні або третьоктавні частотні смуги. Для октавного аналізу вклади частот української мови дорівнюють значенням, приведеним в таблиці 3.2.

Таблиця 3.2. Вклади частот української мови для октавного аналізу

Частотна смуга, кГц	0,25	0,5	1	2	4	8
Розбірливість формант, %	6,7	12,5	21,2	29,4	25	5,2

Від якісного прийому (без спотворень і перешкод) кожної частотної смуги залежить сумарна розбірливість. Граничне значення розбірливості формант, при якій можливе розуміння змісту мовного повідомлення, дорівнює 15 %, що відповідає 25 %-ої розбірливості складів. Завдання оцінки каналу витоку зводиться до вимірювання або обчислення розбірливості мови і порівняння отриманого значення з граничним.

Реверберація звуку. Окрім послаблення мовних сигналів на розбірливість робить вплив ефект реверберації в приміщеннях, який проявляється в накладенні мовних відрізків один на одного за рахунок перевідбиття сигналу від поверхонь конструкцій. Міра запаздывання мовних сигналів залежить від обробки приміщення: якщо воно має звукопоглинальну поверхню, то час реверберації незначний, В гучних приміщеннях воно може істотно спотворити мову. Час реверберації

менше 0,85 з непомітно для слуху.

Для більшості кабінетів і приміщень їх об'єми і акустична обробка дозволяють не враховувати тимчасові спотворення, оскільки час реверберації в середньому дорівнює 0,2 ... 0,6 с. Істотні ревербераційні спотворення у вібраційних каналах, особливо в трубопроводах, в яких вони знижують розбірливість на 15... 20 %.

Прогнозована розрахункова розбірливість. Усереднені дані очікуваних значень розбірливості розмови, отримані розрахунковим шляхом і підтверджені експериментально при оцінці якості віброакустичних каналів просочування мовної інформації на типових будівельних конструкціях, приведені в таблиці 3.3. Для мінімальних перешкод рівень розрахункової розбірливості близький до 25 % складової.

Таблиця 3.3. Звукоізоляція основних будівельних конструкцій, дБ

Тип будівельної конструкції	Центральні частоти октавних смуг, Гц				
	250	500	1000	2000	4000
Обштукатурена цегляна стіна завтовшки 270 мм	44	51	58	64	65
Залізобетонна стіна завтовшки 100 мм	40	44	50	55	60
Гіпсобетонна перегородка завтовшки 80 мм	33	37	39	44	44
Перегородка ДСП завтовшки 20 мм	26	26	26	26	26

3.3 Поширення акустичних сигналів в приміщеннях і будівельних конструкціях

Акустичні коливання, що поширюються в приміщенні, падають на конструкції, які захищають, в основному відбиваються від них, а частково взаємодіють з ними, викликаючи відповідні коливання конструкцій, і поширюються далі у вигляді вібраційних коливань.

Кількість акустичної енергії, що пройшла з одного середовища в інше, залежить від співвідношення їх щільності або акустичних опорів

(рис. 3.3).

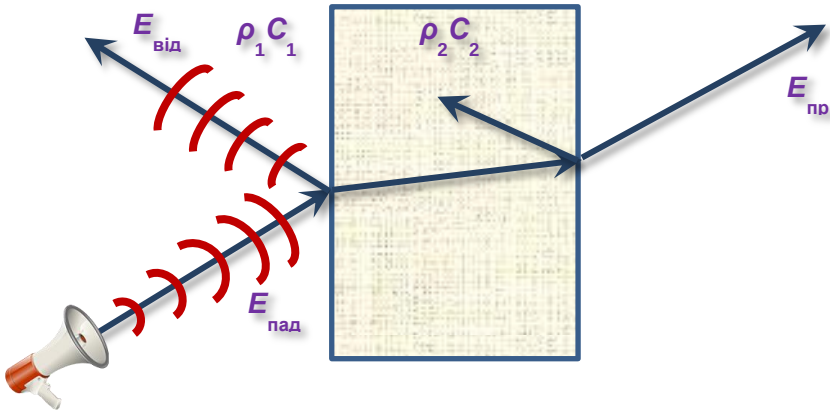


Рисунок 3.3 – Кількість акустичної енергії, що пройшла з одного середовища в інше.

Де ρ_i - щільність i -того середовища

C_i - швидкість звуку в i -тому середовищу.

У будівельній акустиці використовуються наступні основні поняття:

– коефіцієнт поглинання

$$\alpha = \frac{E_{\text{пад}} - E_{\text{від}}}{E_{\text{пад}}}; \quad (3.6)$$

– коефіцієнт відображення

$$\beta = \frac{E_{\text{від}}}{E_{\text{пад}}}; \quad (3.7)$$

– коефіцієнт звукопроникності

$$\gamma = \frac{E_{\text{пр}}}{E_{\text{пад}}}; \quad (3.8)$$

– звукоізоляція

$$Q = 10 \lg \frac{E_{\text{пад}}}{E_{\text{пр}}} . \quad (3.9)$$

3.4 Канали просочування мовної інформації

На рис. 3.4 представлені основні варіанти можливого просочування мовної інформації з об'ємів виділених приміщень. Усі їх можна об'єднати в дві групи - це акустичні канали (позначені буквами *a, б, в*), тобто такі канали, по яких інформація може бути перехоплена за допомогою звичайних мікрофонів або прослухана безпосередньо людиною, а також віброакустичні канали (позначені буквами *г, д, е*), в яких інформація може бути зафіксована за допомогою стетоскопів а також віброметрів, велосиметрів, акселерометрів.

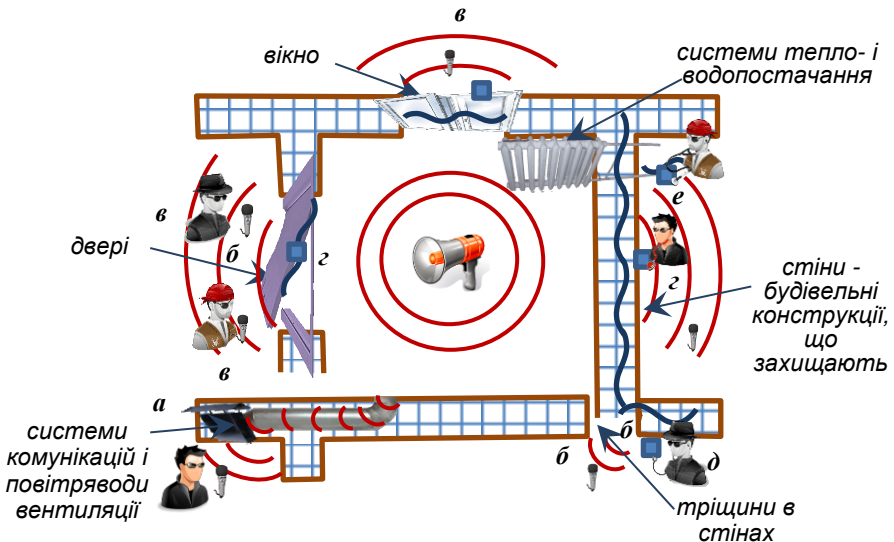


Рисунок 3.4 – Можливі канали просочування мовної інформації

Найбільшу небезпеку представляють технологічні вікна і канали з великою площиною поперечного перерізу, такі як короби комунікацій і повітряводи вентиляції. Ці об'єкти є по суті акустичними хвилеводами, і звукові коливання можуть поширюватися

по них на значні відстані. Так якщо поперечні розміри короба порівнянні з довжиною звукових хвиль $L \approx \lambda$, то загасання при поширенні по ньому звуку складає $\delta = 0,01 \dots 1$ дБ/м і залежить від розмірів короба, матеріалу стінок і ін.

Нагадаємо, що $\lambda_i = C_i / f = C_i T$.

Наступними по мірі небезпеки є звуководи з розмірами, меншими довжини звукових хвиль $L \ll \lambda$. Такими можуть бути отвори електропроводки, щілини і тріщини у будівельних конструкціях, нещільності дверних і віконних отворів. Загасання звуку в таких каналах дуже значне $\delta = 1 \dots 20$ дБ/м. Воно визначається в'язкістю повітря і залежить від поперечних розмірів отворів, шорсткості поверхні і поздовжньої конфігурації отвору.

Незважаючи на значні величини загасання, цього абсолютно недостатньо для забезпечення захисту інформації. Так, якщо в стіні товщиною 0,5 м є тріщина з площею поперечного перерізу 5 мм^2 при довжині 0,75 м, звукоізоляція в області виходу цієї тріщини на поверхню складатиме 18 дБ, тоді як за відсутності тріщини така стіна забезпечує звукоізоляцію більше 65 дБ.

Звукові коливання можуть поширюватися за межі виділеного приміщення не лише за рахунок тих або інших повітряних каналів, але і за рахунок перевипромінювання коливань будівельними конструкціями, що захищають.

3.5 Віброакустичні канали

Будівельні конструкції здійснюють деякі коливання під впливом акустичних хвиль. Щоб перехопити інформацію, перенесену цими коливаннями, не обов'язково реєструвати акустичні коливання, конструкціями, які перевипромінюють. Для цього зручніше зафіксувати коливання власне будівельних конструкцій. Так, наприклад, під впливом звуку $P_{\text{ак}} = 70$ дБ цегляна стіна завтовшки 0,5 м здійснює вібраційні коливання з прискоренням $a \approx 3 \cdot 10^{-5} g$. За таких умов сучасними засобами може бути прослуханий навіть шепіт. Але перевипромінений акустичний сигнал буде $P_{\text{ак.пр}} < 10$ дБ, що практично унеможливорює знімання інформації. Таким чином, вібраційні коливання конструкцій, що захищають, під впливом звукових хвиль утворюють один з найбільш небезпечних каналів

просочування інформації – віброакустичний.

Висока щільність будівельних конструкцій забезпечує можливість поширення коливань на значні відстані. Це створює можливість перехоплення інформації, шляхом реєстрації вібрацій не лише конструкцій виділеного приміщення, що захищають, але і реєструючи коливання видалених на 1-3 стики елементів будівлі. Так створюється реальна можливість перехоплення інформації по стіні, що несе, з виділеного приміщення, розташованого через 1–2 поверхи від місця установки апаратури знімання інформації.

Залежно від конструкції будівлі і якості виконання стиків між його елементами, загасання на стиках варіюється в межах від 1 до 15 дБ.

Деякі елементи будівельних конструкцій, як і у разі розгляду акустичного каналу, є хвилеводи вібраційних коливань. До них відносяться труби різних комунікацій (опалювання, водопостачання, електроживлення і ін.).

Внаслідок добротності більшості будівельних матеріалів, вібраційні коливання, викликані мовним сигналом, можуть бути прийняті на значному видаленні від місця проведення розмови. В зв'язку з цим слід зазначити два важливі аспекти. По-перше, ступень проникнення акустичної енергії з повітряного середовища в тверде тіло залежить від співвідношення акустичних опорів цих середовищ:

$$N \approx \frac{\rho_1 \cdot C_1}{\rho_2 \cdot C_2}. \quad (3.10)$$

де: ρ_1 і ρ_2 - щільність матеріалу будівельної конструкції і повітря;

C_1 і C_2 - швидкості звуку в матеріалі будівельної конструкції і повітрі.

Наприклад співвідношення N для сталі і бетону складає 5.8.

Це положення має просте і практично важливе слідство, яке дістало у будівельній акустиці назву "Закон маси", – чим більше маса одиниці площі конструкції, тим менше вібраційні коливання, викликані звуком, або, простіше кажучи, чим товще стіна, тим вище звукоізоляція. Високі акустичні характеристики будівельних конструкцій створюють хороші умови для поширення вібрацій, викликаних іншими джерелами, такими як вуличні шуми, протікання води в системах опалювання, кроки, хлопання дверей, робота побутової апаратури і т.д., що створює при прийомі мовної

інформації, яка поширюється по будівельних конструкціях, комплекс так званих структурних перешкод.

Віброакустичний канал стає особливо небезпечним, якщо трубопровід сполучений з якоюсь жорсткою і розвиненою поверхнею, яка грає роль погоджувального елементу, при передачі енергії з повітря в трубопровід. Такими погоджувальними елементами, наприклад, є радіатори опалювання.

Слід зазначити, що спектри структурних перешкод мають, як правило, характер, що спадає у бік високих частот, і близькі до спектрів вібрацій мовних сигналів.

Рівень структурних перешкод у будівлі і величина звукоізоляції виділеного приміщення є основними чинниками, що визначають можливість перехоплення інформації по віброакустичному каналу.

Якщо архітектурно-будівельними методами забезпечити необхідну звукоізоляцію не вдалося, доцільно застосувати штучні джерела перешкод – *системи віброакустичного зашумлення*.

3.6. Акустичне підслуховування – пасивний спосіб добування інформації

Метод знімання інформації по віброакустичному каналу відноситься до так званих беззаходових методів, і це є важливою його перевагою. Виявити апаратуру такого знімання інформації украй важко, оскільки вона встановлюється за межами контрольованого приміщення, а у ряді випадків істотно віддалена від нього.

Коротко про фізичний принцип, який лежить в основі цього методу. Мова, що викликає акустичні сигнали, є механічними коливаннями повітряного середовища. Потрапляючи на тверді поверхні (стіни, перегородки), вони перетворюються в структурні вібраційні сигнали, які, залишаючись за своєю природою механічними, поширюються по будівельних конструкціях будівель. На рис. 3.5 схематично показані можливі шляхи витоку акустичних і вібраційних сигналів з приміщення. Можна виділити наступні типові конструкції, по яких передаються мовні сигнали:

у акустичному каналі – це стіни будівель, перегородки, перекриття будівель, вікна, дверей, що несуть, вентиляційні повітряводи;

у вібраційному каналі – це стіни і перегородки, перекриття,

віконні рами, дверні коробки, трубопроводи, короби вентиляції.

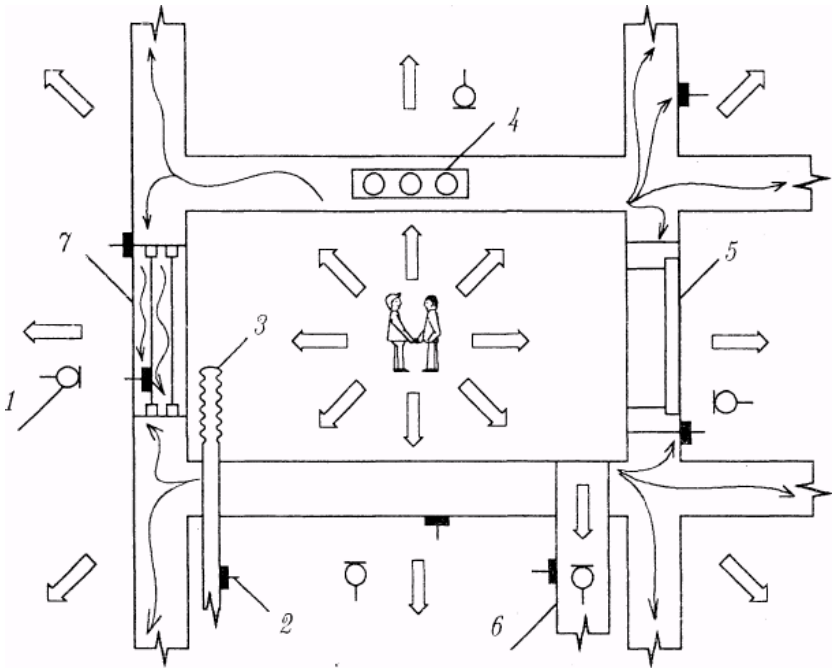


Рисунок. 3.5 Схема акустичних і вібраційних каналів витоку:

1 – мікрофон підслуховування; 2 – вібродатчик підслуховування; 3 – батарея опалювання; 4 – порожнина для кабелів; 5 – двері; 6 – повітряна вентиляція; 7 – вікно;
 ———> – поширення вібраційних коливань; ———> – поширення акустичних коливань.

Якщо акустичні і вібраційні датчики встановлені на цих конструкціях за межами приміщення, це дає можливість прийняти мовні сигнали і проконтролювати розмови усередині нього. При цьому необов'язково потайно проникати в приміщення – достатньо наблизитися до нього зовні. Встановити датчик можна і дистанційним способом – за допомогою спеціальних вистрілюючих пристроїв (наприклад на віконну раму). Іноді використовують лазерні пристрої і спрямовані мікрофони. Дія лазерних пристроїв заснована на принципі зняття вібрацій (мовних сигналів) з шибки, а спрямовані мікрофони знімають мовну інформацію по акустичному каналу (наприклад через відкриті вікна або фрамуги).

Зловмисник вибирає канал прослуховування і тактику дій,

виходячи з виду об'єкту і обстановки навколо нього. Можна вибрати три види об'єктів:

- об'єкт прослуховування є приміщенням у будівлі, зайнятій декількома організаціями. Ця ситуація зустрічається найбільш часто, і звичайними каналами прослуховування при цьому є повітряводи вентиляційної системи, загальної для всієї будівлі, перегородки і перекриття, трубопроводи опалювання і водопостачання;

- об'єкт знаходиться в окремій будівлі, до якої є вільний доступ. Ця ситуація характерна для приміщень, розташованих на нижніх поверхах за відсутності своєї території, що охороняється, хоч би з невеликою (5 ... 10 метрів) зоною контролю. У таких випадках вразливими місцями вважаються віконні рами, виходи вентиляційних отворів, віконні кондиціонери;

- об'єкт – будівля з територією, що охороняється.

В цьому випадку ефективно буде застосування дистанційних методів контролю. Тактика їх використання буде вибрана залежно від розташування приміщення (будівлі) і будов, що оточують його, рослинності і тому подібне, наявність навколо об'єкту місць, з яких можуть потайно використати лазерні засоби, спрямовані мікрофони або доставки віброзакладинок, з пристроїв, що вистрілюють.

Іншим важливим критерієм вибору є те, яка якість інформації може забезпечити використовуваний канал. Для його оцінки застосовується така характеристика, як розбірливість мови. Раніше був розглянутий такий параметр як розбірливість мови. Він залежить від трьох чинників: послаблення мови в каналі, рівня вібраційних і акустичних шумів в місцях установки датчиків і чутливості самих датчиків. Оперативна оцінка цих чинників ускладнюється тим, що вібраційні і акустичні сигнали не піддаються точному розрахунку.

Практично якість каналів знімання оцінюють експериментальним шляхом – за допомогою акустичних вимірювань, що імітують ситуацію контролю інформації.

Послаблення звукових коливань. Найбільш суттєвим для розбірливості є те, що при проходженні мовних сигналів по каналах витоку і будівельних конструкціях вони слабшають залежно від характеру ізоляції і міри поглинання. Для різних конструкцій і каналів витоку звуко- і віброізоляція може мати значення, що відрізняються на 5 ... 10 дБ навіть для конструкцій одного виду. Це залежить не лише від параметрів самих конструкцій (маси, товщини), але і від

якості їх установки, монтажу і обробки.

Рівень мовного сигналу залежить від об'єму і акустичної обробки приміщення, проте для більшості кабінетів в середньому він дорівнює 65 ... 70 дБ, залишаючись практично постійним за об'ємом приміщення (дифузне поле), за винятком зони поблизу людини (0,5...0,7 м), яка говорить.

При поширенні мовних акустичних сигналів по вентиляційним повітряводам вони слабшають із-за змін їх перерізу, поглинань в них і вигинів. Загасання в прямих металевих повітряводах складає 0,15 дБ/м, в неметалевих – 0,2...0,3 дБ/м. На вигинах загасання доходить до 3...7 дБ (на один вигин), при змінах перерізів 1...3 дБ.

Великі віброприскорення, що отримуються шибками утворюють канал витоку аудіоінформації, яка знімається із скла за допомогою лазерних мікрофонів.

Значення сигналу в трубопроводах на 10 ... 15 дБ вище, ніж на несних конструкціях.

Послаблення вібраційних сигналів істотно залежить від типу конструкції будівлі. Для залізобетонних будівель поглинання складає 0,1...0,15 дБ/м для цегляних 0,2...0,4 дБ/м.

Шуми і перешкоди, наявні в місці установки датчика, викликаються численними джерелами – автомобільним транспортом, роботою механічних машин, технічних засобів в приміщеннях, розмовами в суміжних приміщеннях і тому подібне. Характерна особливість шумів – їх не стаціонарність, тобто зміна рівня в часі. Ці зміни залежать від часу доби (увечері рівні шумів набагато менші, ніж вдень), від дня тижня (у вихідні дні рівні шумів знижуються), від погодних умов. Маскуючі властивості перешкод проявляються тим сильніше, чим більше їх перевищення над корисним сигналом в усій смузі частот мовного діапазону. Найбільший маскуючий ефект мають широкосмугові перешкоди з «гладким» спектром. Вузкосмугові ж перешкоди навіть високого рівня не можуть забезпечити необхідній мірі зашумлення мови. Вони можуть створюватися періодичними джерелами, наприклад двигунами. Періодичний характер перешкод дозволяє частково компенсувати їх за допомогою системи фільтрів, налаштованих на відповідні частоти, або адаптованими фільтрами.

Найбільші шуми – вуличні, які створюються автомобільним транспортом, листям (за наявності вітру), а також дворівні шуми. У будівлі джерелами шумів є люди (розмови, кроки), робота механізмів,

водопроводу, ліфта. Середні значення акустичних шумів на вулиці складають 60 ...75 дБ залежно від інтенсивності руху автомашин в районі розташування об'єкту. Різниця в рівні шумів від максимального до мінімального може складати до 30 дБ. Слід мати на увазі, що існуюча норма допустимого рівня акустичних шумів в робочих приміщеннях дорівнює 50 дБ. Цей рівень можна брати в якості розрахункового, якщо невідомі конкретні показники шумності в суміжних сторонніх приміщеннях.

Середні значення вібраційних шумів змінюються від 10...20 дБ на внутрішніх конструкціях вдень і до 15...30 дБ – вночі. На зовнішніх конструкціях шуми, як правило, на 5...10 дБ вище. На вікнах вібраційні перешкоди складають 10...15 дБ на внутрішньому склі, 25...30 дБ – на зовнішньому. У трубопроводах опалювання перешкоди змінюються від 10...15 дБ у відсутності води до 1.5...20 дБ – при її наявності. Усі приведені значення шумів дані для широкосмугових джерел перешкод.

Приймальні датчики. Найкращі з сучасних зразків датчиків для прийому мовних сигналів мають приведену чутливість: 15...30 дБ – мікрофони, 20...30 дБ – вібродатчики. Отже, такими датчиками можливий прийом акустичних і вібраційних сигналів при мінімальному рівні власних шумів. По-цьому в денний час для прийому сигналів в каналах витоку можуть використовуватися і датчики з меншою чутливістю, оскільки їх висока якість не буде реалізована повністю. У вечірній або нічний час в умовах з низькими шумами застосовуються тільки високочутливі датчики, які дозволяють з максимальним ефектом приймати слабкі видалені сигнали.

4 ЗНІМАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЗАКЛАДНИХ ПРИСТРОЇВ

Знімання інформації, що обробляється в ТЗПІ, можливе шляхом установки в них електронних облаштувань перехоплення – *закладних пристроїв*.

Знання конструктивних особливостей і схемних рішень побудови закладних пристроїв дозволяє виявити їх сильні і слабкі сторони і вибрати оптимальні способи протидії.

4.1 Побудова і загальні характеристики закладних пристроїв

Радіoeлектронні закладні пристрої є організованим каналом несанкціонованого отримання і передачі в пункт прийому аудіовізуальної або оброблюваної за допомогою радіoeлектронної апаратури і передаваної інформації в мережах зв'язку.

Закладні пристрої можна класифікувати за декількома ознаками:

- радіозакладні пристрої, випромінюючі в ефір;
- закладні пристрої, не випромінюючі в ефір (з передачею перехопленої інформації по мережах зв'язку, управління, живлення і так далі);
- радіозакладні пристрої з перевипромінюванням;
- закладні пристрої з передачею перехопленої інформації по стандартному телефонному каналу.

До першої групи входять радіозакладні пристрої, призначені для отримання аудіоінформації по акустиці приміщення, телевізійні закладні пристрої, призначені для отримання аудіо- і візуальної інформації, і радіозакладні пристрої в телефонних лініях зв'язку, облаштуваннях обробки і передачі інформації, мережах живлення і управління. Передача перехопленої інформації відбувається радіо- або телевізійним радіосигналом.

До закладних пристроїв з передачею інформації без випромінювання в ефір можна віднести групу закладних пристроїв в лініях зв'язку, живлення, управління і охоронної сигналізації з використанням цих ліній зв'язку для передачі перехопленої інформації.

У ряді закладних пристроїв передача перехопленої інформації

здійснюється по стандартному телефонному каналу. Це так звані закладки типу «довге вухо», «з штучно піднятою трубою».

Існує ціла група закладних пристроїв, що забезпечують отримання інформації по акустиці приміщення за рахунок модуляції акустичним сигналом відбитого мікрохвильового або ІЧ- сигналів від елементів, на які впливає акустичний сигнал. Це можуть бути: скло, вікна, різні перегородки, резонатори, спеціальні схеми і т.д.

Прояв розглянутих вище груп закладних пристроїв при їх передачі перехопленої інформації різняться, оскільки вони можуть проявлятися в радіодіапазоні, як радіовипромінювання з різними видами модуляції або кодування, в ІЧ- діапазоні як низькочастотні випромінювання в лініях зв'язку, управління, живлення, в стандартних телефонних каналах або у вигляді опромінюючих сигналів.

Залежно від призначення закладних облаштувань виділяється передусім «зона несанкціонованого отримання інформації». Це може бути повітряний простір (для повітряної акустичної хвилі), несні конструкції, труби водопровідної або парової мережі для структурної акустичної хвилі, елементи тракту обробки і передачі інформації і тому подібне.

4.1.1 Загальні характеристики закладних пристроїв

Виконання:

– у вигляді технічних модулів закамouflьованих під технічні елементи і пристрої, елементи одягу, побутові предмети.

Потужність випромінювання :

- мала - до 10 мВт;
- середня - від 10 до 100 мВт;
- велика - більше 100 мВт;
- з регульованою потужністю випромінювання.

Використовуваний вид модуляції :

- АМ, FM, TNFM, WFM
- з частотною мозаїкою;
- інверсія спектру;
- дельта-модуляція (адаптивна дельта-модуляція);
- шумоподібні сигнали.

По стабілізації частоти :

- нестабілізовані;
- із схемотехнічною стабілізацією частоти;

– з кварцовою стабілізацією.

Один з обмежуючих моментів використання закладних пристроїв – гарантована дальність перехоплення інформації. Ця дальність у ряді випадків є визначальною в організації пошуку закладних пристроїв. Стосовно закладних пристроїв, що забезпечують перехоплення аудіоінформації, важлива максимальна дальність перехоплення або повітрям, або структурною хвилею датчиками знімання подібної інформації. Як такі датчики використовуються мікрофони, стетоскопи або геофони. Можлива дальність перехоплення аудіоінформації, розмов, що передаються повітряною хвилею в межах 10 м, структурною хвилею - через цегляні і бетонні стіни - 0,8...1,0 м і сейсмічною хвилею - до 10 м при малих акустичних шумах (до 5 м при середніх акустичних шумах).

Установка закладних облаштувань перехоплення інформації з каналів обробки інформації або систем передачі даних і зв'язку визначається або місцем установки комплексу, або можливістю установки закладного пристрою на лінії зв'язку.

Наприклад, радіозакладний пристрій для перехоплення телефонних переговорів може бути встановлений в телефонній трубці, телефонному апараті, з'єднувальній коробці, розподільній телефонній коробці, на відрізках ліній, що сполучають ці пристрої, і так далі, аж до АТС. Місце встановлення комбінованої телефонної закладки (перехоплення телефонних переговорів і акустики приміщення) визначається зоною гарантованого перехоплення акустичної інформації з певного приміщення (як правило, близько 10 м від джерела, що цікавить).

4.1.2 Радіозакладні пристрої

Перехоплена інформація може бути передана по повітрю (радіозакладки), по мережах живлення, управління, зв'язку (закладні пристрої).

Для виявлення випромінюючих в ефір радіозакладок необхідно визначити можливий діапазон їх роботи і використовувати види модуляції і закриття. Як випливає з аналізу існуючих радіозакладних пристроїв, діапазон їх роботи досить широкий і має тенденцію до просування у більш високі діапазони, та до використання пристроїв з «стрибаючими» частотами.

Основні діапазони (по кількості відомих зразків): 270...480 МГц,

115...200 МГц, 75...115 МГц.

За останній час збільшилася кількість радіозакладних пристроїв, працюючих в діапазоні 640...1000 МГц і вище 1000 МГц.

Після введення обмежень на спеціальні технічні засоби для радіозакладних пристроїв виділений діапазон 415...420 МГц. Проте в експлуатації можна зустріти велику кількість раніше випущених пристроїв. Таким чином, радіозакладні пристрої можуть працювати в усьому діапазоні від 20 до 1000 МГц і вище.

Це істотно ускладнює завдання пошуку радіозакладних пристроїв по їх випромінюванню. Серйозне ускладнення в пошуку закладок викликають використовувані в закладних пристроях види модуляції і закриття, що змінюються і удосконалюються. Так, наприклад, широко поширені на початковому етапі радіозакладки будувалися з використанням амплітудної модуляції, що дозволяло використати в якості приймального облаштування комплексу звичайні побутові приймальні пристрої. Проте ця позитивна якість часто перетворювалася на негативну, оскільки перехоплена і передана в ефір інформація легко виявлялася тими, кому вона не призначалася. Так прокручувавши ручку свого побутового приймача, раптом в ефірі виявлялася розмова свого сусіда. Природно, що таке виявлення, як правило, призводило до подальшого знищення іноді з дуже великою працею встановлених закладних пристроїв.

У радіозакладних пристроях в основному застосовується модуляція несучої частоти передавача, проте зустрічаються радіозакладні пристрої з модуляцією сигналу проміжної частоти або подвійної модуляції (наприклад, радіозакладка РК-1970-33). Прийом таких сигналів на звичайний приймач супергетеродина неможливий (після детектування прослуховується звичайний шум). Для прийому може бути використаний тільки спеціальний приймач.

В процесі появи і розвитку радіозакладок на нашому ринку істотну зміну зазнали і види модуляції, використовуваною в них. І хоча у наш час все ще широко використовуються радіозакладки з WFM (широкосмуговою) і NFM (вузькосмуговою) модуляцією, з'явився принципово новий клас радіозакладних пристроїв з дельта-модуляцією. Крім того, в найбільш професійних радіозакладках використовують такі складні сигнали, як шумоподібні або з псевдовипадковою перестановкою частоти, що несе. Наприклад, в радіозакладках SIM-PR-9000T і РК-1970 використовуються

шумоподібні сигнали з фазовою маніпуляцією і шириною спектру 4 і 5 МГц.

При кодуванні перехопленої інформації часто застосовується аналогове скремблювання, що змінює характеристики мовного сигналу таким чином, що він стає нерозбірливим. Так, в радіозакладці РК-2010S використовується проста інверсія спектру з точкою інверсії 1,862 кГц, а в радіозакладці «Брусок-ЛЗБ ДУ», РК-1380SS – складна інверсія спектру. У ряді закладок використовується перетворення мовної інформації в цифровий вигляд (радіозакладки РК-1195-SS, РК-2050), а в радіозакладках SIM-PR-9000T і РК-1970 разом з перетворенням інформації в цифровий вид використовується її шифрування.

У технічних характеристиках ряду радіоприймальних обладштувань пошуку радіозакладок кількість можливих, для гарантованого перехоплення, видів модуляції і кодування не перекриває можливостей, закладених в закладних пристроях. Це істотно ускладнює пошук закладних пристроїв по їх випромінюванню, вимагає постійної модернізації радіокомплексів для забезпечення пошуку і перехоплення, постійно оновлюваних нових видів модуляції що з'являються, і закриття передавання перехопленої закладними обладштуваннями інформації.

Істотне значення для організації каналів передачі перехопленої інформації в радіодіапазоні має використовувана в закладному пристрої антенна система. В якості такої можуть бути використані: *а) власний антенний пристрій, б) випадкова антена.*

В якості власної антени використовується зазвичай чвертьхвильова антена, що має кругову діаграму спрямованості, що зручно для того, хто знімає інформацію, оскільки не пред'являє особливих вимог для установки апаратури перехоплення, але розміри антенної системи залежать від використовуваного діапазону. У діапазонах ОВЧ і УВЧ як антена зазвичай використовуються дротяні чвертьхвильові антени, при переході в НВЧ-діапазон – штирьова. Відомі випадки використання в НВЧ-діапазоні спрямованих антенних систем, що дозволяє зменшити ризик виявлення закладного пристрою, оскільки діаграма спрямованості по максимуму в цьому випадку спрямована на радіоприймальний пристрій знімання інформації. В якості таких антен часто використовують спіральну або рамкову антену.

Випадкові антени. Часто картина істотно змінюється, якщо як передавальна антена використовуються відрізки лінії передач, в які включаються закладні пристрої, так званні випадкові антени. Шнур, що сполучає трубку з телефонним апаратом (у разі, якщо закладка поміщена в телефонну трубку, наприклад в капсулу телефонної трубки) або відрізки телефонної лінії передачі (якщо закладний пристрій включається в розетку телефонної лінії). У останньому випадку довжина цих відрізків може бути найрізноманітнішою, і діаграма спрямованості і поляризаційні характеристики антени виходять найрізноманітнішими.

При використанні радіозакладок, працюючих в ІЧ-діапазоні, приймальний пристрій (з антеною) камуфлюється, як правило, в приладах спостереження або фотографування, оскільки для цього діапазону частот антенний пристрій має бути виконаний у вигляді фокусуєчого пристрою. Разом з такою позитивною якістю, як гарне приховування факту передачі, слід зазначити необхідність строгої фіксації положення закладки і приймального пристрою, а також забезпечення прямої видимості між ними (для забезпечення мінімального загасання на трасі передачі перехопленої інформації). Для протидії перехопленню випромінювань радіозакладних пристроїв в останніх використовується включення радіозакладки тільки на момент проведення переговорів в приміщенні, де встановлена радіозакладка. Це може бути здійснено шляхом включення в схему радіозакладки системи управління включення передавача від голосу (система VAS або VOX). В цьому випадку радіозакладка працює (при відсутності джерела акустичного сигналу) в черговому режимі як приймач акустичного сигналу, що вимагає мінімального споживання енергії від джерела живлення. При появі в приміщенні джерела акустичного сигналу система включає радіопередавач і закладка працює в повному режимі з передачею перехопленого акустичного сигналу. Включення такої системи до складу радіозакладки дозволяє підвищити її скритність і збільшує термін її дії.

Для цих же цілей може бути використана система дистанційного управління. Як правило, ця система використовується для включення і виключення передавача радіозакладки, а також для зміни режиму роботи передавача, величини випромінюваної потужності і параметрів випромінюваного сигналу.

Це досить складні системи, що мають канал прийому сигналів

управління. У такій системі в черговому режимі працює тільки радіоприймальне обладнання контролю управління, після подання сигналу управління включається передавальне обладнання радіозакладки. Для передачі сигналу управління використовується, як правило, УКХ-діапазон, сигнали управління кодуються в цілях уникнення неправдивих спрацювань.

Нині розроблені радіозакладні пристрої, які можуть контролювати декілька приміщень (наприклад, мають два і більше мікрофонів для контролю різних приміщень). Система дистанційного керування дозволяє здійснювати підключення контрольованих приміщень, оптимізувати потужність випромінювання передавача закладки в цілях їх захисту від пере-хвата радіовипромінювань закладного пристрою.

Ще одним способом підвищення скритності передаваної радіозакладкою інформації є використання проміжного накопичення перехопленої інформації. До складу такого радіозакладного пристрою входить безкінематичний цифровий накопичувач, передавач для прискореної передачі накопиченої інформації і канал управління роботою радіозакладки. У подібній радіозакладці впродовж декількох годин (6...14 ч) накопичується перехоплювана інформація, а потім впродовж 7...14 мін передається до ефіру. Природно, що використання можливих способів приховання передаваної інформації істотно позначається на вимогах до радіоприймального обладнання пошуку закладних пристроїв по їх випромінюванню.

Радіозакладні пристрої виконуються у вигляді технологічних модулів або закамуфльованими в певні пристрої.

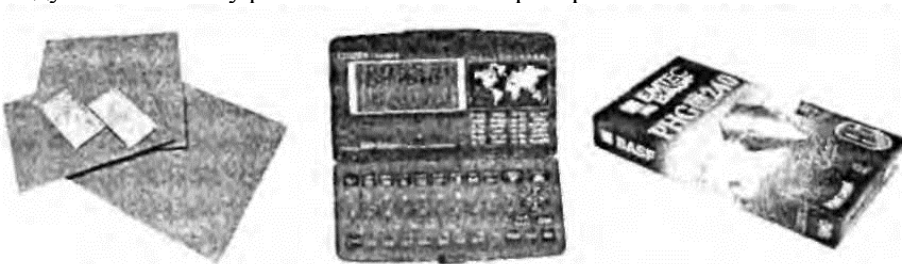


Рисунок 4.1 – Видів закамуфльованих радіомікрофонів

На рис. 4.1 приведені моделі радіомікрофонів, які можуть бути закамуфльовані в різні побутові або господарські предмети (картон,

калькулятор, касету і тому подібне). Одночасно випускається значна кількість радіозакладних пристроїв, закамуюфльованих в предмети і пристрої, як правило, супутні розмовляючим співрозмовникам, – попільничку, вазу, запальничку, калькулятор або розташованими в місцях, де проводяться переговори, - трійники, перехідні пристрої, настільні лампи, елементи одягу і тому подібне (рис. 4.2).

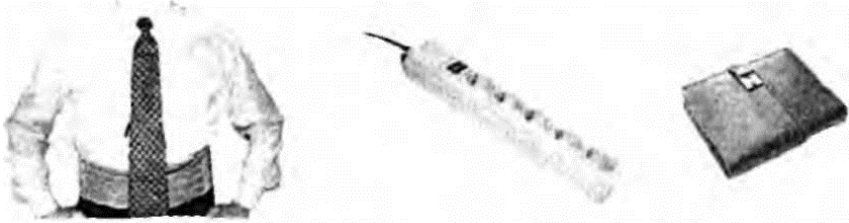


Рисунок 4.2. – Варіанти закамуюфльованих радіозакладок

Певні обмеження на використання радіозакладних пристроїв роблять необхідні для їх роботи джерела живлення. Проблема не стоїть гостро, якщо для живлення використовуються зовнішні джерела живлення – мережа живлення (постійна або змінна), телефонна лінія зв'язку, джерела живлення пристроїв, під які закамуюфльовані радіозакладні пристрої. Проте і при цьому потужність, що відбирається з цих мереж для живлення радіозакладок, має бути обмеженою. Це пов'язано передусім з тим, щоб по відборі цієї потужності не можна було визначити наявність закладного пристрою. Ця вимога обмежує потужність таких радіозакладок і дальність їх дії. При живленні радіозакладних пристроїв від автономних джерел живлення (батарей, акумуляторів і тому подібне) час їх роботи може складати від декількох годин до декількох місяців. Використання схем управління роботою передавача (систем VAS, VOX, дистанційних систем управління роботою передавача і тому подібне) дозволяє збільшити часовий інтервал працездатності радіозакладного пристрою і довести його до декількох років при забезпеченні режиму роботи закладки по включенню до одного-двох місяців.

Відомі випадки, коли живлення радіозакладних облаштувань здійснювалося від систем світлоперетворення, причому такі системи дають живлення, як від природного, так і від штучного світла.

Наприклад, такий світлоперетворювач може починати роботу

при включенні світла в приміщенні, де встановлена закладка, і, отже, така радіозакладка працюватиме тільки в момент наявності світла в приміщенні.

4.1.3 Радіозакладні пристрої, що перевипромінюють

Перші відомості про радіозакладні пристрої з перевипромінюванням відносяться до середини 1940-х років, коли в одному з патентів було описано пристрій, в конструкцію якого був певним чином включений чвертьхвильовий резонатор, налаштований на частоту 330 МГц (рис. 4.3).

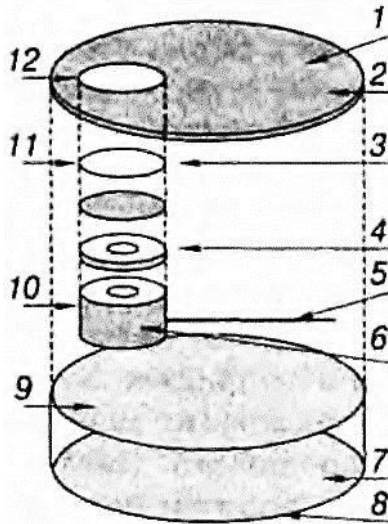


Рисунок 4.3.– Конструкція радіозакладки, що перевипромінює :

1 – кришка з діелектричного матеріалу; 2 – місце стикування з металевою циліндричною склянкою; 3 – вставна кришка з феритового матеріалу; 4 – кільце з ізолятора; 5 – металева антена (чвертьхвильовий вібратор на частоту 330 МГц); 6 – підлаштований конденсатор, що погоджує; 7 – спеціальна рідина; 8 – стакан; 9 – тонкий шар маслянистої рідини, що реагує на звукові коливання; 10 – металевий циліндр, що є $\frac{1}{2}$ котушками індуктивності на 10 мГн; 11 – металевий циліндр; 12 – отвір для встановлення резонатора з антеною.

Оболонка резонатора «прозора» для хвиль УКХ-діапазону і тому хвиля від зовнішнього джерела цієї частоти ефективно відбивається від резонатора. З іншого боку, його розташування на

шарі маслянистої рідини призводить до того, що при виникненні акустичного поля резонатор приходить разом з цим шаром в мікроколивання, що відповідають акустичному (мовному) сигналу, і в такт з цими коливаннями змінюється добротність і резонансна частота резонатора.

Відбитий сигнал таким чином модулюється інформаційним акустичним сигналом і в місці прийому може бути досить легко виділений.

Спецслужба Англії (MU5) створила копію цього пристрою, який використовувався як спецслужбами Англії, так і Америки під кодовою назвою «Сатир». За цим же принципом працюють закладки, що називаються аудіотранспондерами (SIM-АТР-16, РК-500 та ін.).

Подібні пристрої працюють в УКХ і НВЧ-діапазонах. Передавач вузькосмуговим, практично моночастотним сигналом опромінює транспондер, в приймачі якого виділяється зондуєчий сигнал і подається на модулятор. В якості модулюючого використовується сигнал, що поступає з мікрофону або мікрофонного підсилювача.

Промодульований відбитий сигнал перевипромінюється у цілях його маскування на тлі потужнішого опромінюючого сигналу, його частоту дещо зсовують відносно частоти опромінюючого сигналу. Наприклад, для аудіотранспондера SIM-АТР-16 резонансний контур вихідного каскаду транспондера разлагоджений відносно частоти опромінюючого сигналу на частоту 12 кГц (сигнал, що опромінює, – 160 МГц, що перевипромінює, – 160,012 МГц).

Приймальноперевипромінююча система використовує плоску кільцеву антену. Транспондер має розміри 90×90×4 мм, що дозволяє легко маскувати його в приміщенні. Потужність перевипроміненого сигналу залежить від потужності опромінюючого сигналу, і якщо остання знаходиться в межах 10 Вт, то забезпечується дальність перехоплення 50...300 м.

Час функціонування транспортера складає 2000...4000 год. Використання як опромінюючою більш високу частоту дозволяє зменшити розміри аудіотранспондера. Так, в SIM-ТР-40, де для опромінювання використовується частота 800...950 МГц, розміри транспондера дорівнюють 6×24 мм. При живленні від внутрішньої батареї з напругою 3 В час роботи транспондера близько 4 місяців.

4.1.4 Закладні облаштування типу «довге вухо»

Окремої за принципом роботи є група закладних пристроїв, що відноситься до закладок типу «довге (телефонне) вухо» або закладка «з штучно піднятою трубкою». Остання назва досить точно визначає принцип роботи цього типу закладного пристрою.

При опущеній телефонній трубці на телефонну лінію замкнута система виклику (механічна або електрична), яку ініціює сигнал виклику. Коли абонент піднімає трубку, до лінії під'єднується телефонний апарат і забезпечується зв'язок. Закладка з «штучно піднятою трубкою» забезпечує під'єднання телефонного апарату і, отже, мікрофону телефонної трубки (або додаткового мікрофону) до лінії без механічного підйому телефонної трубки.

Подання сигналу про штучний підйом телефонної трубки може здійснюватися різними способами. Наприклад:

- набирається номер телефону із закладкою;
 - після першого (другого і тому подібне) викличного сигналу кладеться трубка (при цьому виклик в самому телефонному апараті пригнічується);
 - через певний інтервал часу (10...40 с) здійснюється повторний виклик;
 - для того, щоб сторонній, що випадково потрапив з викликом в цей відрізок часу, не підключився до системи через 45...60 с йде сигнал відбою;
 - через вказаний проміжок часу закладний пристрій підключається до лінії, і йде контроль акустики приміщення. Треба відмітити, що при підключенні до телефонного апарату додаткових мікрофонів може бути організований контроль інших приміщень;
 - при піднятті телефонної трубки закладка відключається.
- Відомі і інші способи підключення телефонів із закладкою:
- після набору номера телефону із закладкою в телефонну лінію транслюється спеціальний звуковий сигнал через мікрофон апарату прослуховування (подібний пристрій називається біпером);
 - при проходженні цього спеціального сигналу система підключає телефон із закладкою на прослуховування.

Особливістю подібних закладних пристроїв є їх велика дальність дії – практично по усій земній кулі.

4.1.5 Мережеві закладні пристрої

Електромережа будівлі і її елементи можуть бути використані зловмисником для установки і живлення закладних пристроїв, а також передачі перехопленої інформації. Дротяні системи прихованого аудіоконтролю призначені для негласного знімання і передачі аудіоінформації по дротяних лініях. Прийом сигналів аудіоінформації робиться спеціальним приймачами серії КПЛ.

Вироби серії КПЛ призначені для контролю акустичної обстановки приміщення з передачею інформації по лініях дротяних комунікацій: електричній мережі змінного струму - 220 В частотою 50 Гц (КПЛ-С) або телефонній мережі на частотах (КПЛ-Т), що піднесуть. Прийом передаваної інформації здійснюється на спеціальний приймальний пристрій, що дозволяє приймати сигнал від трьох передавачів інформації. Приймач оснащений гніздами для підключення головних телефонів, магнітофона і зовнішнього джерела живлення. Крім того, закладні пристрої можуть бути закамуюфльовані під розетку, трійник-розетку, різні перехідники, в лампах, електричних світильниках, торшерах і тому подібне. Частина закладних пристроїв випускається без камуфляжу для того, щоб споживач міг їх встановлювати на власний розсуд.

Закладні пристрої, пов'язані з електромережею, можуть бути умовно розділені на дві групи:

- закладні пристрої, що забезпечують контроль акустичної інформації приміщення з передачею перехопленої інформації по мережі електроживлення;
- радіозакладні пристрої, що забезпечують акустичний контроль приміщення з живленням від мережі електроживлення і передачею перехопленої інформації по радіоканалу.

Однією з істотних особливостей подібних закладних пристроїв є необмежений час їх роботи (поки є мережа живлення). Закамуюфльовані під широко використовувані в побуті і роботі такі прилади, як подовжувачі, трійники, настінні лампи і інші побутові електроприлади, подібні закладні пристрої досить просто можуть бути «впроваджені» в приміщення, що цікавить.

У подібних пристроях акустичний канал мікрофону виконується як конструктивні складові пристрою, в який камуфлюється закладка.

Габарити облаштувань камуфляжу забезпечують розташування передавальних пристроїв і при необхідності антенних систем.

Усі облаштування камуфляжу зберігають своє пряме призначення. Включення закладних пристроїв забезпечується, як правило, включенням камуфлюючого пристрою (подовжувач, трійник і тому подібне) в мережу.

Проте для таких пристроїв існує ряд обмежень. Наприклад, не рекомендується використати виріб для підключення приладів з великим споживанням електроенергії (більше 0,5 кВт), оскільки інакше може з'явитися мережевий фон в акустичному каналі. Не рекомендується встановлювати радіомікрофон зблизька до джерел акустичних перешкод – холодильника, вентилятора, трансформатора, телевізора і тому подібне.

Для забезпечення більшої скритності закладних облаштувань використовується дистанційне керування, що дозволяє включати закладний пристрій тільки на необхідний час.

Розглянемо основні характеристики деяких закладних пристроїв з живленням від електромережі і передачею інформації по мережі електроживлення.

Мережевий мікрофон «Сеть-ІР» призначений для тривалої передачі мовної інформації по наявній у будівлі електромережі. Виконаний у вигляді стандартної електричної розетки. Дальність передачі інформації не менше 100 м, живлення від електричної мережі, час роботи не обмежено, прийом ведеться на спеціальний приймач.

Мережевий мікрофон «Сеть-2НК» призначений для контролю акустики в приміщенні і передачі отриманої інформації по мережам електроживлення в ультразвуковому діапазоні частот. Прослуховування здійснюється на головні телефони, є можливість підключення магнітофона. Споживана потужність передавача - 100 мВт, частотна модуляція, частота, що несе, - 100 кГц, час роботи не обмежено, чутливість приймача, не менше 20 мкВ.

Комплект передачі інформації по мережі 220 В призначений для контролю акустики в приміщенні і передачі інформації по мережі змінного струму 220 В, 50 Гц. Габаритні розміри складають 45×25×10 мм. Частота, що несе, - 1,6...2,2 МГц, частотна модуляція, девіація сигналу - 30...60 кГц, вихідна напруга - 200...300 мВ, споживаний від мережі струм - 5...15 мА; смуга передаваного сигналу - 0,3...6,0 кГц.

Система аудіоконтролю приміщення по мережі 220 В М220-01 складається з передавального облаштування SEL-M220-01 і приймача

SEL-SP-35/CP. Призначена для негласного отримання акустичної інформації приміщення і передачі її по мережі електроживлення 220 В в межах однієї фази. Діапазон частот - 200...500 кГц, фазова модуляція, дальність передачі - до 100 м.

Система аудіо-контролю приміщення по мережі 220 В КПЛ-С призначена для контролю акустики приміщення з передачею інформації по мережі змінного струму 220 В 50 Гц. Габарити - 45×25×10 мм живлення від лінії електромережі - 220 В частотою 50 Гц або вбудований акумулятор. Передавач інформації з частотою, що несе, 1,6...2,2 МГц фазової модуляції, смуга передаваного сигналу 0,3...6,0 кГц. Приймач інформації з діапазоном перебудови 1,6...2,2 МГц з фазовою модуляцією сигналу, що приймається. Габарити 110×56×21 мм, проміжна частота - 10,7 МГц, ширини смуги тракту sH4 - 180 кГц.

Інша група радіозакладних пристроїв з живленням від електромережі призначена для передачі інформації по радіоканалу.

Подовжувач – радіозакладний пристрій, закамouflьований під звичайний подовжувач. Призначений для контролю акустики приміщення з передачею інформації по радіоканалу і живленням від електромережі 220 В. Напруга живлення - 220 В, частота - 50...60 Гц, час безперервної роботи не обмежений, робочі частоти передачі: 108...130 МГц; 416...424 МГц, 470±10 МГц, WFM -, NFM -модуляція, дальність передачі - 100...300 м, кварцова стабілізація передавача.

Фільтр мережевий призначений для контролю акустики приміщення з передачею інформації по радіоканалу і живленням від електромережі напругою 220 В і частотою 50...60 Гц. Радіомікрофон виконаний у вигляді звичайного мережевого фільтру «Pilot». Час безперервної роботи не обмежений, робочі частоти передачі - 108...130 МГц; 416...424 МГц, 470±10 МГц, WFM -, NFM -модуляція, дальність передачі - 100...300 м, кварцова стабілізація передавача.

Останнім часом отримав широке розповсюдження *шпигунський GSM жучок* для акустичного прослуховування приміщення. Він може бути вбудований у блок живлення, до якого можна підключити будь-який USB пристрій (наприклад, телефон поставити на зарядку) і включити його в розетку. Або це буде на вигляд звичайна електрична розетка, комп'ютерна миша чи навіть кабель USB (рис.4.4).

Суть роботи: в корпус вставляється SIM-карта будь-якого стільникового оператора, закривається корпус. Після дзвінка на номер

встановленої SIM-карти, автоматично і безшумно шпигунський пристрій включається і здійснюється акустичне прослуховування навколо приладу.

Є додаткова функція, яка змушує шпигунський жучок працювати в режимі звукової сигналізації і телефонувати до господаря при виникненні звуку. Ця функція активується SMS-командою.



Рисунок 4.4. – Варіанти встановлення шпигунського GSM жучка

Важливість в тому, що час роботи GSM жучка не обмежена: під час включення до джерела живлення заряджається внутрішній акумулятор, а в стані відключення від зовнішнього живлення жучок прослуховування працює від автономного акумулятора в режимі очікування до 2-х тижнів, в режимі моніторингу 3-5 дня.

ЛІТЕРАТУРА

1. Сёмкин, С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. [Текст] / С.Н. Сёмкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. – М.: Гелиос АРВ, 2005. – 192 с.
2. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений. [Текст] / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Издательский центр “Академия”, 2006. – 256 с.
3. Торокин, А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности. [Текст] / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. [Текст] / А.А. Малюк. – М.: Горячая линия-Телеком, 2004. – 280с.
5. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов. [Текст] / В.И. Ярочкин. – М.: Академический Проект; Гаудеамус, 2-е изд.– 2004. – 544 с.
6. Хорошко, В.А. Методы и средства защиты информации [Текст] / В.А. Хорошко, А.А. Чекатков. – К.: изд. Юниор, 2003. – 504 с.
7. Бузов, Г.А. Защита от утечки информации по техническим каналам: Учебное пособие. [Текст] / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев.– М.: Горячая линия-Телеком, 2005. – 416с.
8. Богуш, В.М. Інформаційна безпека держави. [Текст] / В.М. Богуш, О.К. Юдін. – К.: "МК-Прес", 2005. – 432 с.
9. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. [Текст] / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.
10. Максимов, Ю.Н. Технические методы и способы защиты информации. [Текст] / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. – СПб.: Полигон, 2000. – 320 с.
11. Организация и современные методы защиты информации. [Текст] / Под общей редакцией С.А. Диева и А.Г. Шаваева. – М.: Концерн "Банковский Деловой Центр", 1998, – 472 с.

12. Железняк, В. К. Защита информации от утечки по техническим каналам: учебное пособие [Текст] / В.К. Железняк. – СПб.: ГУАП., 2006. – 188 с.
13. Барсуков, В.С. Обеспечение информационной безопасности. [Текст] / В.С. Барсуков. – М: ТЭК, 1996. – 268 с.
14. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2001. – 688 с.
15. Столинкс, В. Криптография и защита сетей: принципы и практика [Текст] / Пер. с англ. А.Г. Сивака, А.А. Шпака; Под ред. А.Г. Сивака. – 2-е изд. – М. СПб. Киев: Вильямс, 2001. – 672 с.
16. Максим, М. Безопасность беспроводных сетей. [Текст] / Мерритт Максим, Дэвид Поллино; Пер. с англ. А.В. Семенова. – М.: Компания АйТи; ДМК Пресс, 2004. – 228 с.
17. Абалмазов, Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. [Текст] / Э.И. Абалмазов. – М.: Гротек, 1997 г. - 248 с.
18. Завгородний, В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. [Текст] / В.И. Завгородний. – М.: Логос, 2001. – 264 с.
19. Соколов, А.В. Шпионские штучки. Новое и лучшее. [Текст] / А.В. Соколов. – СПб.: ООО «Издательство Полигон», 2000.– 256 с.
20. Бурячок, В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. – К.:ДУТ, 2015. – 345 с.
21. Хорев А.А. Способы и средства защиты информации. [Текст] / А.А. Хорев. – М.: МО РФ, 2000 г. – 316 с.
22. Энциклопедия промышленного шпионажа. [Текст] / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко / под общ. Ред. Е.В. Куренкова. – СПб.: ООО «Издательство Полигон», 1999. – 512 с.
23. Архипов, О.Є. Захист інформації в телекомунікаційних мережах та системах зв'язку: Навч.-метод. посіб. [Текст] / О.Є. Архипов, В.М. Луценко, В.О. Худяков. – К.: Політехніка, 2003. – 40 с.
24. Гайкович, В.Ю. Основы безопасности информационных технологий. [Текст] / В.Ю. Гайкович, Д.В. Ершов. – М.: изд. "Ось", 1995. – 54 с.

25. Гайкович, В.Ю. Безопасность электронных банковских систем. [Текст] / В.Ю. Гайкович, А.М. Першин. – М.: Компания Единая Европа, 1994. – 384 с.
26. Волхонский, В. В. Устройства охранной сигнализации. [Текст] / В.В. Волхонский. – СПб.: Эконопис и культура, 1999. – 272 с.
27. Коржик, В.И. Теоретические основы информационной безопасности телекоммуникационных систем: Учеб. пособие. [Текст] / В.И. Коржик, Д.В. Кушнир– СПб.: СПбГУТ.-СПб, 2000. – 134 с.
28. Мельников, В. П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студ. высш. учеб. заведений [Текст] / В.П. Мельников, С.А. Клейменов, А.М. Петраков; Под. ред. С.А. Клейменова. – 3-е изд. – М.: Издательский центр «Академия», 2008. – 336 с.
29. Петраков, А.В. Основы практической защиты информации: Учеб. пособие. [Текст] / А.В. Петраков – М.: Радио и связь, 1999. – 368 с.
30. Смит, Р.Э. Аутентификация: от паролей до открытых ключей [Текст] / Р.Э. Смит; Пер. с англ. – М. СПб. Киев : Вильямс, 2002. – 432 с.
31. Фергюсон, Н. Практическая криптография. Монография. [Текст] / Н. Фергюсон, Б. Шнайер; Пер. с англ. Н.Н. Селиной. – М. СПб. Киев: ИД Вильямс : Диалектика, 2005. – 421 с.
32. Сمارт, Н. Криптография. [Текст] / Н. Сمارт; Пер. с англ. С.А. Кулешова; Под ред. С.К. Ландо. – М.: Техносфера, 2005. – 528 с.
33. Рассел Р. и др. Защита от хакеров коммерческого сайта [Текст] / Пер. с англ. – М.: Компания АйТи: ДМК Пресс: ТЕТРУ, 2004. – 552 с.