Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут"

Іванченко С.О., Гавриленко О.В., Липський О.А.,

Шевцов А.С.

ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. ПОРЯДОК СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Київ
2016

УДК 621.39
ББК Ч23(4Укр)
І 231

РЕЦЕНЗЕНТИ:

Воронов В.В. заступник начальника 1 управління Департаменту технічного захисту інформації Адміністрації Держспецзв'язку, к.т.н., доцент;

Самойлов Д.В. начальник кафедри застосування засобів криптографічного захисту інформації Військового інституту телекомунікацій та інформатизації, к.т.н., доцент.

Рекомендовано Вченою радою НТУУ "КПІ" в якості навчального посібника
Протокол № 1 від 18.01.2016 р.

І231 Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

Навчальний посібник призначений для ознайомлення курсантами та студентами з найбільш поширеними причинами витоку інформації та нормативно визначеними діями щодо їх знешкодження.

Проведено огляд загального підходу з забезпечення безпеки інформації, що визначено в Україні; наведено основні різновиди та сутність технічних каналів витоку інформації, що можуть утворюватись на об'єктах інформаційної діяльності, та на основі діючих нормативних документів розглянуто порядок створення комплексів технічного захисту інформації.

Посібник може бути використаний у вищих начальних закладах, в яких програми підготовки містять тематику з технічного захисту інформації.

УДК 621.39
ББК Ч23(4Укр)

© НТУУ «КПІ», 2016

ЗМІСТ

ПЕРЕДМОВА 5
I. ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ 6
1.1. Інформація як об’єкт захисту. Основні визначення та положення.....6
1.2. Технічний захист інформації. Основні визначення та положення..... 11
2. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ..... 17
2.1. Технічні канали витоку інформації. Загальні поняття..... 17
2.2. Класифікація технічних каналів витоку інформації..... 22
2.3. Сутність та шляхи утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами 26
2.3.1. Канал побічних електромагнітних випромінювань ОТЗС..... 26
2.3.2. Канал побічних електромагнітних випромінювань ДТЗС 28
2.3.3. Канал “паразитної” модуляції сигналів ВЧ генераторів..... 29
2.3.4. Канал “паразитної” ВЧ генерації підсилювачів..... 31
2.3.5. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС..... 33
2.3.6. Канал побічних електромагнітних наведень на комунікації ДТЗС..... 37
2.3.7. Канал ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС)..... 39
2.4. Технічні канали витоку мовної інформації..... 44
2.4.1. Акустичні канали витоку інформації..... 45
2.4.2. Акустовібраційні (віброакустичні) канали витоку інформації.. 47
2.4.3. Акустоелектричні канали витоку мовної інформації..... 48
2.4.4. Акустооптоелектронні (лазерні акустичні) канали витоку інформації..... 53

2.4.5. Канали ВЧ нав’язування (для зняття мовної інформації) 55
2.5. Технічні канали витоку інформації на основі закладних пристроїв 60
2.5.1. Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв)..... 60
2.5.2. Загальні характеристики та особливості деяких типів закладних пристроїв 62
2.5.3. Заходи захисту інформації від витоку каналами на основі закладних пристроїв 66
2.6. Канали перехоплення (зняття) інформації з каналів зв’язку .. 70
2.7. Технічні канали витоку видової інформації 74
2.8. Матеріально-речовинні канали витоку інформації 75
2.8.1. Способи гарантованого знищення та добування інформації з магнітних носіїв 76
3. СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ 81
3.1. Створення комплексів технічного захисту інформації. Загальні положення 81
3.2. Розроблення комплексу ТЗІ 86
3.2.1. Передпроектні роботи 86
3.2.2. Розроблення технічного проекту комплексу ТЗІ 88
3.3. Упровадження комплексу ТЗІ 91
3.4. Атестація комплексу ТЗІ 92
3.5. Будівельні норми на приміщення для зберігання секретних документів та роботи з ними 95
3.5.1. Загальні положення та вимоги щодо розміщення режимних приміщень 95
3.5.2. Вимоги до будівельних конструкцій режимних приміщень 96
3.5.3. Вимоги щодо сигналізації в режимних приміщеннях 99
СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 101

ПЕРЕДМОВА

Стрімкий розвиток суспільства призвів до широкого використання в усіх сферах діяльності (політичній, економічній, соціальній, побутовій та інших) швидкодіючих інформаційних систем та технологій, які надають можливість доступу до світового інформаційного простору. Одночасно збільшилися загрози для інформації, тяжкість наслідків реалізації яких посприяли оновленню розуміння захисту інформації, який полягає у забезпеченні цілісності, доступності та конфіденційності інформації. Законодавством України передбачено захист певної інформації, включаючи персональні дані кожної людини.

У навчальному посібнику розглянуті основні причини, що обумовлюють утворення технічних каналів витоку інформації, та порядок створення комплексів технічного захисту від витоку технічними каналами на об'єктах інформаційної діяльності та в інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних системах.

Посібник містить три модуля. У першому модулі надаються організаційно-правові засади технічного захисту інформації в Україні та основні напрями діяльності з захисту інформації та охорони державної таємниці. У другому модулі надаються основні поняття з витоку інформації, причини, що обумовлюють утворення технічних каналів витоку, та класифікація технічних каналів витоку інформації. У третьому модулі надається порядок створення комплексів технічного захисту інформації як взаємопов'язаної сукупності організаційних, інженерних і технічних заходів та засобів, призначених для захисту інформації від витоку технічними каналами.

Посібник рекомендовано для курсантів та студентів вищих начальних закладів, програма підготовки яких включає тематику з захисту інформації від витоку технічними каналами.

І. ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

1.1. Інформація як об’єкт захисту. Основні визначення та положення

Інформація, яка є важливою для особи, суспільства та держави і втрата якої може спричинити шкоду особі, суспільству або національним інтересам держави в економічній, політичній, військової або інших сферах, повинна захищатися від несанкціонованого ознайомлення спотворення, знищення та блокування, тобто бути **об’єктом захисту**.

Обов'язковість захисту певної інформації встановлена відповідними законами України.

Обов'язковість захисту інформації, що становить державну таємницю, встановлена Законом України “Про державну таємницю”.

Обов’язковість захисту інформації, яка відноситься до державних інформаційних ресурсів, та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, при її обробці в інформаційних, телекомунікаційних або інформаційно-телекомунікаційних системах, встановлена Законом України “Про захист інформації в інформаційно-телекомунікаційних системах”.

Обов’язковість захисту персональних даних, які обробляються в базах персональних даних, встановлена Законом України “Про захист персональних даних”.

Інформація [information] – відомості про об'єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які зменшують наявну про них ступінь невизначеності, неповноти знань [1].

У широкому розумінні інформація – це загальнонаукове поняття, що включає в себе обмін відомостями між людьми, обмін сигналами між живою й неживою природою, людьми і пристроями.

З позицій філософії інформація є відображення реального світу за допомогою відомостей (повідомлень).

Повідомлення – це форма подання інформації у вигляді мови, тексту, зображення, цифрових даних, графіків, таблиць і та ін.

Термін “інформація” походить від латинського “information”, що означає роз'яснення, повідомлення, виклад.

Згідно з Законом України “Про інформацію” за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Інформацією з обмеженим доступом (ІзОД) є конфіденційна, таємна та службова інформація.

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

Таємна інформація – інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону України “Про доступ до публічної інформації”, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю. [Закон України “Про доступ до публічної інформації”].

Державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [11].

Секретна інформація за ступенем секретності (категорією, яка характеризує важливість секретної інформації, ступінь обмеження

доступу до неї та рівень її охорони державою) поділяється на інформацію "особливої важливості", "цілком таємно", "таємно".

Інформація, що становить державну таємницю, визначається Законом України “Про державну таємницю” та Зводом відомостей, що становлять державну таємницю (ЗВДТ), затвердженим наказом СБ України № 440 від 12.08.2005 та зареєстрованим в Міністерстві юстиції України 17.09.2005 за № 902/11182.

Згідно з Законом України “Про доступ до публічної інформації” до **службової інформації** може належати така інформація:

1) що міститься у документах суб'єктів владних повноважень, що становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування".

Міністерствами, іншими центральними органами виконавчої влади, обласними та Київською міською держадміністраціями складаються та затверджуються переліки відомостей, які містять службову інформацію.

Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. [Закон України “Про доступ до публічної інформації”]

Державні інформаційні ресурси – це систематизована інформація, що є доступною за допомогою інформаційних технологій,

право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Важливою категорією для людини та суспільства є безпека.

Безпека – стан, при якому будь-кому, будь-чому не загрожує будь-що (небезпека, загрози будь-якого виду) [1]. Поняття безпеки можна представити у вигляді моделі (рис.1.1).

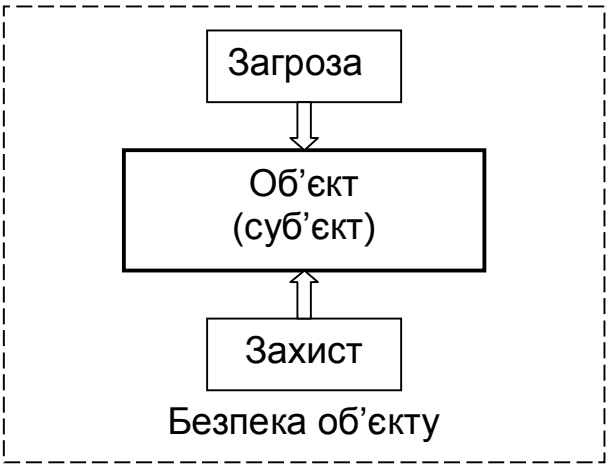


Рис.1.1. Модель безпеки об'єкту.

Однією з головних функцій держави є забезпечення національної безпеки.

Національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам [9].

Однією з складових національної безпеки **є інформаційна безпека.** Статтею 17 Конституції України [13] визначено, що

забезпечення інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив, ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства та умисне спричинення негативних наслідків застосування інформаційних технологій [3].

Інформаційна безпека забезпечується діяльністю, спрямованою на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України [3]. Зокрема діяльність із запобігання порушення цілісності та доступності інформації і несанкціонованого обігу інформації з обмеженим доступом складає захист інформації.

Безпека інформації – стан інформації, інформаційних ресурсів та інформаційних систем, при якому з потрібною імовірністю забезпечується захист інформації від [22]: витоку, спотворення (модифікації), блокування, втрати (несанкціонованого знищення, крадіжки), несанкціонованого копіювання і т.п.

Таким чином, у пункті 1.1 надані поняття інформації як об’єкту захисту. Відповідно до законів України до інформації, що підлягає захисту, відноситься:

–інформація, яка становить державну або іншу передбачену законом таємницю;

–службова інформація;

–відкрита інформація, яка належить до державних інформаційних ресурсів, а також про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

–конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації";

–інформація, вимога щодо захисту якої встановлена законом (зокрема, персональні дані).

1.2. Технічний захист інформації. Основні визначення та положення

Захист інформації – діяльність із забезпечення конфіденційності, цілісності та доступності важливої для особи, суспільства та держави інформації, яка обробляється в інформаційних (автоматизованих), телекомунікаційних або інформаційно-телекомунікаційних системах або озвучується на об’єктах інформаційної діяльності, а також із забезпечення використання інформації у відповідності з встановленими правилами.

Конфіденційність, цілісність та доступність – це властивості, які характеризують інформацію як об’єкт захисту.

Конфіденційність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого ознайомлення з нею.

Цілісність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого спотворення, руйнування або знищення.

Доступність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого блокування.

Захищеність інформації – стан інформації, при якому забезпечена відповідність показників захищеності інформації нормам та вимогам захищеності інформації.

Одним з різновидів захисту інформації є технічний захист інформації.

Технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Мета ТЗІ – запобігання витоку та/або порушенню цілісності та доступності інформації, що підлягає захисту.

Для забезпечення технічного захисту інформації в України створена система технічного захисту інформації (рис. 1.2):

Рис. 1.2. Система технічного захисту інформації.

Система ТЗІ – сукупність організаційної інфраструктури (об’єкту захисту, органів та об’єктів, де здійснюється ТЗІ, суб'єктів системи ТЗІ,), нормативно-правової бази та матеріально-технічної бази, об'єднаних цілями та завданнями захисту інформації організаційними, інженерними та технічними заходами.

Органами, де здійснюється технічний захист інформації, є:

- органи державної влади,
- органи місцевого самоврядування,

– органи управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України,

– підприємства, установи, організації, військові частини, де здійснюється діяльність з інформацією, що підлягає захисту.

Об’єктами, де здійснюється технічний захист інформації, є:

– об'єкти інформаційної діяльності;

– інформаційні (автоматизовані) телекомунікаційні, інформаційно-телекомунікаційні системи.

Об’єкт інформаційної діяльності (ОІД) – інженерно-технічна споруда (приміщення), транспортний засіб, зона, визначена територія, де здійснюється діяльність, пов’язана з державними інформаційними ресурсами або інформацією, вимога щодо захисту якої встановлена законом.

Серед ОІД відокремлюються ОІД, де здійснюється озвучування інформації, та ОІД, на яких здійснюється обробка інформації технічними засобами (засобами електронно-обчислювальної техніки або пристроями обробки інформації). Останні мають назву “об’єкти електронно-обчислювальної техніки”.

Об’єкт електронно-обчислювальної техніки (об’єкт ЕОТ) – різновид об’єкта інформаційної діяльності, де здійснюється обробка інформації розташованими на ньому на певному місці засобами електронно-обчислювальної техніки або пристроями обробки інформації.

Інформаційно-телекомунікаційна система (автоматизована система) **(ІТС)** – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів, в якій передбачена можливість реалізації програмних процедур розмежування доступу користувачів і яка об’єднує обчислювальну систему, фізичне середовище, де розташована ця система, персонал і оброблювану інформацію.

Суб’єктами системи ТЗІ є:

– уповноважений орган у сфері захисту інформації;

– виконавці робіт у сфері захисту інформації;

– розпорядники, користувачі інформації, що підлягає захисту;

– власники, розпорядники, користувачі об’єктів, де здійснюється захист інформації;

– фізичні та юридичні особи, що здійснюють підготовку фахівців, наукову, науково-технічну та виробничу діяльність у сфері захисту інформації.

Вимоги та завдання щодо захисту та охорони інформації визначаються нормативними документами в залежності від порядку доступу та ступеню обмеження доступу до інформації.

Заходи із захисту інформації мають здійснюватися спільно із заходами її охорони. Так стосовно інформації, що становить державну таємницю, тобто секретної інформації, передбачені заходи з її технічного захисту та охорони державної таємниці, які в узагальненому вигляді наведені на рис. 1.3:

Рис.1.3. Основні заходи з технічного захисту інформації та охорони державної таємниці.

Для захисту інформації створюються системи (комплекси) захисту інформації. Для забезпечення роботи з матеріальними носіями секретної

та службової інформації і їх зберігання (в робочий та неробочий час) створюються системи охорони (здійснюється організація режиму доступу). Системи (комплекси) захисту інформації будуються за такими узагальненими етапами:

1 етап – визначення й аналіз загроз для інформації;

2 етап – розробка політики безпеки та плану захисту інформації;

3 етап – розробка технічного завдання на створення системи (комплексу) захисту інформації;

4 етап – розробка проекту системи (комплексу) захисту інформації;

5 етап – упровадження системи (комплексу) захисту інформації (реалізація плану захисту);

6 етап – оцінювання захищеності інформації (атестація, експертиза);

7 етап – введення системи (комплексу) захисту інформації в експлуатацію.

Таким чином, у пункті 1.2 надані основні положення технічного захисту (визначення та мета технічного захисту інформації, властивості інформації як об’єкта захисту, система технічного захисту інформації та її складові), загальні заходи з технічного захисту інформації та узагальнені етапи побудови систем (комплексів) захисту інформації.

Перелік питань для самоконтролю за 1 розділом

1. Визначення понять інформаційна безпека, безпека інформації.
2. Класифікація інформації за порядком доступу до неї.
3. Поняття секретна, службова, конфіденційна інформація.
4. Основні властивості інформації як об’єкта захисту та їх визначення.
5. Що відноситься до інформації, що підлягає захисту?
6. Основні види діяльності, що проводяться із захисту інформації.
7. Визначення технічного захисту інформації.
8. Система технічного захисту: визначення та складові.

9. Визначення об’єкта інформаційної діяльності та інформаційно-телекомунікаційної системи (автоматизованої системи).
10. Узагальнені етапи побудови систем (комплексів) захисту інформації.

2. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

Однією з найнебезпечніших загроз для інформації, що озвучується на об’єктах інформаційної діяльності або обробляється технічними засобами в тому числі і інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем, є витік інформації технічними каналами.

2.1. Технічні канали витоку інформації. Загальні поняття

Під **витоком інформації** розуміється неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило, технічні, то і канали витоку також називають технічними.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки (рис. 2.1) [2, 4-6].

Також враховуються завади, що діють на вході засобу технічної розвідки.

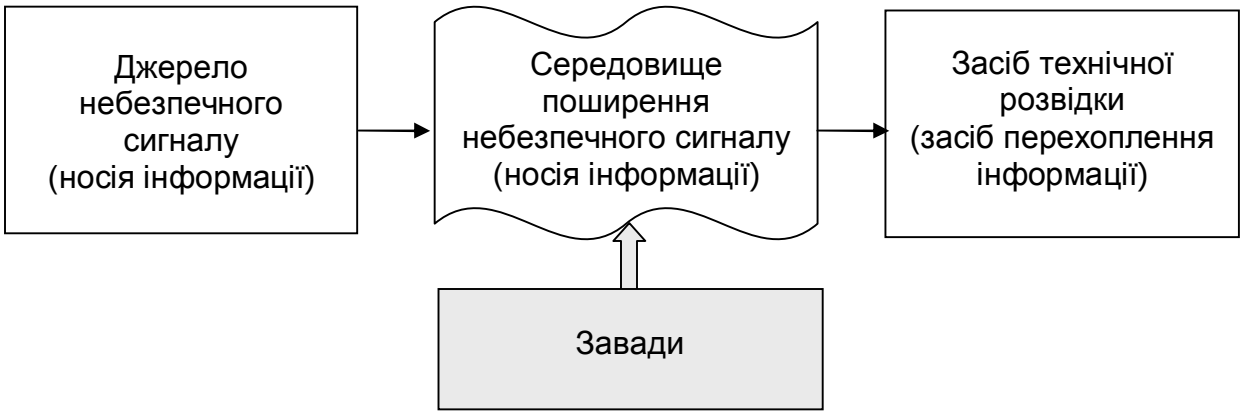


Рис. 2.1. Технічний канал витоку інформації.

Тобто, технічним каналом витоку інформації є фізичний шлях небезпечного сигналу (носія інформації) від джерела небезпечного сигналу до противника.

Небезпечний сигнал – сигнал (поле), у тому числі паразитний (побічний), або його компоненти (фрагменти) будь-якого фізичного походження, які містять інформацію з обмеженим доступом і які можуть бути зняті (перехоплені) засобами технічної розвідки

Носій інформації - небезпечний сигнал чи хімічна речовина, які містять інформацію з обмеженим доступом.

Носієм інформації можуть бути:

- електричний струм;
- електромагнітне поле;
- світло (електромагнітне поле в світловому діапазоні частот);
- лазерний промінь (електромагнітне поле в оптоелектронному діапазоні частот);
- акустичне поле;
- вібраційне поле;
- хімічні матеріали, речовини тощо;
- інші носії.

Середовище поширення небезпечного сигналу (носія інформації) – повітряне, водне та інші фізичні середовища; хімічні речовини; струмопровідні та пружні матеріали, (лінії електроживлення, заземлення, зв’язку, сигналізації, управління, спостереження та інші лінії; кінцеве та з’єднувальне обладнання; інженерні комунікації і спорудження, огороджувальні будівельні конструкції, світлопроникні елементи будинків і споруд (отвори), ґрунт, поверхня земної кори, рослинність тощо), якими може поширюватися небезпечний сигнал (носій інформації).

Засоби технічної розвідки (ЗТР) – технічні засоби, які призначені для несанкціонованого знімання (здобування, перехоплення) інформації.

Розглянемо можливість витоку інформації. Припустимо, що на ОІД передбачаються всі види робіт з інформацією: зберігання носіїв інформації, озвучування інформації, обробка інформації технічними засобами та системами (ТЗС), візуалізація інформації. Схематично можливість витоку інформації наведена на рис. 2.2.

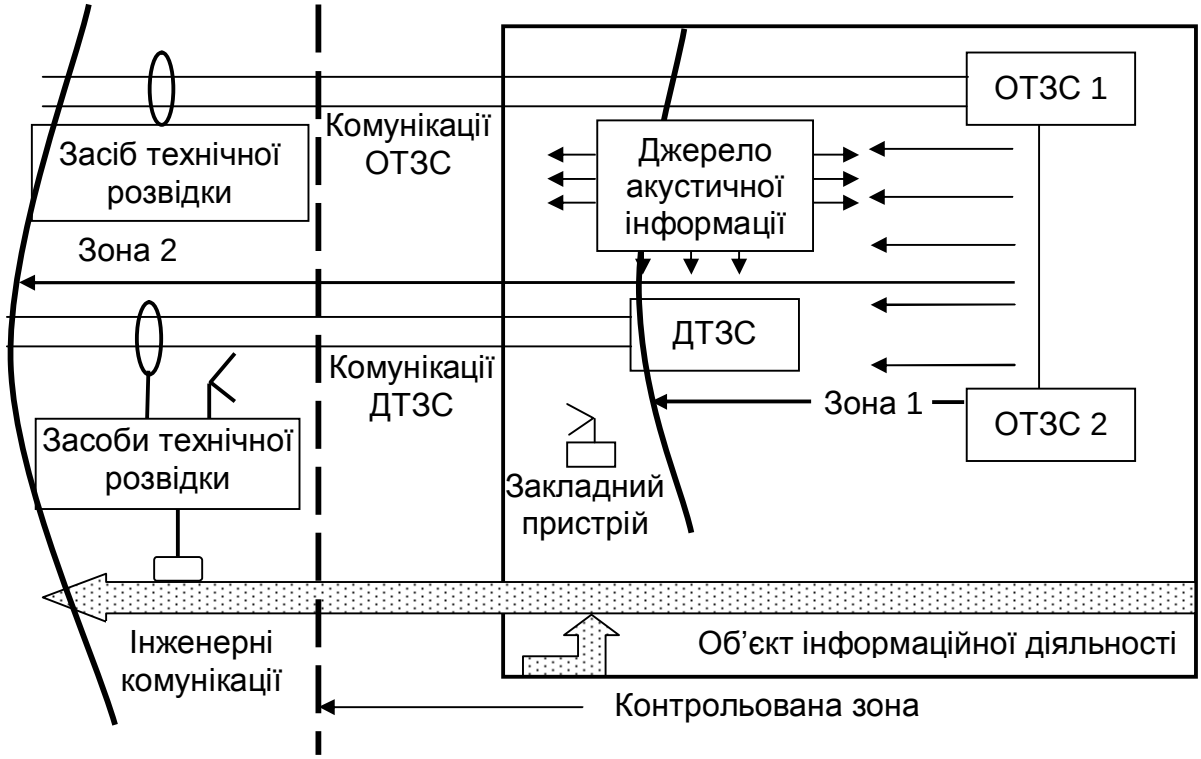


Рис. 2.2. Схематична можливість витоку інформації.

Відповідно до інформаційної діяльності на ОІД можна виділити такі первинні джерела небезпечного сигналу:

– людина, що озвучує інформацію, засоби відтворення або підсилення звуку;

– технічні засоби та системи, що обробляють інформацію;

– монітори засобів електронно-обчислювальної техніки, екрани, секретні документи з надрукованим текстом тощо, на яких візуалізується інформація.

Також можна виділити такі середовища поширення небезпечного сигналу:

– вільний простір;

– комунікації ОТЗС та ДТЗС, які виходять за межі контрольованої зони;

– інженерні комунікації (жорсткі пружні поверхні), які виходять за межі контрольованої зони.

За межами контрольованої зони можливе застосування засобів технічної розвідки, які перехоплюють небезпечний сигнал у вільному просторі, або знімають небезпечний сигнал безпосередньо підключившись до комунікацій ОТЗС, комунікацій ДТЗС або до інженерних комунікацій.

Таким чином, наявні усі три складові технічних каналів витоку інформації, що уможливлює створення певних технічних каналів витоку інформації.

На ОІД одні ТЗС використовуються для обробки і передачі секретної інформації, а інші – для інших завдань, не пов’язаних з обробкою секретної інформації, але необхідних для виробничої діяльності об’єкту. В залежності від того, обробляють технічні засоби секретну інформацію або не обробляють вони розділяються на основні та допоміжні. До допоміжних ТЗС можуть належать засоби міського зв’язку, охоронної та пожежної сигналізації та ін.

Основні технічні засоби та системи (ОТЗС) – розташовані на об’єкті інформаційної діяльності технічні засоби та їх комунікації, які здійснюють обробку секретної інформації.

Допоміжні технічні засоби та системи (ДТЗС) – розташовані на об’єкті інформаційної діяльності технічні засоби та системи і їх комунікації, які не здійснюють обробку секретної інформації, але перебувають під впливом небезпечних сигналів основних технічних засобів або небезпечних акустичних полів.

Основні технічні засоби та системи є джерелом небезпечного сигналу, який може розповсюджуватись в просторі на досить великі

відстані і може бути перехопленим (знятим) засобами технічної розвідки противника поза межами контрольованої зони.

Однак поля (акустичні, вібраційні, електричні, магнітні, електромагнітні) при їх розповсюдженні мають властивість загасати. При цьому знайдеться така відстань від джерела небезпечного сигналу, на якій перехоплення (зняття) небезпечного сигналу та відтворення інформації стане неможливим. Цей принцип використовується практично в усіх пасивних системах захисту інформації від витоку технічними каналами. Так для акустичних джерел створюють акустичні зони, локалізують акустичну енергію звукоізолюючими огороджувальними конструкціями, а вібраційну – віброізолюючими вставками в середовище розповсюдження. Для ОТЗС визначають небезпечні зони 1 та 2.

Зона 2 – територія (сфера) навколо технічних засобів обробки інформації, за межами якої вважається неможливим перехоплення небезпечного сигналу з метою відтворення інформації, характеризується радіусом R2, що визначає найбільшу відстань від технічних засобів обробки інформації до межі, за якою напруженості електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення.

В Зоні 2 можливе перехоплення інформації, а за її межами ні.

Зона 1 – територія (сфера) навколо основних технічних засобів, в межах якої здійснюється наведення небезпечних сигналів на інші технічні засоби, системи та їх комунікації, характеризується радіусом R1, що визначає граничну відстань від основних технічних засобів до межі, за якою вважається неможливим наведення небезпечних сигналів на технічні засоби.

В межах зони 1 на ОІД під впливом небезпечного сигналу від ОТЗС знаходяться ДТЗС, лінії яких можуть виходити за межі ОІД або за межі контрольованої зони, або знаходяться сторонні провідники (наприклад: арматура залізобетонних конструкцій, стара електропроводка, тощо), які

виходять за межі контрольованої зони. Допоміжні технічні засоби та системи, а також сторонні провідники можуть виступати в ролі випадкових антен або середовищ поширення небезпечного сигналу. Цілком природно, що ДТЗС або сторонні провідники не будуть достатньо ефективними антенами, однак достатньо близьке розташування засобів технічної розвідки може призвести до витоку інформації. Тому технічні засоби та системи, а також сторонні провідники мають розташовуватися на ОІД поза Зоною 1.

Зона 1 та Зона 2 є фізичними характеристиками (показниками) ОТЗС та визначаються експериментально-розрахунковим методом при спеціальних дослідженнях ОТЗС.

Як правило радіус Зони 1 менший ніж радіус Зони 2.

Для неможливості перехоплення небезпечного сигналу у вигляді електромагнітних полів необхідно навколо ОІД організаційно створити і забезпечити контрольовану зону, найменша відстань до межи якої від ОТЗС має бути більшою за радіус Зони 2 (R2).

Контрольована зона (КЗ) – територія (простір) навколо об’єкта інформаційної діяльності, на якій (у межах якого) виключено несанкціоноване розташування технічних і транспортних засобів та неконтрольоване перебування сторонніх осіб.

2.2. Класифікація технічних каналів витоку інформації

Для встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками. Зокрема відокремлені типи ТКВІ за такими ознаками:

- за видом інформаційної діяльності на ОІД,
- за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації),
- за середовищем поширення небезпечного сигналу,

– за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ:

1) технічні канали витоку мовної інформації,
2) технічні канали витоку інформації, що обробляється в ОТЗС,
3) технічні канали витоку візуальної інформації,
4) матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за принципом (фізичним ефектом, процесом) формування небезпечного сигналу, середовищем поширення небезпечного сигналу та способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника доцільно розглянути у межах визначених вище типів ТКВІ.

Технічні канали витоку мовної інформації за цими ознаками поділяються на такі:

1. Акустичні канали.
2. Акустовібраційні (віброакустичні) канали.
3. Акустооптоелектронні (лазерні акустичні) канали.
4. Акустоелектричні канали.
5. Відеоакустичні канали.
6. Канали ВЧ нав’язування (для зняття мовної інформації).
7. Канали витоку мовної інформації на основі закладних пристроїв.

Технічні канали витоку інформації, що обробляється в ОТЗС, поділяються на такі:

1. Канали побічних електромагнітних випромінювань.
2. Канали побічних електромагнітних наведень.
3. Канали “паразитної” модуляції сигналів ВЧ генераторів.
4. Канали “паразитної” ВЧ генерації підсилювачів.
5. Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.

6. Канали перехоплення (зняття) інформації з каналів зв’язку.

7. Канали ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).

8. Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на такі:

1. Візуальні канали.

2. Візуально оптичні канали.

3. Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації:

1. Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.

2. Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.

3. Хімічні канали.

За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі ТКВІ:

електромагнітні канали витоку інформації, до яких відносяться канали побічних електромагнітних випромінювань, канали “паразитної” ВЧ генерації підсилювачів, канали “паразитної” модуляції ВЧ генераторів, канали перехоплення інформації з ліній радіо- (радіорелейного, стільникового, мобільного) зв’язку та тому подібні;

електричні канали витоку інформації, до яких відносяться канали побічних електромагнітних наведень на комунікації, канали зняття інформації з ліній провідного зв’язку та тому подібні;

параметричні канали витоку інформації, до яких відносяться, канали ВЧ нав’язування, канали “паразитної” модуляції та тому подібні.

За місцем перехоплення інформації засобами технічної розвідки противника відокремлюються такі типи ТКВІ:

1) канали перехоплення (зняття) інформації за межами КЗ,

2) канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації (наприклад, канал ВЧ нав'язування),

3) канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Розглянута класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про них та встановити вимоги і заходи щодо захисту інформації від витоку відповідними ТКВІ.

Перелік питань для самоконтролю

1. Що розуміють під витоком інформації?
2. Що таке небезпечний сигнал?
3. Визначення технічному каналу витоку інформації.
4. Визначення ОТЗС, ДТЗС.
5. Визначення Зони 1, Зони 2, контрольованої зони.
6. Що може бути носієм інформації?
7. За якими ознаками класифікують технічні канали витоку інформації?
8. Класифікація технічних каналів витоку мовної інформації.
9. Класифікація технічних каналів витоку інформації, що обробляється в ОТЗС.
10. Класифікація технічних каналів витоку видової інформації.
11. Класифікація матеріально-речовинних каналів витоку інформації.

2.3. Сутність та шляхи утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами

Розглянемо сутність та шляхи (фізичні основи, принципи та порядок) утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами. Найнебезпечнішими для витоку інформації, що обробляється в ОТЗС, є канали побічних електромагнітних випромінювань та наведень (канали ПЕМВН).

2.3.1. Канал побічних електромагнітних випромінювань ОТЗС

Канал побічних електромагнітних випромінювань ОТЗС (канал ПЕМВ ОТЗС) утворюється шляхом перехоплення приймачами засобів технічної розвідки побічних електромагнітних полів, які формуються навколо електронних елементів та провідників (шлейфів) ОТЗС при проходженні ними інформаційних сигналів та поширення цих полів за межі контрольованої зони.

Інформаційними сигналами у даному випадку є електричні струми, що несуть інформацію.

Обробка та передача інформації в ОТЗС здійснюється за допомогою електричних струмів провідності, що представляють собою спрямований потік заряджених частинок – електронів. Як відомо з фізики, навколо нерухомих електронів чи групи електронів завжди присутнє електростатичне поле. Якщо ж цей заряд привести до руху, то в полі виникає магнітна складова і воно стає електромагнітним. Електромагнітне поле розповсюджується в просторі.

Навколо ОТЗС, як системи електронних елементів та провідників (шлейфів), в яких відповідно з принципом основної дії ОТЗС циркулюють

електричні струми, що несуть інформацію, завжди присутні поля випромінювання. Оскілки ці випромінювання небажані та носять паразитичний (побічний) характер, їх називають побічними електромагнітними випромінюваннями (ПЕМВ). Побічні електромагнітні випромінювання поширюються у вільному просторі і можуть бути перехоплені за межами КЗ приймачами засобів технічної розвідки противника, таким чином утворюється канал ПЕМВ ОТЗС (рис. 2.3).

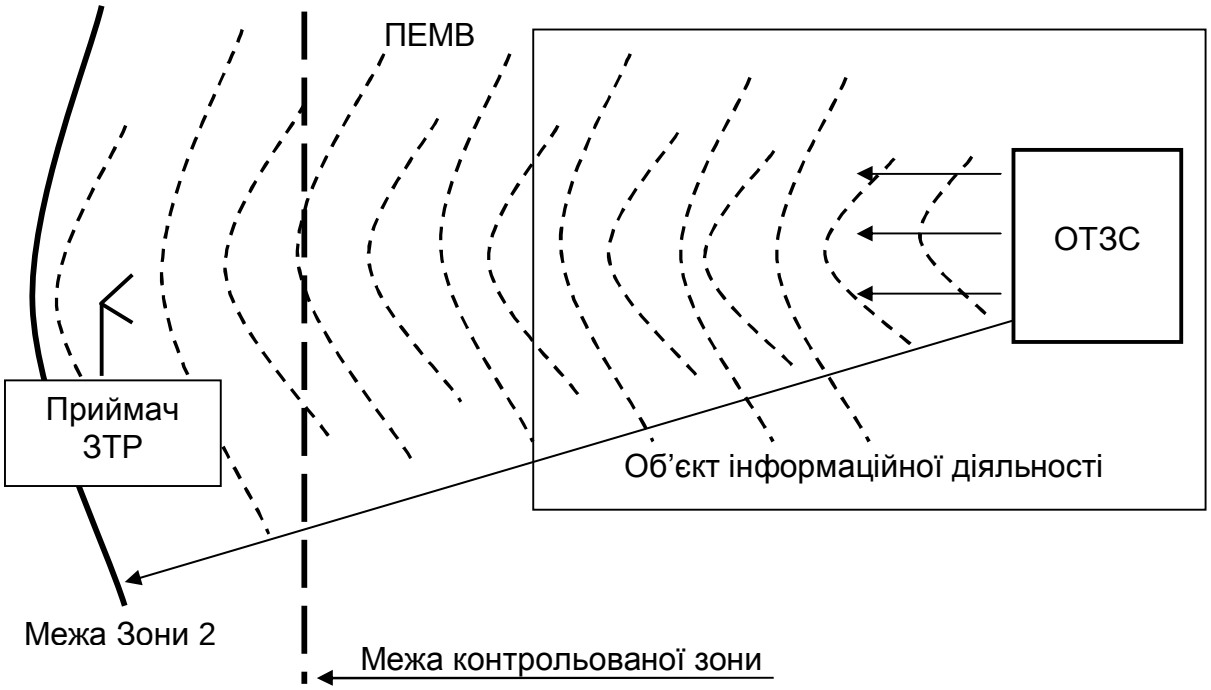


Рис. 2.3. Канал побічних електромагнітних випромінювань ОТЗС.

З фізики також відомо, що при поширенні електромагнітного поля воно загасає. Тому є така відстань від джерела випромінювання – ОТЗС, на якій поле випромінювання згасне до рівня, при якому стає неможливим його приймання (виявлення та вимірювання його параметрів). При цьому небезпечний сигнал, що несеться цим полем, буде, практично, зруйнований звичайними завадами та шумами. Як вже відмічалося раніше, простір, за межами якого відношення сигналу до завади не перевищує допустиму норму, є Зоною 2 даного ОТЗС.

Розташування приймачів ЗТР противника за межами Зони 2 не дасть можливості перехоплення інформації.

Запобігання витоку інформації каналом ПЕМВ ОТЗС (унеможливлення створення такого ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗ та на ОІД;

– екранування ОТЗС або локального екранування електронних елементів та провідників (шлейфів) ОТЗС, зменшення довжини провідників (шлейфів) ОТЗС;

– просторового електромагнітного зашумлення на об’єкті ЕОТ.

2.3.2. Канал побічних електромагнітних випромінювань ДТЗС

Канал побічних електромагнітних випромінювань ДТЗС, як різновид каналів ПЕМВ, утворюється шляхом перехоплення приймачами засобів технічної розвідки за межами КЗ небезпечних сигналів у вигляді побічних електромагнітних полів ОТЗС, які перевипромінюються допоміжними технічними засобами та системами, а також сторонніми провідниками (рис. 2.4).

Допоміжні технічні засоби та системи, а також сторонні провідники, якщо вони знаходяться в зоні 1 ОТЗС або мають спільні пробіги з лініями, якими поширюються небезпечні сигнали (в тому числі сигнали побічних електромагнітних наведень) ОТЗС, є випадковими антенами і можуть призвести до витоку інформації небезпечними сигналами, наведеними на них побічними електромагнітними випромінюваннями основних технічних засобів та систем.

Запобігання витоку інформації каналом побічних електромагнітних випромінювань ДТЗС (унеможливлення створення такого ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗ на ОІД;

– розташування ДТЗС та сторонніх провідників поза Зоною 1 ОТЗС;

– екранування ОТЗС;

– екранування ДТЗС;

– просторового електромагнітного зашумлення на об’єкті ЕОТ.

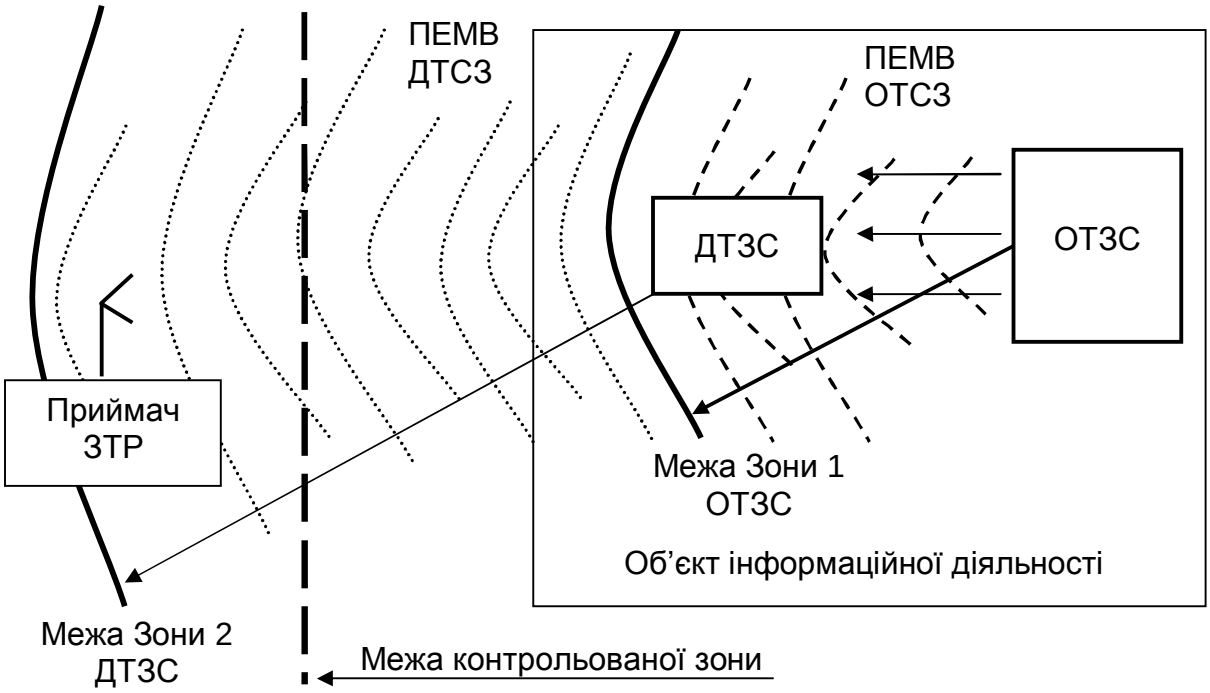


Рис. 2.3. Канал побічних електромагнітних випромінювань ДТЗС.

2.3.3. Канал “паразитної” модуляції сигналів ВЧ генераторів

Канал “паразитної” модуляції сигналів ВЧ генераторів, як різновид каналів ПЕМВ, утворюється шляхом модуляції небезпечним сигналом високочастотних сигналів ВЧ генераторів ОТЗС, випромінювання модульованих ВЧ коливань у вільний простір та перехоплення таких коливань радіоприймальними пристроями засобів технічної розвідки за межами КЗ (рис. 2.4).

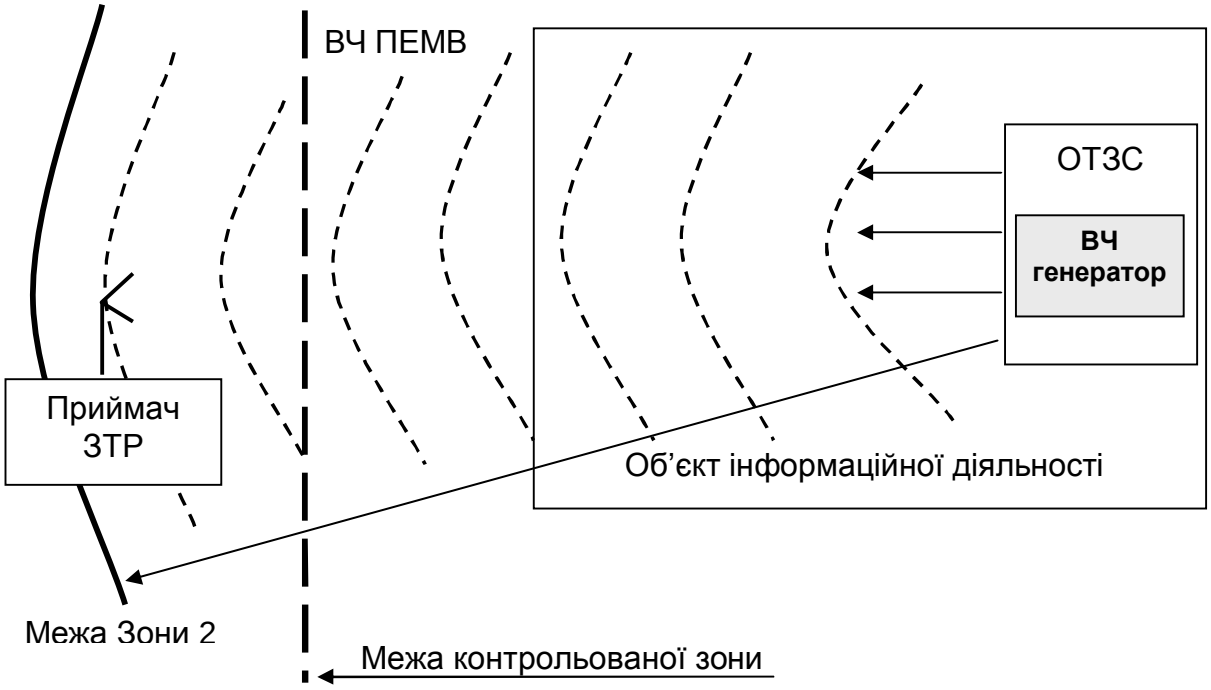


Рис. 2.4. Канал “паразитної” модуляції сигналів ВЧ генераторів.

Основні технічні засоби та системи в своєму складі мають генератори високих частот (ВЧ генератори). Практично всі засоби ЕОТ в своєму складі мають генератори тактових частот, гетеродини та інші ВЧ генератори. Високочастотний сигнал ВЧ генератора модулюється низькочастотними небезпечними сигналами, що циркулюють в ОТЗС, та випромінюється у вигляді електромагнітного поля у вільний простір. Оскільки згасання електромагнітного поля на високих частотах менше ніж на низьких, то поле розповсюджується дальше. А це, в свою чергу, дає можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої для сигналу без модуляції. Слід відмітити, що модуляція розширює спектр частот сигналу, підвищує його потужність і завадостійкість. Тому Зона 2 має розраховуватись з врахуванням модульованого випромінювання на частотах ВЧ генераторів ОТЗС.

Запобігання витоку інформації каналом “паразитної” модуляції сигналів ВЧ генераторів (унеможливлення створення такого ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2, яка розрахована з врахуванням паразитної модуляції небезпечним сигналом коливань ВЧ генераторів ОТЗС, та організації режиму доступу до КЗ та на ОІД;

– екранування ОТЗС або унеможливлення “паразитної” модуляції сигналів ВЧ генераторів ОТЗС (локальне екранування ВЧ генераторів, оцінювання випромінювань та блокування роботи ОТЗС у разі виявлення “паразитної” модуляції тощо);

– просторового електромагнітного зашумлення на об’єкті ЕОТ.

2.3.4. Канал “паразитної” ВЧ генерації підсилювачів

Канал “паразитної” ВЧ генерації підсилювачів, як різновид каналів ПЕМВ, утворюється шляхом самозбудження підсилювачів низької частоти (НЧ) ОТЗС на гармоніках, кратних небезпечному сигналу, поширення їх у вигляді поля електромагнітного випромінювання за межі КЗ та перехоплення цього поля радіоприймальними пристроями засобів технічної розвідки (рис. 2.5).

Сучасні технічні засоби обробки інформації в своєму складі часто мають підсилювачі низької частоти (НЧ). Як правило, буд-який підсилювач складається безпосередньо з підсилювального (напівпровідникового) елементу та негативного зворотного зв’язку. Нелінійність характеристик напівпровідникових елементів при підсиленні сигналів обумовлює наявність в суміші вихідного підсиленого сигналу кратних гармонік, тобто небезпечного сигналу на подвоєних, потроєних і так далі частотах. Якщо підсилювач з його негативним зворотнім зв’язком правильно розрахований, і підсилення здійснюється на лінійній

ділянці характеристики підсилення, то сам сигнал підсилюється практично без спотворень і його кратні гармоніки мінімальні.

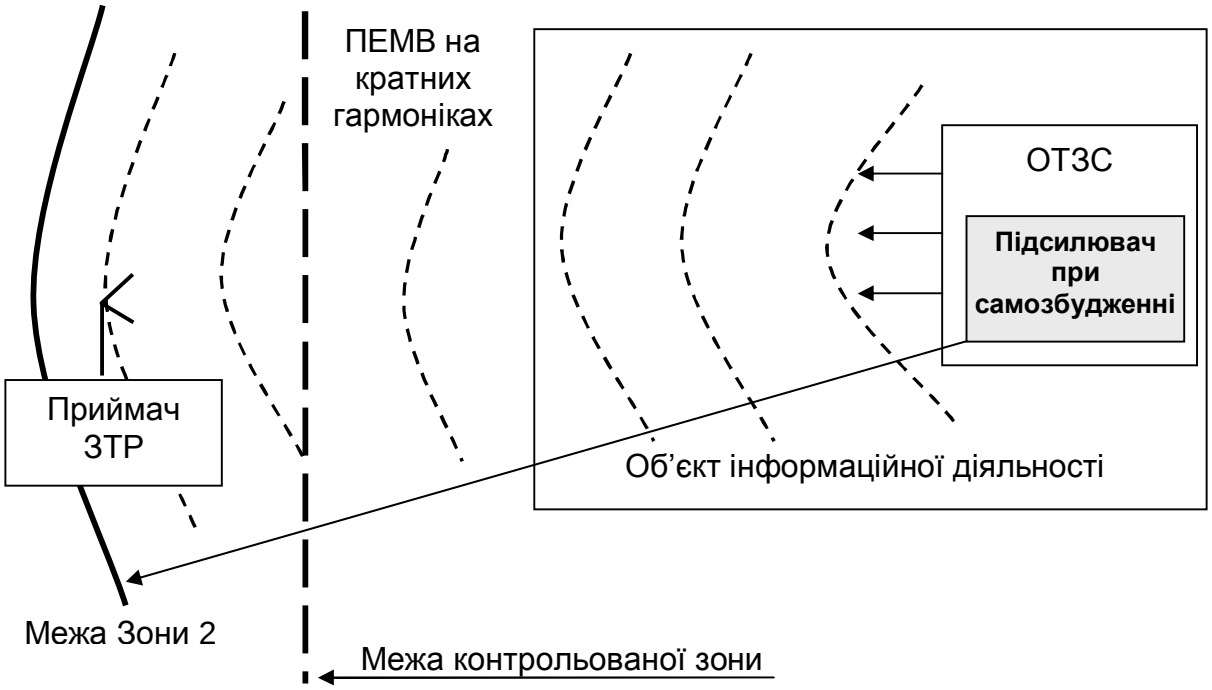


Рис. 2.5. Канал “паразитної” ВЧ генерації підсилювачів.

У результаті старіння чи інших причин параметри електронних елементів та характеристики негативного зворотного зв'язку можуть змінитись і призвести до порушення режиму роботи самого підсилювача вцілому. Негативний зворотній зв'язок може змінюватися в бік позитивного, коефіцієнт підсилення збільшується і, разом з цим, зростає нелінійність підсилення, підсилювальний елемент переходить в режим насичення. Зворотній зв’язок на деяких частотах стає позитивним, і підсилювач перетворюється в генератор. При цьому в режимі насичення кратні гармоніки сигналу можуть суттєво зростати, а їх поле електромагнітного випромінювання може досягти значного рівня. А це, в свою чергу, може дати можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої без врахування “паразитної” генерації.

Ефект “паразитної” генерації характеризується нерегулярністю появи, тому одним із способів запобігання витоку інформації таким каналом є своєчасне виявлення (індикація) сигналів “паразитної” генерації та блокування роботи ОТЗС.

Запобігання витоку інформації каналом “паразитної” ВЧ генерації підсилювачів (унеможливлення створення такого ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2, яка розраховується з врахуванням небезпечного сигналу на кратних гармоніках підсилювачів, організації режиму доступу до КЗ на ОІД;

– екранування ОТЗС, унеможливлення “паразитної” ВЧ генерації підсилювачів ОТЗС (локального екранування підсилювачів, оцінювання випромінювань та блокування роботи ОТЗС у разі виявлення “паразитної” ВЧ генерації, оцінювання, індикації та сигналізації відхилення параметрів підсилювачів та блокування роботи ОТЗС при виявленні позитивного зворотного зв’язку тощо);

– просторового електромагнітного зашумлення на об’єкті ЕОТ.

2.3.5. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС

Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС, як різновид каналів побічних електромагнітних наведень (каналів ПЕМН), утворюється шляхом безпосереднього зняття з ліній електроживлення (заземлення) ОТЗС засобами технічної розвідки за межами КЗ небезпечних електричних сигналів, що наводяться в цих лініях побічними електромагнітними полями ОТЗС та/або просочуються (стікають) в ці лінії (або виникають в лінії електроживлення через нерівномірність споживання електроенергії)

при функціонуванні ОТЗС (рис. 2.6).

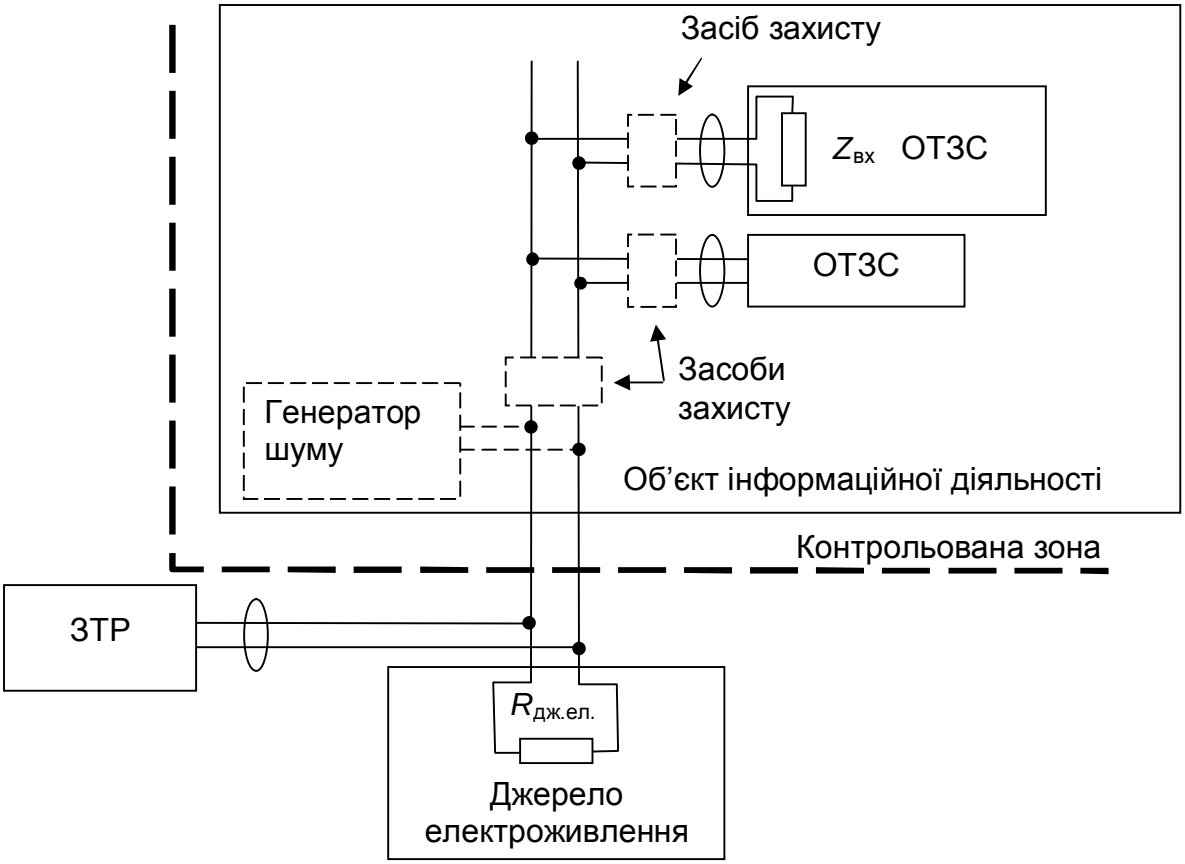


Рис. 2.6. Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС.

Практично всі технічні засоби та системи обробки та передачі інформації живляться електричною енергією. Лінії електроживлення (заземлення) даних ОТЗС знаходяться в Зоні 1 ОТЗС, тому на них може наводитися за принципом електромагнітної індукції електричний струм, якій змінюється аналогічно небезпечному електромагнітному сигналу, і поширюється лініями електроживлення (заземлення). Також під час обробки інформації вхідний опір ОТЗС може змінюватись за законом сигналів, що обробляються в них. Так, наприклад, підсилювачі (ключові схеми) працюють так, що вхідний (управляючий) сигнал управляє в схемі опором напівпровідника, який формує від джерела живлення підсилений сигнал. В результаті коливання вхідного опору ОТЗС в ланцюгу електроживлення з'явиться змінна складова небезпечного сигналу по

струму, яка на власному опорі джерела електроживлення створюватиме змінну складову напруги. Остання може стати доступною всім абонентам цієї мережі електроживлення, а якщо джерело електроживлення знаходиться за межами КЗ (лінії електроживлення виходять за межи КЗ), то противник може зняти інформацію шляхом безпосереднього підключення засобів технічної розвідки до лінії електроживлення.

Крім побічних електромагнітних наведень на лінію заземлення ОТЗС має місце просочування небезпечних сигналів в ланцюги заземлення.

Під час роботи технічних засобів обробки інформації в наслідок ємнісних та інших зв'язків на корпусах цих засобів може накопичуватися небезпечний для життя потенціал. Цей потенціал може змінюватися за законом небезпечного сигналу, і небезпечний сигнал просочується в ланцюги заземлення.

Для забезпечення безпеки життєдіяльності персоналу всі технічні засоби заземлюються. Сутність заземлення полягає у тому, що корпус технічного засобу гальванічно зв’язується з ґрунтом "Землі" і потенціал, який накопився на корпусі, ланцюгами заземлення стікає в ґрунт, приймаючи його нульовий потенціал. Якщо система заземлення надійна і опір її досить малий, то стікання буде проходити швидше і корпус технічного засобу обробки інформації практично постійно буде нейтрально зарядженим.

Однак на практиці система заземлення не завжди може мати потрібний опір і противник може цим скористатися. Технічний канал витоку інформації ланцюгами заземлення ОТЗС наведений на рис. 2.7.

Основні способи перехоплення небезпечних сигналів в ланцюгах заземлення:

1. Перехоплення небезпечного сигналу з низькоомних ділянок ланцюга заземлення. Наприклад, слабко зварювальний шов, окислення контактів, мала площа перетину шини заземлення, тощо.

2. Зняття різниці потенціалів ґрунту по віддаленню від заземлювача – джерела небезпечного сигналу, що можливе у разі великого опору заземлення.

3. Зняття потенціалу зі сторонніх провідників, що близько розташовані з заземлювачем та мають з ним ємнісний зв'язок.

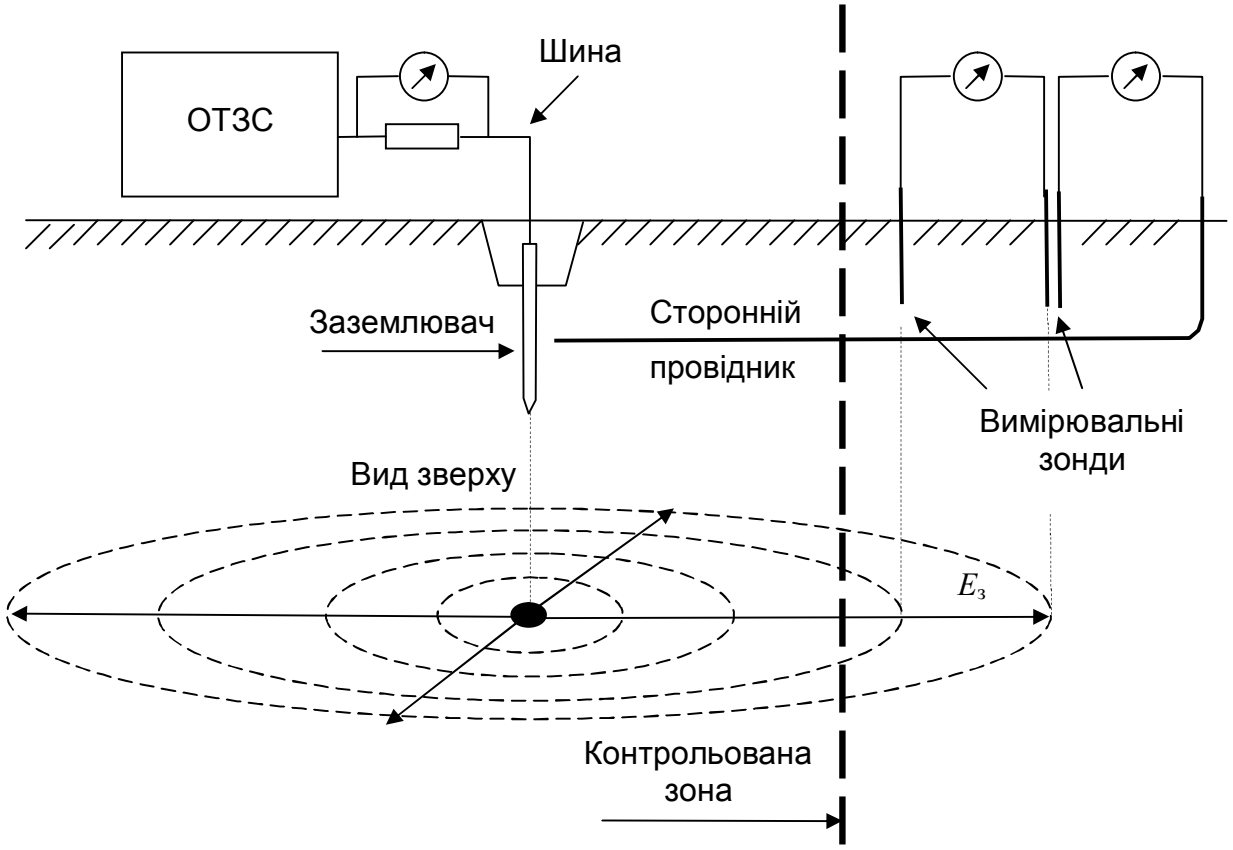


Рис. 2.7. Технічний канал витоку інформації ланцюгами заземлення ОТЗС.

Запобігання витоку інформації каналами побічних електромагнітних наведень на лінії електроживлення ОТЗС (унеможливлення створення таких ТКВІ) досягається шляхом:

– створення КЗ та організації режиму доступу до КЗ на ОІД;

– електроживлення ОТЗС від автономних електричних джерел: електростанцій, акумуляторів, тощо, що розташовані у межах КЗ та не мають сторонніх споживачів;

– використання в лінії електроживлення ОТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів, систем двигун-генератор;

– використання лінійного зашумлення ліній електроживлення ОТЗС.

Запобігання витоку інформації каналами побічних електромагнітних наведень на лінії заземлення ОТЗС, включаючи просочування небезпечних сигналів в ланцюги заземлення, (унеможливлення створення таких ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗ на ОІД;

– автономного від ДТЗС заземлення ОТЗС;

– забезпечення вимог щодо монтажу та опору заземлення ОТЗС;

– розташовування заземлювача з шинами заземлення в межах контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;

– використання лінійного зашумлення ліній заземлення ОТЗС.

2.3.6. Канал побічних електромагнітних наведень на комунікації ДТЗС

Канали побічних електромагнітних наведень на комунікації ДТЗС, як різновид каналів ПЕМН, утворюється шляхом безпосереднього зняття з комунікацій ДТЗС (ліній електроживлення, заземлення та передачі даних ДТЗС, ліній зв’язку, ліній охоронних, протипожежних чи загальних систем безпеки, систем енергопостачання та інших систем) небезпечних електричних сигналів, що наводяться в цих комунікаціях побічними електромагнітними полями ОТЗС, полями комунікацій ОТЗС при їх

спільному пробігу з комунікаціями ДТЗС (рис. 2.8).

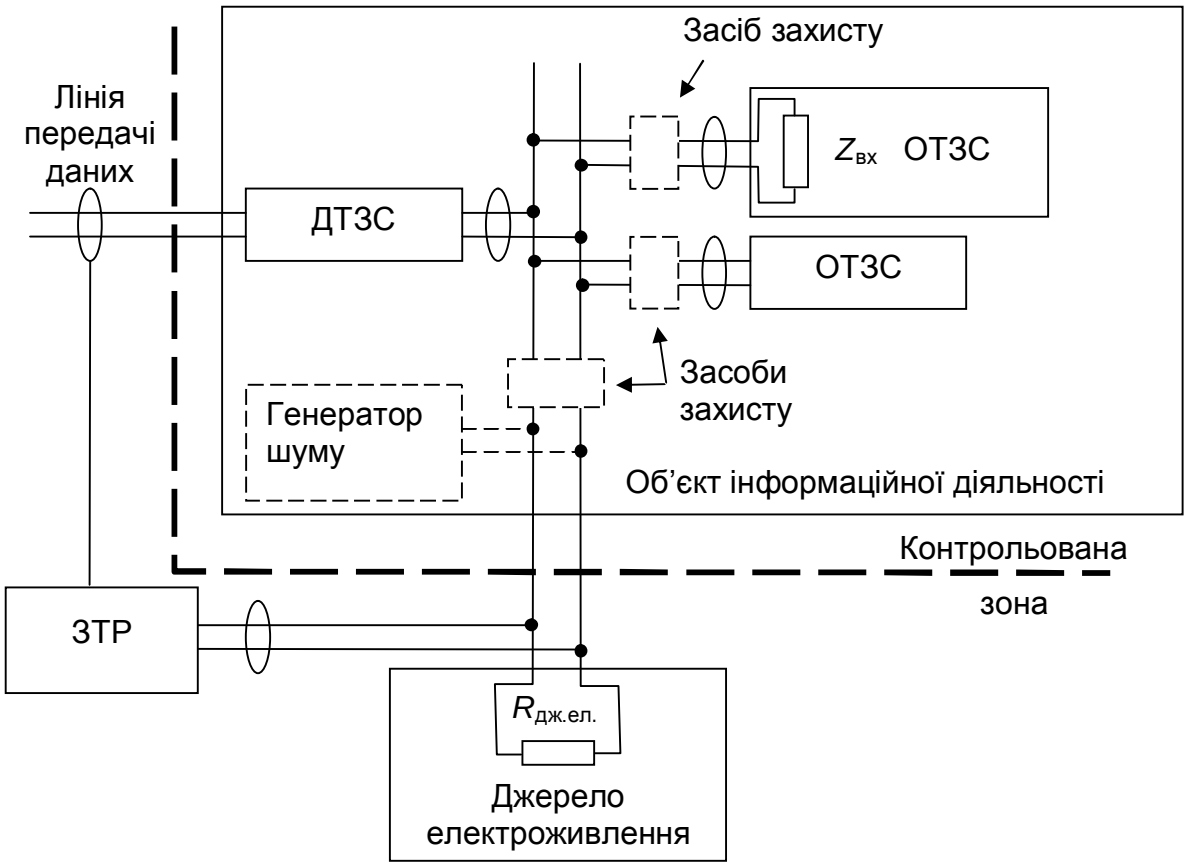


Рис. 2.8. Канали побічних електромагнітних наведень на комунікації ДТЗС.

Якщо ДТЗС та їх лінії електроживлення, заземлення та передачі даних знаходяться в Зоні 1 ОТЗС, то на них може наводитися за принципом електромагнітної індукції електричний струм, якій змінюється аналогічно небезпечному сигналу, і поширюється лініями електроживлення, заземлення та передачі даних ДТЗС. Також, якщо ці лінії мають спільні пробіги з лініями, якими поширюються небезпечні сигнали, то можливі перенаведення небезпечних сигналів на лінії ДТЗС. Крім того, небезпечні сигнали через ланцюги живлення ДТЗС можуть просочуватися в лінії живлення ДТЗС. Якщо такі лінії електроживлення, заземлення або передачі даних ДТЗС виходять за межі КЗ, то противник

може зняти інформацію шляхом безпосереднього підключення засобів технічної розвідки до цих ліній.

Запобігання витоку інформації каналами побічних електромагнітних наведень на комунікації ДТЗС (унеможливлення створення таких ТКВІ) досягається шляхом:

– створення КЗ та організації режиму доступу до КЗ на ОІД;

– розташування ДТЗС та їх комунікацій за межами Зони 1 ОТЗС;

– електроживлення ДТЗС від автономних електричних джерел: електростанцій, акумуляторів, тощо, що розташовані у межах КЗ;

– використання в лінії електроживлення ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів, систем двигун-генератор;

– використання лінійного зашумлення ліній електроживлення ДТЗС;

– забезпечення вимог щодо монтажу та опору заземлення ДТЗС;

– розташовування заземлювача з шинами заземлення в межах контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;

– використання лінійного зашумлення ліній заземлення ДТЗС.

2.3.7. Канал ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС)

Канал ВЧ нав’язування (для зняття інформації, що обробляється технічними засобами), як різновид параметричних каналів, утворюється шляхом введення (“нав’язування”) спеціально створеного високочастотного сигналу (ВЧ-сигналу) в основні та/або допоміжні технічні засоби та системи їх комунікаціями з-за меж контрольованої зони, модуляції цього ВЧ-сигналу небезпечним сигналом на нелінійних елементах ОТЗС та/або ДТЗС та

– або відбиття цього ВЧ-сигналу від неузгоджених навантажень в ОТЗС та/або ДТЗС, поширення такого модульованого ВЧ-сигналу комунікаціями ОТЗС та/або ДТЗС за межі КЗ та його зняття засобами технічної розвідки при безпосередньому їх підключенні до комунікацій ОТЗС та/або ДТЗС за межами КЗ;

– або випромінювання такого модульованого ВЧ-сигналу у вільний простір та перехоплення такого випромінювання радіоприймальними засобами технічної розвідки за межами КЗ (рис. 2.9).

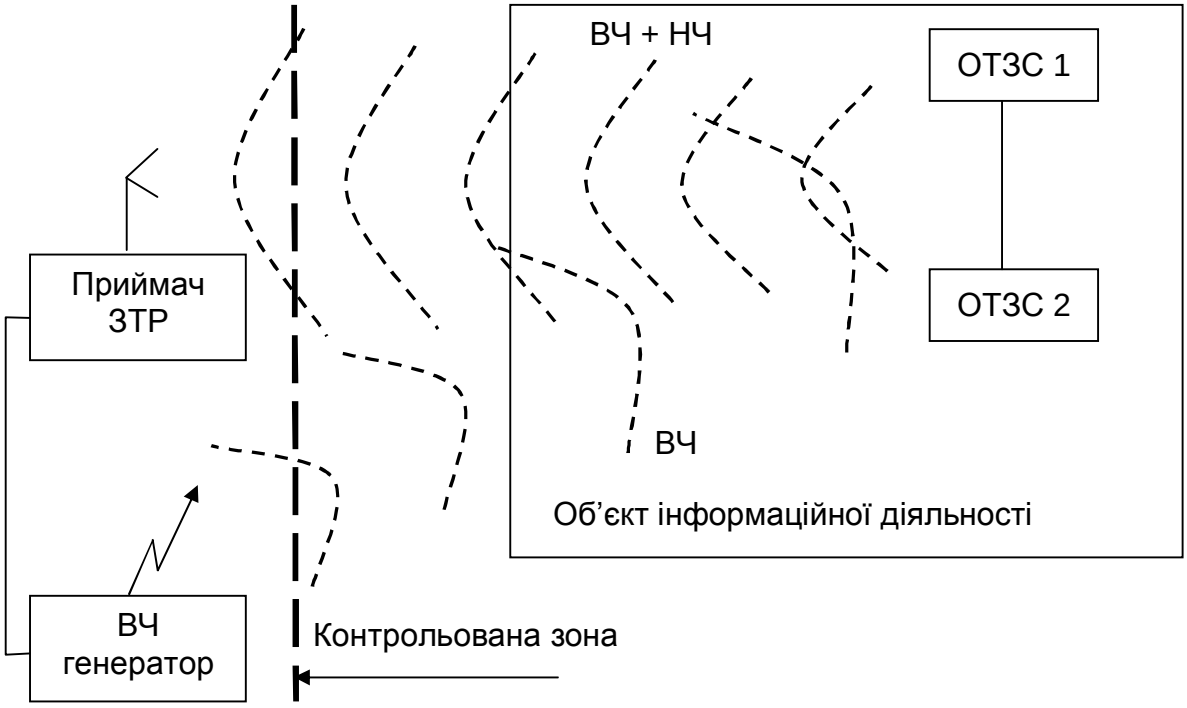


Рис. 2.9. Канал ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).

Майже всі технічні засоби обробки інформації використовують напівпровідникові електронні елементи, провідність (опір) яких залежить від різниці потенціалів на їх полюсах. Якщо опромінити технічні засоби обробки інформації електромагнітним полем високої частоти (в мегагерцовому діапазоні), то в його ланцюгах, де циркулює небезпечний сигнал, з’являться наведені ВЧ струми, які, в свою чергу, впливатимуть на опори напівпровідників та інші параметри схем ТЗС. В результаті в

схемах здійсниться паразитна модуляція небезпечного сигналу з переносом його спектру ВЧ область. Перевипромінювання такого модульованого ВЧ сигналу може спричинити витік інформації.

Слід відмітити, що при цьому досить просто реалізувати перехоплення такого модульованого ВЧ сигналу, використавши когерентний прийомом, який забезпечує максимум завадостійкості.

Запобігання витоку інформації каналом ВЧ нав'язування (унеможливлення створення такого ТКВІ) досягається шляхом:

– створення КЗ не меншої за Зону 2, яку розраховують з врахуванням можливого ВЧ нав'язування, та організації режиму доступу до КЗ на ОІД;

– екранування ОТЗС;

– просторового електромагнітного зашумлення на об'єкті ЕОТ;

– індикації, сигналізації поля ВЧ опромінення та блокування роботи ОТЗС.

Таким чином у пункті 2.3 розглянуті основні різновиди технічних каналів витоку інформації, які утворюються при її обробці в ОТЗС та основні заходи щодо запобігання витоку інформації цими каналами (унеможливлення створення таких ТКВІ).

В цілому способами запобігання витоку інформації, що обробляється в ОТЗС, та унеможливлення створення ТКВІ з врахуванням розглянутих ефектів є:

– створення КЗ не меншої за найбільшу Зону 2, яку розраховують з врахуванням усіх властивих об'єкту ЕОТ технічних каналів витоку інформаці;

– організація режиму доступу до КЗ та ОІД;

– екранування ОТЗС;

– просторове електромагнітне зашумлення на об'єкті ЕОТ;

– індикація відхилення параметрів підсилювачів та блокування роботи ОТЗС;

– розміщення ДТЗС не ближче Зони 1 ОТЗС, а ОТЗС – на ближче своєї Зони 1 до можливих сторонніх провідників;

– використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня;

– використання в лініях ДТЗС та сторонніх провідниках лінійного зашумлення;

– живлення ОТЗС від автономних електричних джерел: електростанцій, акумуляторів;

– використання в ланцюгу живлення ОТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів;

– використання в ланцюгу живлення ОТЗС лінійного зашумлення;

– автономне заземлення ОТЗС;

– забезпечення вимог щодо монтажу на опору заземлення ОТЗС;

– розташовування заземлювача з шинами заземлення в межах контрольованої зони на максимальній відстані від границі КЗ та сторонніх провідників;

– зашумлення ліній заземлення ОТЗС та ДТЗС.

Перелік питань для самоконтролю

Сутність та шляхи утворення каналу побічних електромагнітних випромінювань ОТЗС.

Сутність та шляхи утворення каналу побічних електромагнітних випромінювань ДТЗС.

Сутність та шляхи утворення каналу “паразитної” модуляції сигналів ВЧ генераторів.

Сутність та шляхи утворення каналу “паразитної” ВЧ генерації підсилювачів.

Сутність та шляхи утворення каналу побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС.

Сутність та шляхи утворення каналу побічних електромагнітних наведень на комунікації ДТЗС.

Сутність та шляхи утворення каналу ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).

Способи запобігання витоку інформації каналом побічних електромагнітних випромінювань ОТЗС.

Способи запобігання витоку інформації каналом побічних електромагнітних випромінювань ДТЗС.

Способи запобігання витоку інформації каналом “паразитної” модуляції сигналів ВЧ генераторів.

Способи запобігання витоку інформації каналом “паразитної” ВЧ генерації підсилювачів.

Способи запобігання витоку інформації каналом побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС.

Способи запобігання витоку інформації каналом побічних електромагнітних наведень на комунікації ДТЗС.

Способи запобігання витоку інформації каналом ВЧ нав’язування (для зняття інформації, що обробляється в ОТЗС).

2.4. Технічні канали витоку мовної інформації

Розглянемо сутність та шляхи (фізичні основи, принципи та порядок) утворення технічних каналів витоку мовної інформації. Найнебезпечнішими для витоку мовної інформації є акустооптоелектронні (лазерні акустичні) канали.

Дуже часто, функціонування об’єктів інформаційної діяльності пов’язане з циркуляцією в них акустичної мовної інформації. Наприклад, проведення закритих засідань (нарад, семінарів, конференцій, занять тощо), а також спілкування обслуговуючого персоналу ОТЗС при проведенні обслуговуючих робіт, де, як правило, джерелом акустичного небезпечного сигналу є людина.

Власне звук має таку природу. Коливання голосових зв'язок спричиняє механічне коливання молекул повітряного середовища, яке розповсюджується у просторі завдяки збудженню до коливання сусідніх молекул. Такого типу коливання називають акустичним коливанням, а його розповсюдження – акустичною хвилею. Розповсюдження акустичних хвиль від джерела небезпечного сигналу за межі контрольованої зони спричиняє витік інформації.

Для акустичних коливань середовища розрізняють на два типи:

– дифузійне середовище (повітря, рідина), в якому молекули не мають пружних зв’язків;

– пружне середовище (тверде тіло, або система зв’язаних між собою твердих тіл), молекули якого жорстко та структурно зв’язані між собою.

Якщо канали витоку інформації утворились в наслідок розповсюдження акустичних хвиль тільки в дифузійному середовищі, то такі канали називають **акустичними каналами витоку**. Канали ж витоку, що утворилися в результаті розповсюдження акустичних хвиль в

пружному середовищі називають **акустовібраційними (віброакустичними) каналами витоку інформації**.

2.4.1. Акустичні канали витоку інформації

Акустичні канали утворюється шляхом перехоплення мовних сигналів (акустичних полів) з ОІД акустичними мікрофонами направленої дії чи акустичними антенами засобів технічної розвідки, що встановлюються за межами КЗ в зоні прямої видимості з вікон (з інших отворів) ОІД (рис. 2.10).

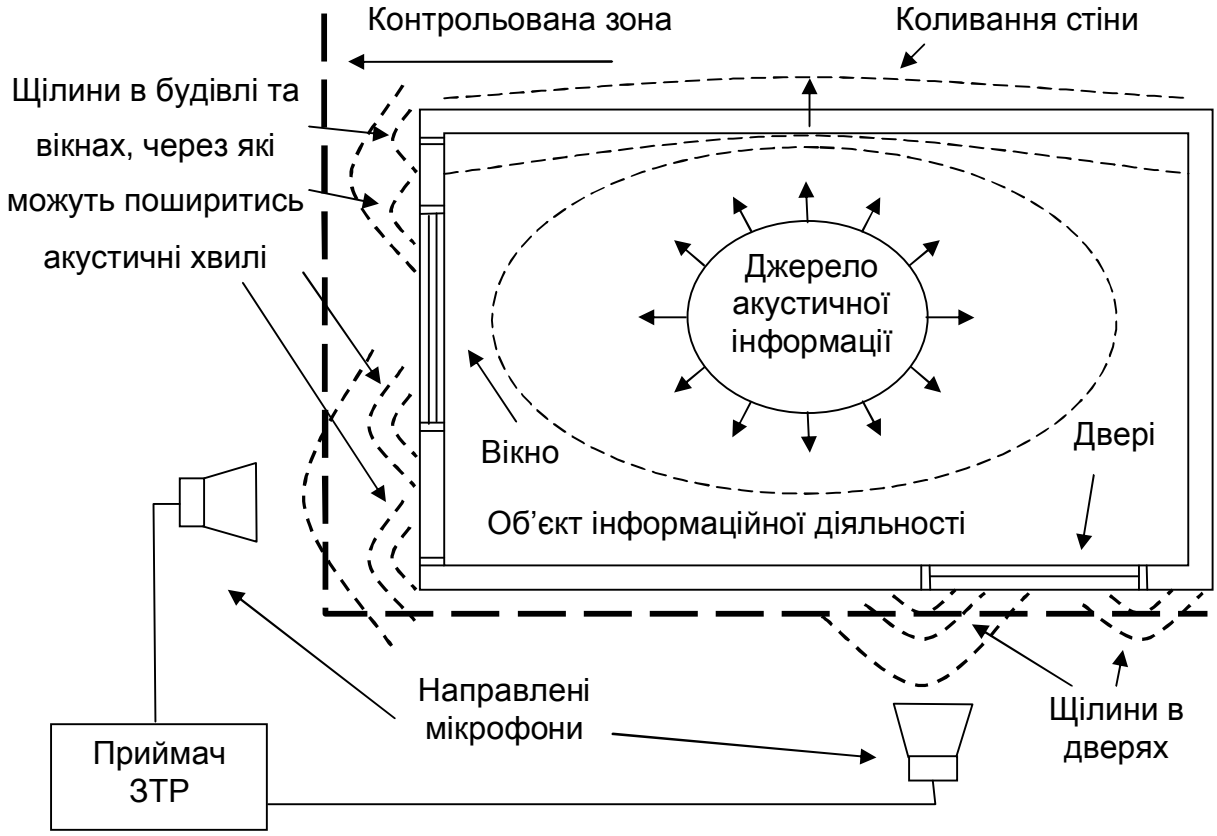


Рис. 2.10. Акустичні канали витоку інформації.

Нехай ОІД представляє собою приміщення, де огороджувальними конструкціями є стіни з вікнами та дверми, стеля та підлога.

Проходження акустичних хвиль через конструкції можливе по двом причинам.

1. Парусність огороджувальних конструкцій. Якщо стіна чи інша огороджувальна конструкція не достатньо масивна, то під дією акустичного тиску вона починає коливатися подібно мембрані акустичної системи та створювати звуковий тиск за межами ОІД.

2. Щілини (замкові отвори в дверях, зазори між дверми (рамами вікон) та коробкою), мікрощілини (тріщини швів панелей, штукатурки), технологічні вікна, вікна вентиляції, тощо. Прохід акустичної хвилі через щілину залежить від її розмірів та подовженості. Чим більша довжина щілини та менші її поперечні розміри по відношенню до довжини хвилі, тім більше її згасання. Великі пройми сприяють практично безперешкодному розповсюдженню акустичного сигналу. Якщо контрольована зона не велика, а інколи і обмежено стінами приміщення, противник може використати ЗТР з направленими мікрофонами те перехопити небезпечний сигнал.

Запобігання витоку інформації акустичним каналом (унеможливлення створення такого ТКВІ) досягається способами:

– використання таких огороджувальних конструкцій ОІД, щоб виключався ефект парусності (стіни, стеля та підлога повинні бути досить масивними: залізобетонними, цегляними, тощо);

– ліквідації щілин в огороджувальних конструкціях (шпаклювання тріщин, герметизація щілин звукоізолюючими матеріалами, тощо);

– використання в технологічних вікнах та системі вентиляції звукопоглинаючих резонаторів, систем та матеріалів;

– просторового акустичного зашумлення повітряного середовища зовні ОІД.

2.4.2. Акустовібраційні (віброакустичні) канали витоку інформації

Сутність акустовібраційних (вібролакустичних) каналів витоку полягає у тому, що акустична хвиля небезпечного сигналу, впливаючи на поверхню твердого матеріалу (пружного середовища), приводить його до вібрації – коливання його молекул, яке, в залежності від густини матеріалу може розповсюджуватись на досить великі відстані. Чим більша густина, тим більша дальність розповсюдження сигналу. Так на ОІД (рис. 2.11), де озвучується інформація, такими твердими тілами та пружними середовищами, є огороджувальні конструкції приміщення (стіни з дверям та вікнами, стеля, підлога) та всі інші предмети (система опалення, водопостачання та водовідведення, газопровід, тощо), що трапляються на шляху змінного акустичного тиску та які виходять за межі ОІД, або мають щільний контакт з предметами за межами ОІД.

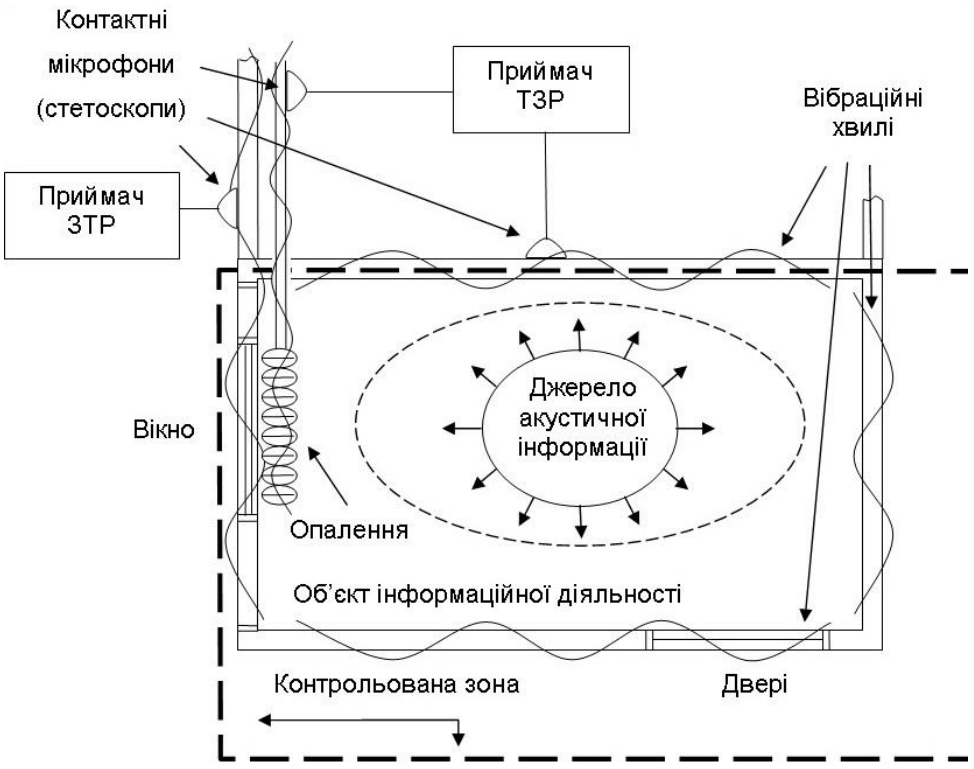


Рис. 2.11. Акустовібраційні канали витоку інформації

Запобігання витоку інформації акустовібраційним (віброакустичним) каналом (унеможливлення створення такого ТКВІ) досягається способами:

– покриття, штукатурки огороджувальних конструкції ОІД (стін, стелі, підлоги, дверей) звукопоглинаючими матеріалами та використання переважно звукопоглинаючих матеріалів та вібраційних розв'язок в побудові систем опалення, водопостачання, водовідведення, тощо;

– вібраційне зашумлення огороджувальних конструкції ОІД (стін, стелі, підлоги, дверей) та систем опалення, водопостачання, водовідведення, тощо.

2.4.3. Акустоелектричні канали витоку мовної інформації

Акустоелектричні канали витоку виникають в результаті паразитного перетворення акустичних сигналів в електричні на елементах ДТЗС за принципом мікрофонного ефекту (рис. 2.12).

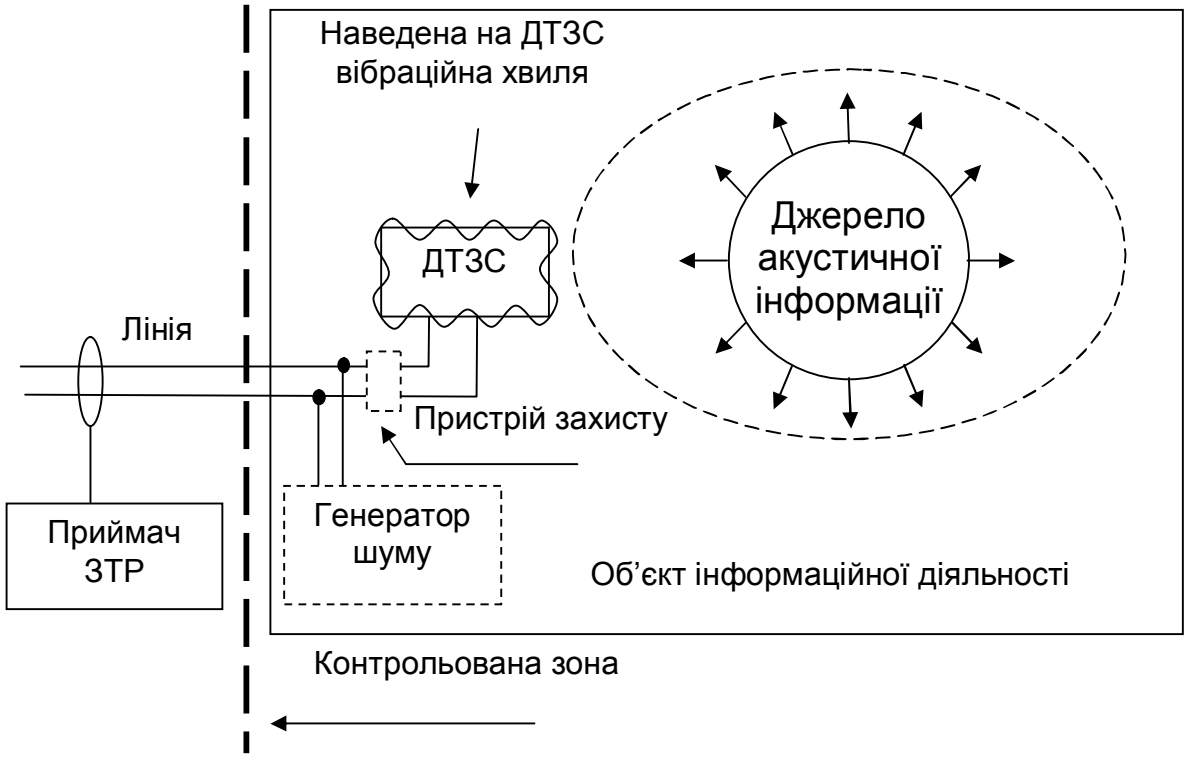


Рис. 2.12. Акустоелектричні канали витоку інформації.

Практично в усіх електронних елементах в тій чи іншій мірі проявляється ефект акустоелектричного перетворення. Розглянемо сутність мікрофонного ефекту на декількох прикладах.

1. Ефект акустоелектричного перетворення на прикладі електричного дзвінка телефонного апарату. Нехай на ОІД розташований телефонний апарат (ТА) місцевого зв'язку, лінії якого виходять за межі КЗ. При покладеній трубці переговорна частина ТА знаходиться у відключеному стані. До лінії постійно підключений лише приймач виклику – електромагнітний дзвінок (рис.2.13).

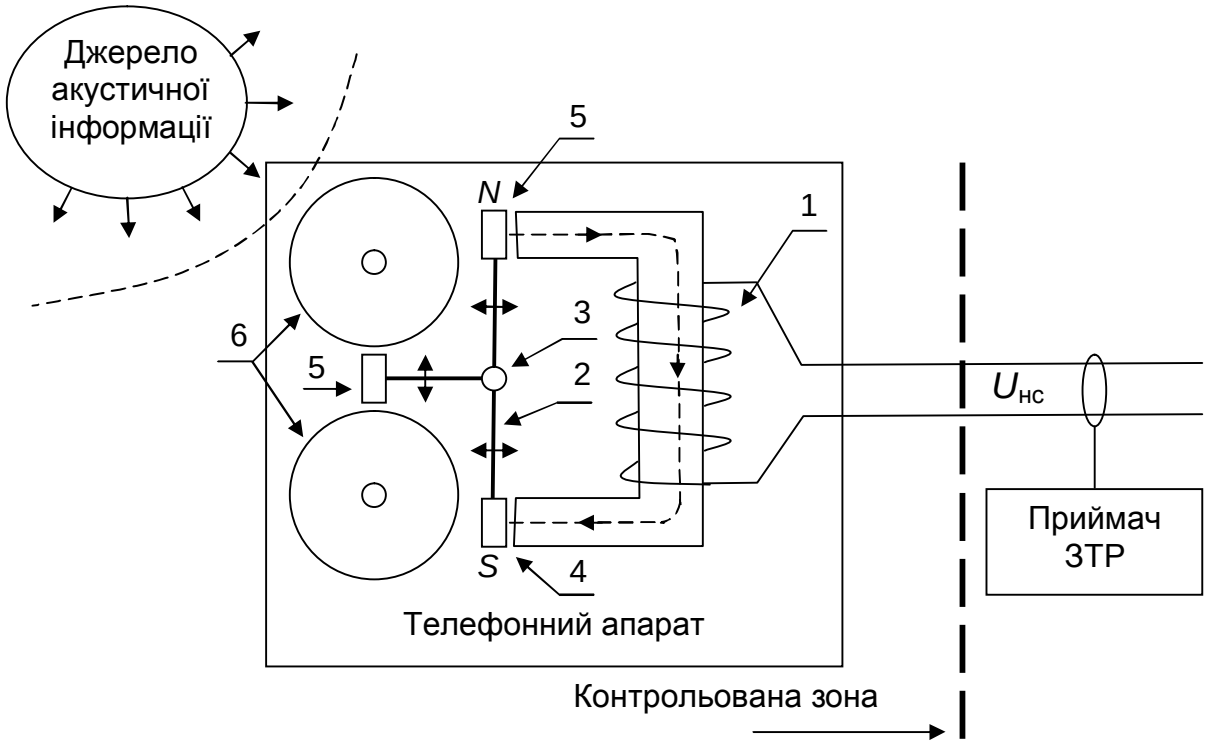


Рис. 2.13. Акустоелектричні перетворення у електричному дзвінку телефонного апарату.

Електромагнітний дзвінок складається з котушки індуктивності –1, якоря – 2, закріпленого на осі – 3 з намагніченими плечами – 4 та молоточком – 5, що б'є по дзвінковим чашечкам, та з самих дзвінкових чашечок – 6. При виклику абонента (трубка ТА покладена) на котушку індуктивності подається напруга змінного струму, яка створює магнітне поле та приводить до коливання якір. В результаті молоточок ударяє по

чашечкам, а ті, в свою чергу, виробляють дзвінковий акустичний сигнал. Якщо сигнал виклику не подається, то якір знаходиться в стані спокою.

Якщо на дзвінок впливає акустичний тиск від джерела небезпечного сигналу, то він призводить до вібрації всі складові дзвінка, що виготовлені з твердого тіла, в тому числі і якір, плечі якого мають остаточну намагніченість. Коливання пліч вносять в котушку змінне магнітне поле та наводять електрорушійну силу в його обмотках. Так виникає напруга небезпечного сигналу на полюсах дзвінка, яку противник може виміряти в лінії, що виходить за межі КЗ та ОІД, безпосередньо підключившись засобами технічної розвідки до лінії.

Такий ефект характерний також і для інших елементів, що містять котушки індуктивності. До них можна віднести реле, електромагніти (в годинниках), тощо.

2. Ефект акустоелектричного перетворення на прикладі конденсатора пристрою ДТЗС. Як правило, всі електронні схеми ТЗС містять конденсатори. Будь-яку схему ТЗС можна представити у виді схеми заміщення (рис. 2.14).

Якщо на конденсатор в схемі впливає акустичний тиск, то він приводить до вібрації пластинки конденсатора, в результаті чого поміж ними змінюється відстань та, відповідно, його ємність. Остання виражається формулою:

$$C \updownarrow = K \frac{S}{d \updownarrow},$$

де K – деякий коефіцієнт узгодження величин,

S – площа пластин конденсатора,

d – відстань між пластинами конденсатора.

В результаті коливання ємності на пластинках конденсатору при фіксованій різниці потенціалів відбувається перерозподіл заряду, а в електричному ланцюгу, що з’єднує ці пластини, утворюється

електричний струм. Останній, в свою чергу, приводить до падіння напруги на опорі навантаження, яка визначається формулою:

$$U_{нс} \updownarrow = Z_н i_{нс} \updownarrow ,$$

де $Z_н$ – комплексний опір навантаження,

$i_{нс}$ – струм небезпечного сигналу, що виник в результаті перерозподілу заряду на пластинах конденсатору.

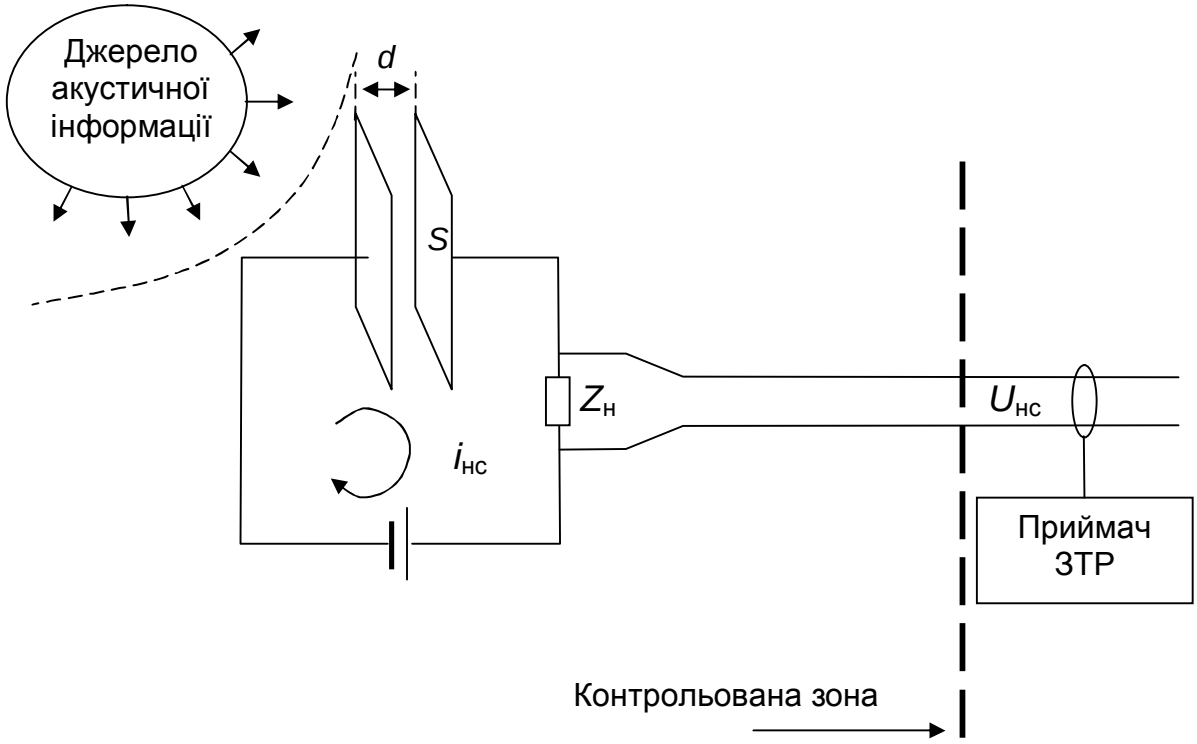


Рис. 2.14. Акустоелектричні перетворення на прикладі конденсатора пристроїв ДТЗС.

Якщо лінія, що зв’язана зі схемою з конденсатором, виходить за межі КЗ та ОІД, то противник може перехоплювати небезпечний сигнал.

3. Акустоелектричний ефект п’єзоелектрика. Ефект акустоелектричного перетворення є основною властивістю п’єзокристалу. Якщо його механічно стискувати, то на полюсах п’єзокристалу пропорційно до посилення стискування з’являється різниця потенціалів (рис. 2.15 (а)). Якщо розтягувати – потенціали на полюсах змінюються на протилежний (рис. 2.15 (б)). Тому на сьогоднішній день п’єзокристали дуже широко використовується в

мікрофонах, сучасних телефонних та інших апаратах для перетворення акустичних сигналів в електричні та електричних в акустичні.

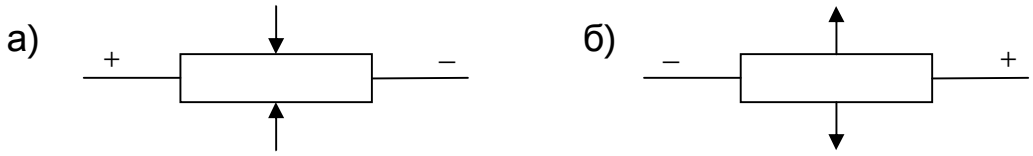


Рис. 2.15. Акустоелектричний ефект п’єзоелектрика.

Однак, ця властивість може відігравати і негативну роль, якщо схеми ДТЗС на ОІД використовують п’єзоелектрик. Вплив на нього акустичного тиску приводитиме до змінної складової напруги на полюсах та в схемі. Якщо лінія виходить за межі КЗ та ОІД, противник зможе перехоплювати інформацію.

4. Акустоелектричний ефект інших елементів ТЗС, що мають активний опір. Як правило, кожна електронна схема ДТЗС використовує резистори – активні опори, яких також можуть утворювати ТКВІ. Розглянемо даний акустоелектричний ефект на прикладі схеми заміщення (рис. 2.16).

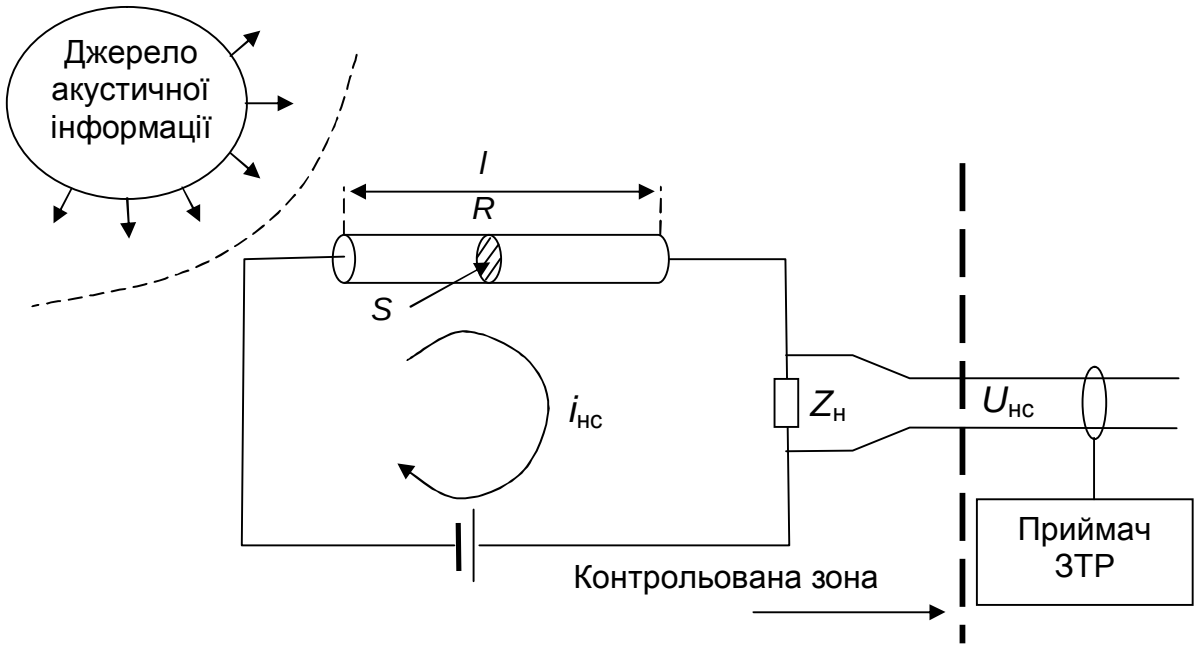


Рис. 2.16. Акустоелектричні перетворення на струмопровідному стержні, що має активний опір.

Якщо на електричну схему впливає акустичне поле, то він приводить до вібрації елемент з активним опором (нехай, для простоти, у виді звичайного стержня). В результаті вібрації змінюється площа його поперечного перетину, від якої залежить його власний опір. Останній виражається формулою:

$$R \updownarrow = \rho \frac{l}{S \updownarrow},$$

де ρ – питомий опір матеріалу досліджуваного стержня,

S – площа його поперечного перетину,

l – довжина стержня.

Якщо в схемі протікає електричний струм, то під дією змінного опору в струмі з'явиться відповідна змінна складова струму небезпечного сигналу, а останній, в свою чергу, може проникнути через ланцюги ДТЗС в лінію, що виходить за межі КЗ та бути перехопленим противником.

Запобігання витоку інформації акустоелектричним каналом (унеможливлення створення такого ТКВІ) досягається способами:

– використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, діодних та компенсаційних схем;

– використання в лініях ДТЗС лінійного зашумлення.

2.4.4. Акустооптоелектронні (лазерні акустичні) канали витоку інформації

Акустооптоелектронний (лазерний акустичний) канал утворюється шляхом дистанційного із-за меж КЗ зняття лазерними засобами акустичної розвідки вібраційних коливань поверхонь інженерних або будівельних комунікацій, предметів інтер'єру ОІД тощо, що спричинені акустичним полем (небезпечним мовним сигналом).

Сутність акустооптоелетронних (лазерних акустичних) каналів витоку інформації полягає в такому. На ОІД, де озвучується інформація, під впливом небезпечного акустичного сигналу знаходяться усі предмети. Деякі предмети, що мають оптичні властивості віддзеркалення, приводяться до вібрації. Такими предметами є скло вікна, дзеркало тощо. Вібрація таких предметів зв’язана з коливанням їх поверхні. Якщо з зовні ОІД на поверхню скла, дзеркала, що вібрують, спрямувати лазерний промінчик, то він віддзеркалиться від поверхні у вигляді промінчика, модульованого тремтінням від сигналу вібрації, і розповсюджуватиметься далі (рис. 2.17). Тремтіння Віддзеркалений промінчик може бути перехоплений противником, здійснена його демодуляція (виділене тремтіння) і відновлений початковий інформаційний мовний сигнал.

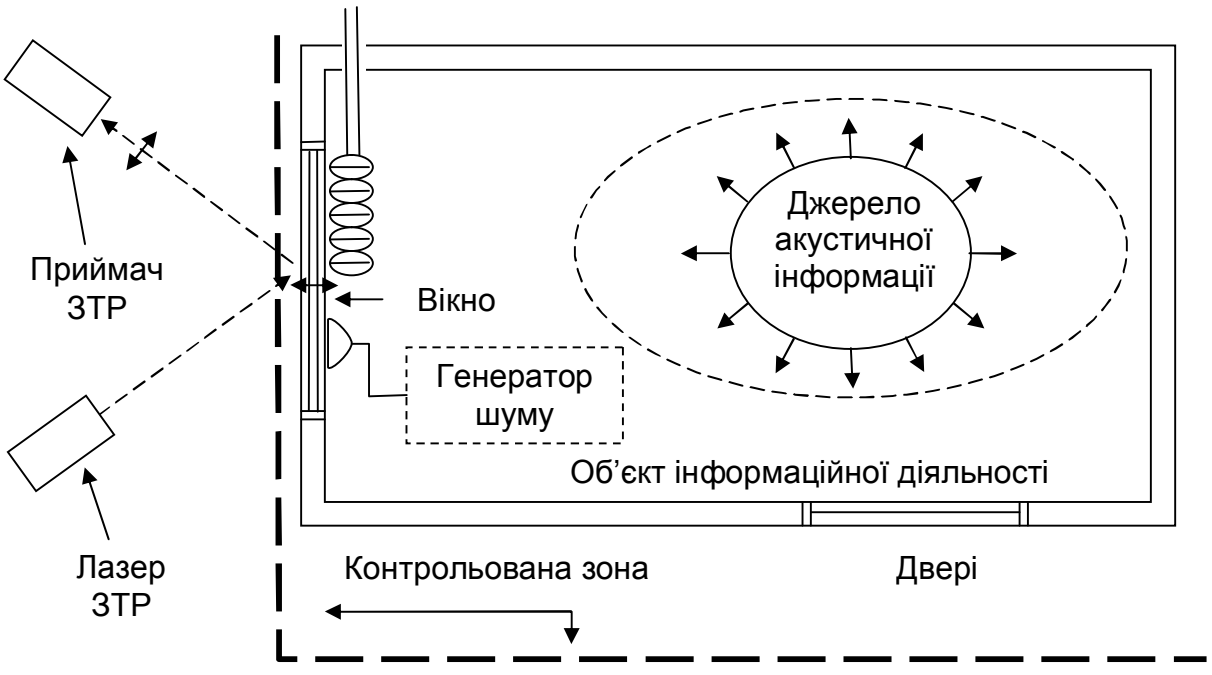


Рис. 2.17. Акустооптоелектронний (лазерний акустичний) канал витоку інформації

Запобігання витоку інформації акустооптоелектронним (лазерним акустичним) каналом (унеможливлення створення такого ТКВІ) досягається способами:

– використання вакуумних та інших захищених вікон, матування в вікнах зовнішньої поверхні скла;

– використання щодо вікон та інших предметів відзеркалення вібраційного зашумлення.

2.4.5. Канали ВЧ нав'язування (для зняття мовної інформації)

Канали ВЧ нав'язування (для зняття мовної інформації) є різновидами параметричних каналів витоку акустичної інформації. Параметричні канали витоку акустичної інформації на ОІД, подібно параметричним каналам витоку інформації, що обробляється ОТЗС, засновані на впливі противника на параметри схем ТЗС та інші провідні матеріали, що розташовані на ОІД, знаходяться в полі акустичного сигналу та приводяться до вібрації. Такими матеріалами можуть бути буд-які струмопровідні матеріали: музичні інструменти, годинники з боєм, навіть звичайний цвях, який має резонансну частоту в мовному діапазоні.

Якщо на струмопровідний предмет впливати високочастотним електромагнітним полем, то в ньому виникатимуть електричні ВЧ струми (рис. 2.18). Якщо одночасно цей самий предмет знаходитиметься і під дією акустичного тиску та вібруватиме, в ньому, як вже розглядалося, коливатиметься власний опір та здійснюватиметься його модуляція ВЧ струмом. Останній в свою чергу перевипромінюватиме ВЧ поле та модульований небезпечний мовний сигнал, який може розповсюджуватиметься на відносно великі відстані за межі КЗ та ОІД та бути перехопленим противником. Окрім того такий спосіб перехоплення

дозволяє досить нескладно реалізувати перехоплення з когерентним прийомом, який як відомо, забезпечує максимум завадостійкості.

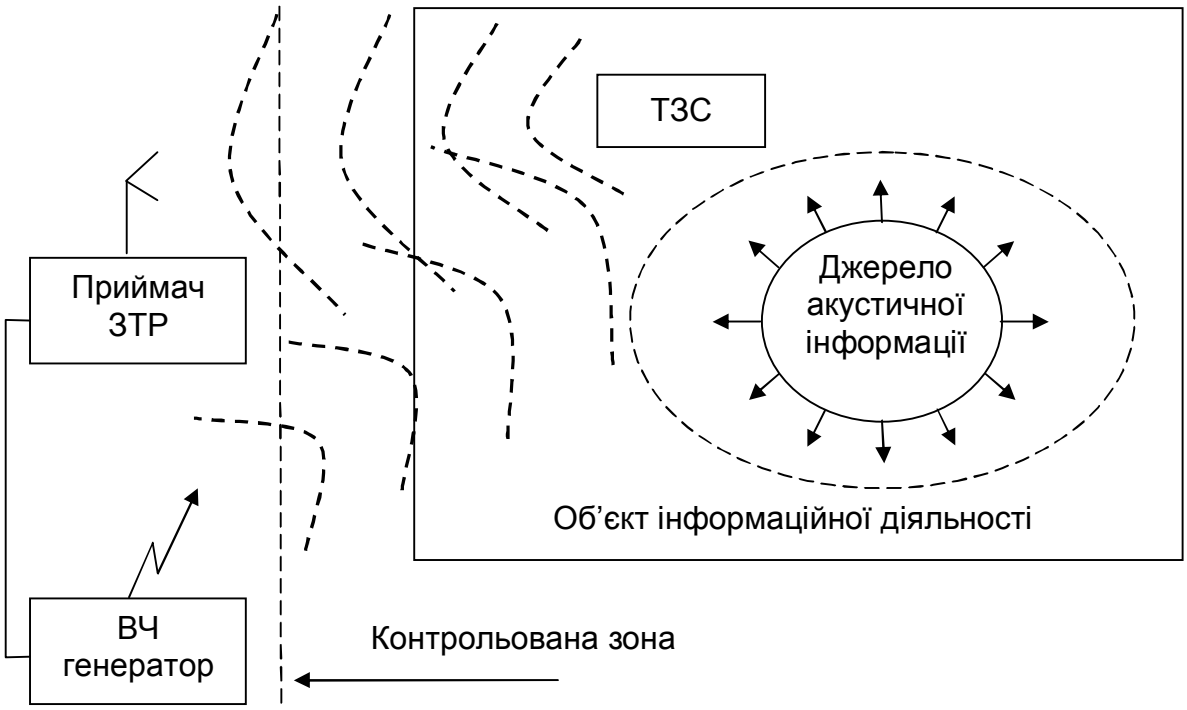


Рис. 2.18. Канал ВЧ нав'язування (для зняття мовної інформації).

Запобігання витоку інформації каналом ВЧ нав'язування (для зняття мовної інформації), унеможливлення створення такого ТКВІ досягається способами:

– просторового електромагнітного зашумлення ОІД на частотах ВЧ опромінення;

– індикації, сигналізації поля ВЧ опромінення.

Одним з різновидів каналів ВЧ нав'язування є канал ВЧ нав'язування лініями телефонного зв'язку (рис. 2.19). Високочастотний сигнал (струм) ВЧ генератора вводиться в телефонну лінію. Оскільки струм високочастотний, то для нього група розімкнутих контактів (при покладеній трубці), представлятиме конденсатор з ємнісним опором:

$$Z_c = \frac{1}{j\omega \uparrow C \downarrow},$$

де ω – частота струму,

С – ємність контактної групи.

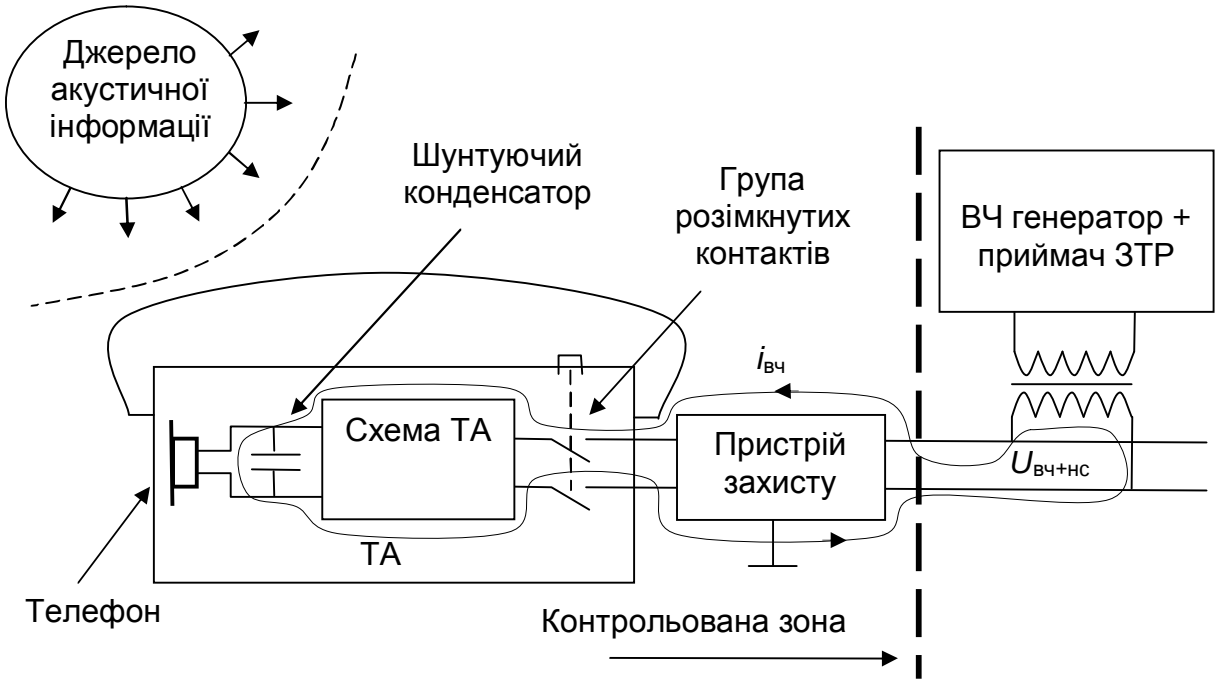


Рис. 2.19. Канал ВЧ нав’язування (для зняття мовної інформації) лініями телефонного зв’язку.

За рахунок високої частоти при малій ємності групи контактів цей опір буде відносно невеликим.

Струм, що проникає в телефон, моделюється змінним опором під дією коливання мембрани від небезпечного акустичного сигналу. Модульований ВЧ струм відбивається від нелінійностей схеми телефону та поширюється лінією зв’язку у зворотному напрямку. За межами КЗ такий модульований ВЧ сигнал знімається засобами технічної розвідки, які безпосередньо підключаються до лінії зв’язку, здійснюється його демодуляція, тобто виділення низькочастотного електричного сигналу, еквівалентного небезпечному акустичному сигналу і перетворення його в акустичний сигнал. Таким чином, може знімається акустична інформація, що озвучується на ОІД.

Запобігання витоку інформації каналом ВЧ нав’язування (для зняття мовної інформації) лініями телефонного зв’язку (унеможливлення створення такого ТКВІ) досягається способами:

– шунтування телефону (елементу, де відбувається модуляція) конденсатором та використання інших компенсаційних схем;

– використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня або відключення лінії на момент ведення секретних переговорів.

Таким чином у пункті 2.4 розглянуті основні різновиди ТКВІ, які утворюються на ОІД при озвучуванні інформації. Основними способами запобігання витоку інформації такими каналами та унеможливлення створення таких ТКВІ є:

– огороджувальні конструкції ОІД (стіни, стеля та підлога) повинні бути досить масивними (залізобетонними, цегляними, тощо), такими, що виключався ефект парусності;

– ліквідація щілин в огороджувальних конструкціях (шпаклювання тріщин, герметизація щілин звукоізолюючими матеріалами, тощо);

– покриття, штукатурка огороджувальних конструкції ОІД (стін, стелі, підлоги, дверей) звукопоглинаючими матеріалами та використання переважно звукопоглинаючих матеріалів та вібраційних розв’язок в побудові систем опалення, водопостачання, водовідведення тощо;

– просторове акустичне зашумлення повітряного середовища зовні ОІД та вібраційне зашумлення огороджувальних конструкції ОІД (стін, стелі, підлоги, дверей) та систем опалення, водопостачання, водовідведення, тощо;

– використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, діодних та компенсаційних схем, або відключення лінії на момент ведення секретних переговорів;

– використання в лініях ДТЗС та СП лінійного зашумлення;

– використання вакуумних та інших захищених вікон, матування в вікнах зовнішньої поверхні скла;

– просторове електромагнітне зашумлення ОІД;

– індикація, сигналізація поля ВЧ опромінення та блокування роботи ОТЗС;

– шунтування телефону (елементу, де відбувається модуляція) та використання інших компенсаційних схем.

Перелік питань для самоконтролю

1. Сутність та класифікація акустичних каналів витоку інформації.
2. Основні заходи по запобіганню витоку інформації акустовібраційним (віброакустичним) каналом.
3. Сутність "мікрофонного ефекту" електронних елементів ТЗС.
4. Основні заходи по запобіганню витоку інформації акустоелектричним каналом.
5. Сутність акустооптоелектронного (лазерного акустичного) каналу витоку інформації та основні заходи по запобіганню витоку інформації цим каналом.
6. Сутність параметричних каналів витоку мовної інформації та основні заходи по запобіганню витоку інформації цими каналами.

2.5. Технічні канали витоку інформації на основі закладних пристроїв

2.5.1. Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв)

Одним зі шляхів витоку, а точніше можливостей перехоплення противником інформації на ОІД є витік інформації через засоби несанкціонованого перехоплення. Сутність їх полягає в тому, що вони знаходячись в межах ОІД (КЗ) приймають (перехоплюють) сигнал, що циркулює, та передають його противнику. Засоби несанкціонованого перехоплення приховано розміщують на об'єкті та камуфлюють під звичайні предмети та інші елементи так, щоб їх було складно виявити. Умовно цей канал витоку можна зобразити у вигляді рис. 2.20:

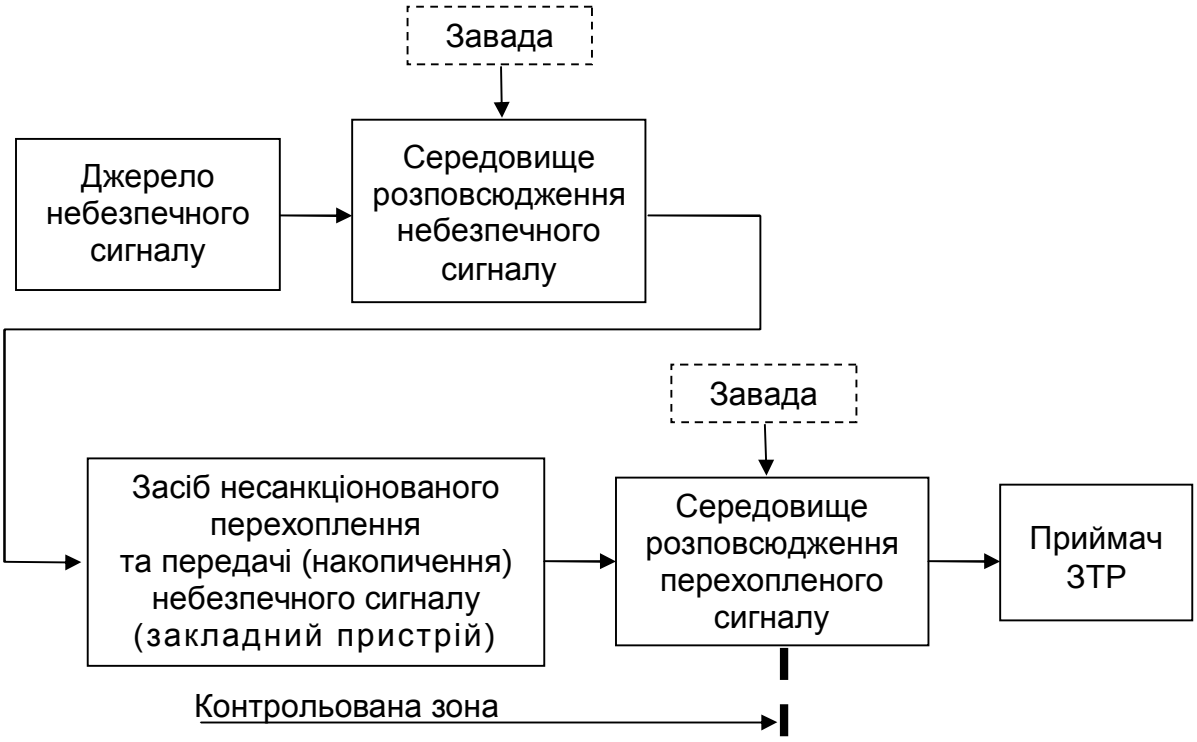


Рис. 2.20. Канали витоку інформації на основі закладних пристроїв.

Розміщення засобів несанкціонованого перехоплення на ОІД або в межах КЗ можливе шляхом:

– несанкціонованого проникнення на ОІД (в КЗ) сторонніх осіб;

– порушення правил режиму доступу штатних осіб на ОІД (в КЗ);

– закладки цих засобів у приміщенні до (під час) обладнання в них ОІД та комплексу ТЗІ.

Тому засоби несанкціонованого перехоплення, як зазвичай, отримали назву закладних пристроїв, яке і використовується в сучасній літературі та підручниках.

Закладні пристрої класифікують: (1) за видом та способом прийому інформації та (2) за способом передачі перехопленої інформації до приймача ТЗР противника.

1. За видом та способом прийому інформації закладні пристрої розділяють на:

– закладні пристрої, призначені для одержання мовної акустичної інформації, що циркулює в приміщенні – аудіо-закладні пристрої;

– закладні пристрої, призначені для одержання аудіо- та відео-інформації – телевізійні закладні пристрої;

– закладні пристрої з підключенням до телефонних ліній зв'язку, пристроям обробки та передачі інформації та ін.

2. За способом передачі перехопленої інформації противнику закладні пристрої розділяють на:

– закладні пристрої, що використовують для передачі перехопленої інформації радіоефір – радіозакладні пристрої;

– закладні пристрої з передачею перехопленої інформації по мережам зв'язку, управління, живлення і т.п.;

– радіозакладні пристрої з перевипромінюванням (пасивні);

– закладні пристрої з передачею перехопленої інформації по стандартному телефонному каналу – так названі закладні пристрої типу «довге вухо», або «зі штучно піднятою трубкою» та ін.

2.5.2. Загальні характеристики та особливості деяких типів закладних пристроїв

Загальні характеристики закладних пристроїв.

1. **Оформлення (виконання):**

– у вигляді технічних модулів закамуфльованих під технічні елементи та пристрої, елементи одягу, побутові предмети та ін.

2. **Потужність випромінювання:**

– до 10 мВт – мала потужність;

– від 10 до 100 мВт – середня потужність;

– більше 100 мВт – велика потужність;

– с регульованою потужністю випромінювання.

3. **Використовуваний вид модуляції:**

– AM, FM, WFM (широкосмугова), NFM (вузькосмугова) – стандартні види модуляції;

– модуляція з інверсією спектру;

– модуляція з частотною мозаїкою;

– дельта-модуляція;

– модуляція в шумоподібні сигнали.

4. **Стабілізація частоти:**

– нестабілізовані;

– зі схемотехнічною стабілізацією частоти;

– с кварцовою стабілізацією.

5. **Гарантована дальність перехоплення або спосіб підключення:**

– до 10 м з посередництвом звукової хвилі через мікрофон, або з підключенням до мікрофонів (слухавок) пристроїв обробки та передачі інформації;

– до 1 м з посередництвом вібраційної хвилі (через цегельні й бетонні стіни) та контактний мікрофон – стетоскоп;

– контактне підключення та установка закладних пристроїв перехоплення інформації в каналах обробки інформації, систем передачі даних та зв'язку.

Особливості деяких типів радіозакладних пристроїв

Радіозакладні пристрої – це закладні пристрої, які для передачі перехопленої інформації до засобів ТЗР використовують радіоефір. Передача в них здійснюється шляхом перетворення (модуляції) перехоплених сигналів в електромагнітні хвилі, що розповсюджуються в просторі – ефірі.

Для виявлення випромінюючих в ефір радіозакладок необхідне визначення діапазону їхньої роботи, виду модуляції та закриття.

Як правило, діапазон роботи існуючих радіозакладних пристроїв досить широкий і має тенденцію до зростання в сторону більш високих частот. Основні діапазони відомих зразків закладок складають: 270...480 МГц, 115...200 МГц, 75...115 МГц. Сучасні ж радіозакладні пристрої працюють у діапазоні до 1000 МГц і вище. Це приводить до ускладнення проведення пошукових заходів.

Суттєве ускладнення в пошуку закладних пристроїв також викликають види модуляції й закриття (скремблювання, рандомізація, шифрування, тощо), які постійно змінюються і удосконалюються. Так, наприклад, якщо в радіозакладних пристроях, що були широко поширені на початковому етапі їх розвитку, використовувалась амплітудна (частотна) і перехоплений сигнал можна було прийняти звичайним побутовим приймачем, то в сучасних – види модуляції зазнали істотних змін. З'явився принципово новий клас радіозакладних пристроїв з дельта-модуляцією (кодування інформації в короткотривалі імпульси та передача їх в зазначений час) та модуляцією в шумоподібні сигнали (передача інформації з рівнем нижче звичайних шумів). Крім того, у найбільш професійних радіозакладках використовують складні види модуляції з псевдовипадковою перестановкою несучої частоти.

Закладні пристрої типу «довге вухо» або закладка «зі штучно піднятою трубкою» – це закладні пристрої, які комплексуються з абонентськими пристроями телефонного зв’язку загального користування, що знаходяться на ОІД, та можуть дистанційно керуватися з використанням цієї ж телефонної мережі.

Принцип роботи зручно розглянути на прикладі. При покладеній трубці телефонного апарату до лінії підключена система виклику, яка приймає у випадку виклику абонента сигнал виклику. Коли абонент піднімає трубку, система виклику відключається, до лінії підключається переговорна система телефонного апарату і забезпечується зв'язок. Закладка з «штучно піднятою трубкою» забезпечує підключення переговорної систем телефонного апарату з мікрофоном трубки, або додаткового мікрофона до лінії без механічного підйому трубки.

Подача сигналу для штучного підйому трубки може здійснюватися різними способами. Наприклад:

– *набирається номер абонента*, якому встановили в телефонний апарат закладку для прослуховування;

– *після декількох сигналів виклику кладеться трубка* так, щоб абонент не встиг її підняти, ніби хтось помилився, і система виклику у телефонному апараті з закладкою відключається;

– *через певний інтервал часу (10...40 с) здійснюється повторний виклик*. При цьому для того щоб сторонній виклик, що випадково потрапив у цей інтервал часу, не підключився до системи, на протязі 45...60 с закладка виробляє сигнал відбою;

– через зазначений інтервал часу (45...60 с) *закладний пристрій підключається до лінії*, і йде контроль акустики приміщення (слід зазначити, що при підключенні до телефонного апарата додаткових мікрофонів може бути організований контроль інших приміщень);

– при піднятті трубки абонента, що прослуховується, закладка відключається.

Відомі й інші способи несанкціонованого підключення телефонів із закладкою до лінії, особливо для сучасних цифрових систем обслуговування.

Суттєвою особливістю закладних пристроїв типу «довге вухо» або «зі штучно піднятою трубкою» є їхня велика дальність дії – практично по всій земній кулі.

Радіозакладні пристрої з перевипромінюванням – це закладні пристрої, які реалізують перевипромінювання ВЧ поля з модуляцією його небезпечним сигналом, що циркулює на ОІД. Як правило, даний тип закладок використовується для перехоплення мовних акустичних сигналів.

Суть пристрою полягає в наступному. Структура цією закладки складається з двох резонаторів: електромагнітного ВЧ резонатора (в мегагерцовому діапазоні) та акустичного, налаштованого на частоту мовного сигналу. Вказані резонатори взаємодіють так, що акустичний, знаходячись під впливом поля мовного сигналу, вібрує та приводить до зміни добротність електромагнітного ВЧ резонатора. В результаті перевипромінення відбувається модуляція.

Суттєвою особливістю такого пристрою є те, що він не використовує джерела електроживлення і може працювати необмежено довго. Крім того сама закладка не випромінює, якщо немає поля опромінення, що ускладнює її пошук.

Мережеві закладні пристрої – це закладні пристрої, які для свого функціонування використовують мережу електроживлення. Їх умовно розділяють на дві групи:

– закладні пристрої, що для передачі перехопленої інформації використовують мережу електроживлення як середовище;

– закладні пристрої, що живляться від мережі електроживлення і для передачі перехопленої інформації використовують не мережу електроживлення, а інше середовище, наприклад, радіоефір.

Ці закладки, як правило, камуфлюються під побутові прилади (електролампа, електрочайник, тощо), і можуть бути досить просто впровадженими на ОІД. Включення заставних пристроїв забезпечується, як правило, включенням камуфлюючого пристрою у мережу.

Однієї з суттєвих особливостей подібних закладних пристроїв є необмежений час їхньої роботи (поки є мережа живлення).

Однак для таких пристроїв існує ряд обмежень. Наприклад, не рекомендується використовувати камуфлюючий виріб з великим споживанням електроенергії, більше 0,5 кВт. Це може викликати в акустичному каналі заважаючий мережевий фон. Не рекомендується встановлювати радіомікрофон поблизу джерел акустичних завад: холодильника, вентилятора, трансформатора, телевізора й т.п.

Для забезпечення більшої прихованості закладних пристроїв може бути використане дистанційне управління, що дозволяє включати закладний пристрій тільки на необхідний час.

2.5.3. Заходи захисту інформації від витоку каналами на основі закладних пристроїв

Канали витоку інформації на основі закладних пристроїв є рукотворними (штучними) технічними каналами витоку, призначеними для несанкціонованого перехоплення (зняття, прихованого отримання) інформації. Тому при їх установці, вживають заходи для маскування різними способами. Маскування закладних пристроїв істотно ускладнює їх пошук і захист від витоку інформації.

Для захисту інформації від витоку каналами на основі закладних пристроїв проводяться такі заходи:

– недопущення установки закладних пристроїв на ОІД (як правило, для постійно діючих ОІД);

– виявлення та протидія роботі закладних пристроїв на ОІД (як

правило, для тимчасових ОІД).

Зазначені заходи розрізняють на організаційні та технічні.

Заходи з недопущення установки закладних пристроїв.

Організаційні заходи включають:

– організацію режиму роботи виділених приміщень та ОІД;

– організацію контролю за доступом відвідувачів і співробітників, що мають обмеження за доступом;

– організацію контролю роботи співробітників;

– організацію перевірки приміщень об'єкта і техніки, що перебуває на ньому, на наявність закладних пристроїв, у тому числі і нової, що поступає;

– аналіз методів і способів установки закладних пристроїв, їхнього камуфляжу, конструкцій та технологій.

Технічні заходи включають:

– створення системи технічних засобів охорони;

– створення системи охоронної сигналізації;

– створення телевізійної системи спостереження;

– створення системи контролю керування доступом;

– використання технічних засобів, що сигналізують про підключення в виділених приміщеннях закладних пристроїв до лінії зв'язку, мережі живлення й т.п.;

– використання технічних засобів контролю на наявність закладних пристроїв у техніці, що поступає, та приміщеннях;

– використання технічних засобів контролю радіовипромінювань та випромінювань у лініях зв'язку, живлення та керування;

– використання технічних засобів контролю інфрачервоних випромінювань;

– використання технічних засобів нелінійної радіолокації та підповерхневої локації;

– використання рентгенівських установок, тепловізійних систем, металодетекторів, тощо.

Заходи з виявлення та протидії роботі закладних пристроїв.

Організаційні заходи включають:

– аналітичну роботу з виявлення можливих місць установки закладних пристроїв (з урахуванням особливостей їхньої роботи);

– організацію роботи служби безпеки по контролю випромінювань в ефірі, мережах зв'язку, управління;

– аналіз частотного діапазону й способів роботи закладних пристроїв.

Технічні заходи включають:

(заходи, пов'язані з виявленням закладних пристроїв)

– контроль сигналів у лініях зв'язку, керування, живлення, охоронних систем;

– контроль радіовипромінювань у районі ОІД;

– контроль інфрачервоних випромінювань у районі розташування ОІД;

– використання апаратури нелінійної радіолокації та підповерхневої локації;

– використання рентгенівських установок, тепловізійних систем, металодетекторів;

– використання технічних засобів, що сигналізують про підключення закладних пристроїв;

– використання засобів візуального контролю;

(заходи, пов'язані з протидією роботі закладних пристроїв)

– використання електромагнітних засобів зашумлення;

– використання акусто-вібраційного зашумлення;

– демонтаж, руйнування та відключення закладних пристроїв.

Перелік питань для самоконтролю

1. Технічні канали витоку інформації на основі закладних пристроїв.
2. Засоби несанкціонованого перехоплення (закладні пристрої) та їх класифікація.
3. Основні особливості радіозакладних пристроїв.
4. Принцип роботи закладних пристроїв типу «довге вухо» та «зі штучно піднятою трубкою».
5. Принцип роботи мережевих закладних пристроїв.
6. Організаційні заходи захисту інформації від витоку каналами на основі закладних пристроїв.
7. Технічні заходи захисту інформації від витоку каналами на основі закладних пристроїв.

2.6. Канали перехоплення (зняття) інформації з каналів зв'язку

Функціонування сучасних інформаційно-телекомунікаційних систем пов'язано з передаванням великих об'ємів інформації на великі відстані з використанням різноманітних каналів зв'язку та середовищ розповсюдження носіїв інформації. Самі середовища розповсюдження байдужі до інформації, яка передається, і підпорядковуються лише законам фізики, у відповідності з якими хто має доступ до середовища, той має змогу отримати сигнал. На теперішній час існує багато методів, а саме криптографічних методів шифрування, які дозволяють гарантовано захистити відкритий канал для передачі інформації. Тому поняття витоку інформації в каналах зв'язку, як зазвичай, не використовується і вважається, що для передачі секретної інформації використовуються лише захищені канали. Однак, якщо канали (лінії) не захищені, або недостатньо захищені, то користування ними може призвести до витоку інформації, що передається. Розглянемо, які процеси цьому сприяють.

За середовищем розповсюдження носіїв інформації розрізняють наступні типи (канали, лінії) зв'язку:

– *безпровідний зв'язок* (радіо, радіорелейний, тропосферний, космічний, тощо), який для передачі сигналів використовує ефір – навколишнє середовище.

– *провідний зв'язок*, який для передачі інформації використовує спеціально створені середовища для носія – провідні лінії. В залежності від фізичної природи ліній та носіїв, що в них використовуються, останні поділяють на *електропровідні* лінії ти *волоконно-оптичні* лінії зв'язку (ВОЛЗ).

Безпровідний зв'язок. Якщо інформаційний сигнал передається від передавача до приймача через ефір (рис. 2.21), то противник з використанням ЗТР зможе перехопити електромагнітну хвилю, що

формується передавачем та розповсюджується, та добути інформацію, що його цікавить.

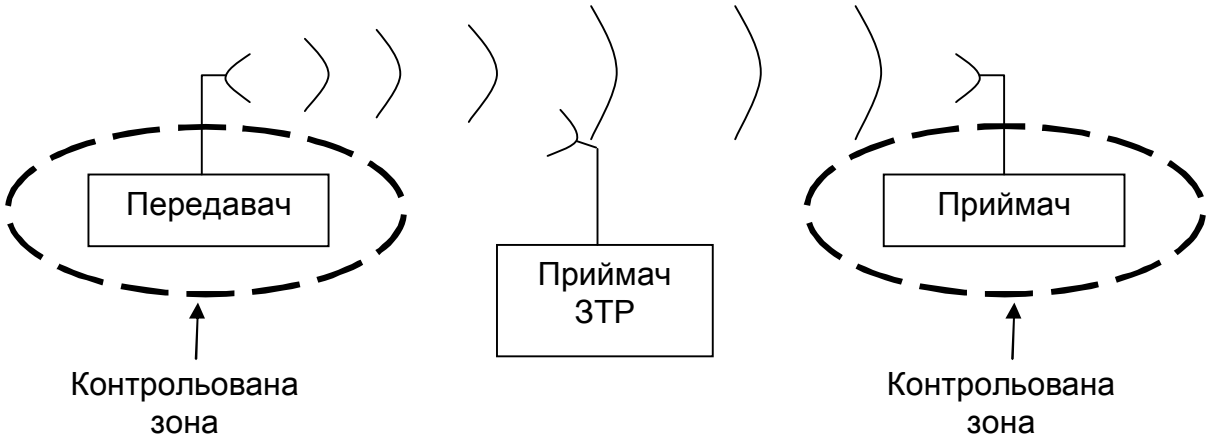


Рис. 2.21. Канал перехоплення (зняття) інформації з каналу безпровідного зв’язку.

Електропровідний зв’язок. Для електропровідного зв’язку носієм є електричний струм, а середовищем розповсюдження – кабель (система проводів). Перехоплення інформації, що зводиться до вимірювання струму, або напруги в проводах кабелю, можливе контактним з безпосереднім підключенням до проводів ЗТР (рис. 2.22(а)) та безконтактним (індуктивним) способами (рис. 2.22(б)). Як недолік, при контактному способі підключення вносяться зміни параметрів лінії, які можуть бути зафіксованими.

Волоконно-оптичні лінії зв’язку. Аналогічно як і для електропровідного зв’язку для ВОЛЗ характерні контактний та безконтактний способи перехоплення інформації.

Контактний спосіб перехоплення реалізується шляхом очищення ізоляції, як правило, хімічним способом щоб не порушити поверхню світловоду, та відкачуванням енергії світла (див. рис. 2.23(а)). Така відкачка енергії може бути виявлена і передача інформації припинена.

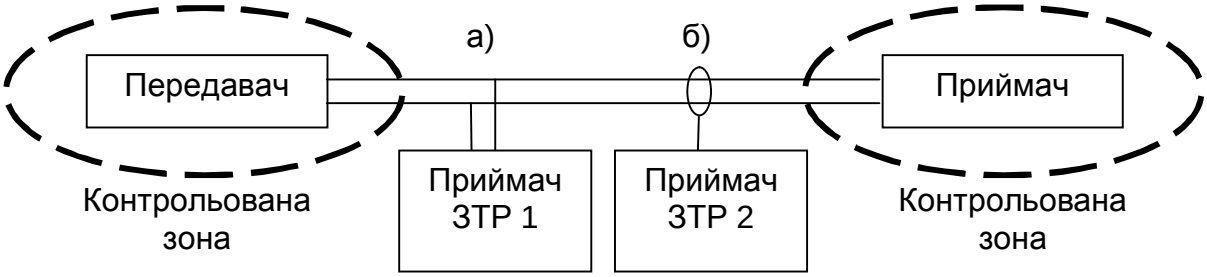


Рис. 2.22. Канал перехоплення (зняття) інформації з каналів електропровідного зв’язку: (а) контактним способом, (б) безконтактним індуктивним способом.

Безконтактний спосіб перехоплення використовує просочування світла через ізоляцію: на ділянках просторово-неустановленого режиму, шляхом перегинання кабелю та на стиках світловодів.

Сутність перехоплення на ділянках просторово-невстановленого режиму полягає в тому, що світловий потік на початку ВОЛЗ є досить інтенсивним. Його промені, що мають хаотичний напрямок, нагрівають ізоляцію та, переважно в тепловому діапазоні, просочуються через неї. Енергія світла, що просочилась, може бути перехоплена ТЗР противника.

Перегинання кабелю ВОЛС приводить до тих же ефектів, що і на ділянках просторово-невстановленого режиму (рис. 2.23(в)). Промені світла, які були направленні вздовж лінії при перегині стають під кутом до стінок світловоду і інтенсивно діють на ізоляцію. В результаті частина енергії просочується за межі ізоляції та може стати причиною перехоплення інформації, що передається.

Значна частина енергії світла в волоконно-оптичних системах зв’язку може витікати на роз’ємних стиках волокон світловодів за ряду причин (рис. 2.24), а саме:

а) радіальна неузгодженість волокон світловодів;

б) кутова неузгодженість осей волокон світловодів;

в) наявність зазору поміж торцями волокон світловодів;

г) непаралельність торців волокон світловодів;

д) різниця радіусів волокон світловодів.

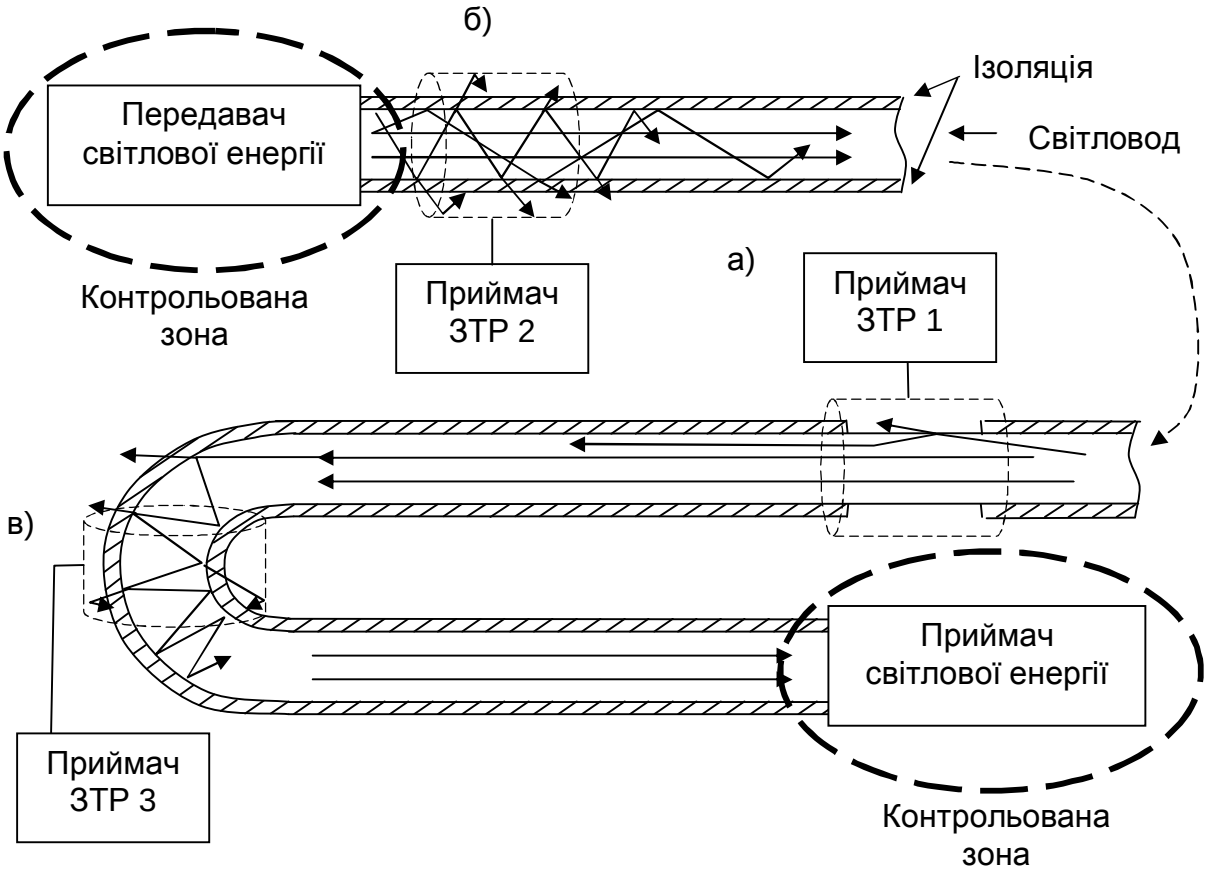
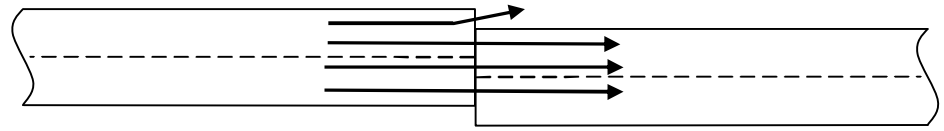


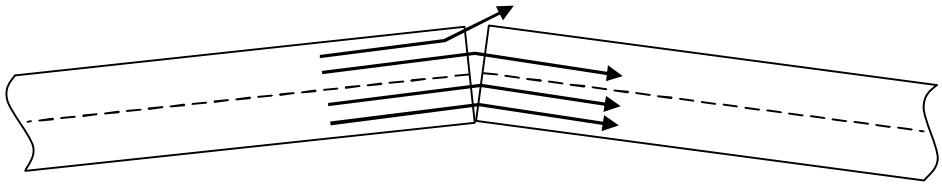
Рис. 2.23. Схема перехоплення інформації в ВОЛЗ: (а) контактним способом, (б) безконтактним способом на ділянках просторово-неустановленого режиму, (в) безконтактним способом на інших ділянках ВОЛЗ

Запобігання витоку інформації досягається шляхом:

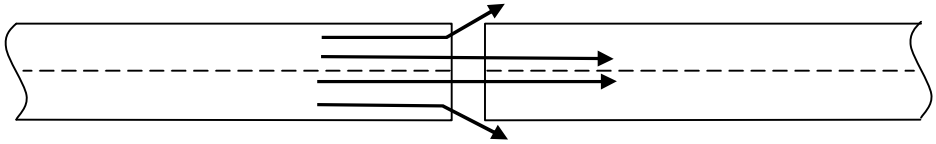
- використання засобів криптографічного захисту інформації;
- створення навколо лінії КЗ не меншої за Зону 2;
- організація режиму доступу в КЗ, на ОІД;
- екранування, бронювання ліній;
- лінійного та просторового зашумлення.



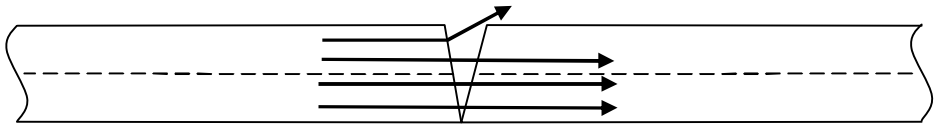
а) радіальна неузгодженість волокон світловодів



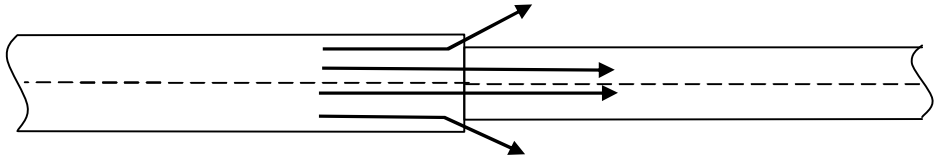
б) кутова неузгодженість осей волокон світловодів



в) наявність зазору поміж торцями волокон світловодів



г) непаралельність торців волокон світловодів



д) різниця радіусів волокон світловодів

Рис. 2.24. Причини витоку інформації на стиках волокон світловодів

2.7. Технічні канали витоку видової інформації

Під візуальною інформацією будемо розуміти в розгорнутому (відкритому) вигляді всякі зображення, тексти, схеми, документи, зовнішній вид засобів та об’єктів, зображення на моніторах та екранах, які можна бачити органами зору. Витік видової інформації можливий шляхом таких дій противника:

– спостереження,

– зйомки,

– копіювання.

Спостереження, зйомка та копіювання може проводитись:

– відкрито та приховано;

– з використанням та без використання відповідної фото-, відео- та ксерокопіювальної техніки;

– в денний час, в сутінках з підсвітлюванням та в нічний час з використанням засобів нічного бачення;

– з використанням транспортних засобів та без них.

Запобігання витоку інформації досягається шляхом:

– створення ОІД, режимної зони та виконання робіт, пов’язаних з приховуванням видової інформації в її межах в спеціально обладнаних місцях, приміщеннях, павільйонах, тощо;

– організації режиму доступу в режимну зону, на ОІД.

2.8. Матеріально-речовинні канали витоку інформації

Матеріально-речовинні канали витоку обумовлені можливістю противника знімати інформацію з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу, з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо, а також аналізувати структуру, хімічний склад матеріалів та речовин, інформація про які має обмежений доступ. Наприклад, такою інформацією може бути технологія виготовлення сталі бронетехніки та озброєння, хімічний склад отруючих речовин, структура матеріалу носія інформації тощо. Фізичний доступ противника до таких матеріалів та речовин, може призвести до отримання противником інформації з обмеженим доступом.

Однією з небезпечніших загроз є **добування інформації з магнітних носіїв**, яка вважається стертою.

Суть запису інформації на магнітні носії полягає в тому, що магнітна головка проходить над поверхнею магнітного середовища (феромагнетику), та впливає полем запису на орієнтацію доменів – структурних магнітних елементів феромагнетику. В залежності від напрямку силових ліній поля запису домени відповідно повертаються та, завдяки ефекту гістерезису, залишаються в тому ж положенні після зняття поля – запам'ятовують поле намагнічування. Зчитування здійснюється таким чином: головка, проходячи над поверхнею магнітного середовища запису, фіксує поле намагнічування доменів та передає відповідний сигнал в інформаційну систему.

На цьому принципі побудовані всі жорсткі та гнучкі магнітні носії, що використовуються в засобах ЕОТ. На теперішній час технології виготовлення магнітних носіїв дозволяють забезпечити досить велику щільність запису, яка досить швидко зростає з часом та забезпечує зберігання великих об'ємів даних.

2.8.1. Способи гарантованого знищення та добування інформації з магнітних носіїв

Як відомо, "стирання" файлу не приводить до знищення інформації на носії. Знищується лише його заголовок та шлях до нього на носії. З часом в результаті користування носієм на місця попередніх записів (знищеного файлу) може бути записана нова інформація, яка переорієнтує намагніченість доменів. Дані, поверх яких нічого не записувалось, залишаються і можуть бути доступними та відновленими за допомогою штатних засобів на програмному рівні, без аналізу середовища носія.

Для знищення інформації, стирання записів в магнітному середовищі носія існують програми, які дозволяють знищити непотрібний файл з перезаписом на його доріжках інших даних. В даному разі

відновлення інформації штатними засобами вже не буде можливим. Однак, якщо інформація має велику цінність та носій якимось чином потрапив до противника (списування та утилізація, ремонт, тощо), противник може провести мікроскопічний аналіз (наприклад, методом зондової, візуальної мікроскопії) магнітного середовища та по залишковому намагніченню добути деякі масиви інформації, які можуть бути досить великими та змістовними.

Суть залишкового намагнічення полягає в тому, що при перезапису даних магнітна головка не може в точності повторити свою траєкторію попереднього запису на цій же доріжці. Неточність юстировки головки значно перевищує розміри доменів і тому не всі з них переорієнтовуються новим записом. Однак якась частина інформації при цьому все таки втрачається. Тому для підвищення імовірності знищення записаної інформації цим способом здійснюють багатоциклові перезаписи, алгоритми яких представлено в табл. 2.1. Слід відмітити, що ці алгоритми знищення реалізуються з використанням штатних засобів.

Таблиця 2.1

Алгоритми знищення даних на магнітному носії з використанням штатних засобів

Алгоритм	**Зміст алгоритму**	**Примітки**
Посібник із захисту інформації МО США (NISPO) Do 5220.22-M, 1995р.	Кількість циклів запису – 3: Цикл 1 - запис довільного коду; Цикл 2 - запис інвертованого коду; Цикл 3 - запис випадкових кодів.	NISPO забороняє використання цього алгоритму для знищення даних із грифом ЦТ Альтернативні способи (відповідно до NISPO): - розмагнічування; - фізичне

Алгоритм	Зміст алгоритму	Примітки
		руйнування
Стандарт VISR, 1999р. (Німеччина)	Кількість циклів запису – 3: Цикл 1 - запис нулів; Цикл 2 - запис одиниць; Цикл 3 - запис коду із чергуванням нулів і одиниць.	
Держстандарт Р 50739-95Г. (Росія)	Для класів захисту даних 1 ..3 кількість циклів запису – 2: Цикл 1 - запис нулів; Цикл 2 - запис випадкових кодів. Для класів захисту даних 4..6 кількість циклів запису – 1: Цикл 1 - запис нулів.	
Алгоритм Брюса Шнейера (Bruce Schneier)	Кількість циклів запису – 7: Цикл 1 - запис одиниць; Цикл 2 - запис нулів; Цикли 3..7 - запис випадкових кодів.	
Алгоритм Пітера Гутмана (Peter Gutman)	Кількість циклів – 35: Цикли 1 ..4 - запис довільного коду; Цикли 5..6 - запис кодів 55h, AAh; Цикли 7..9 - запис кодів 92h, 49h, 24h; Цикли 10..25 - послідовний запис кодів від 00, 11 h, 22h і т.д. до FFh; Цикли 26..28 - аналогічно циклам 7..9; Цикли 29..31 - запис коду 6Dh, B6h; Цикли 32..35 - аналогічно циклам 1..4.	

Головним недоліком цих алгоритмів є те, що будь-яка кількість перезаписів не може дати гарантій (гарантованої імовірності) знищення, і тому для знищення секретної інформації вони не використовуються.

Висока гарантія забезпечується лише при повному знищенні структури магнітного середовища, що здійснюється, як правило, з використанням позаштатних засобів. Способи знищення даних на

магнітному носії з використанням позаштатних засобів представлені в табл. 2.2.

Таблиця 2.2

Способи знищення даних на магнітному носії з використанням позаштатних засобів

Назва	Сутність	Особливості та гарантії
Механічний	Роздрібнювання носія, його руйнування механічним впливом.	Руйнуючий метод. Можливо гарантоване знищення.
Термічний	Нагрівання носія до температури руйнування його основи (або до точки Кюрі).	Руйнуючий метод. Гарантоване знищення.
Піротехнічний	Руйнування носія вибухом.	Руйнуючий метод. Можливо гарантоване знищення. Проблема забезпечення безпеки оператора.
Металотермічний	Знищення основи носія високою температурою високотемпературним синтезом, що самопоширюється.	Руйнуючий метод. Гарантоване знищення.
Хімічний	Руйнування робочого шару або основи носія хімічно агресивними речовинами.	Руйнуючий метод. Гарантоване знищення. Проблема забезпечення безпеки оператора.
Радіаційний	Руйнування носія іонізуючими випромінюваннями.	Руйнуючий метод. Небезпека опромінення.
Електромагнітний	Вплив сильного електромагнітного поля на магнітне середовище	Руйнуючий метод. Гарантоване знищення.

Перелік питань для самоконтролю

1. Класифікація каналів зв’язку та основні способи перехоплення інформації в них.
2. Особливості витоку візуальної інформації та заходи по запобіганню витоку.
3. Сутність матеріально-речовинних каналів витоку інформації.
4. Методи знищення інформації на магнітних носіях.
5. Методи гарантованого знищення інформації на магнітних носіях.

3. СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

3.1. Створення комплексів технічного захисту інформації. Загальні положення

Технічний захист інформації (ТЗІ) є невід'ємною складовою частиною системи забезпечення національної безпеки України в інформаційній сфері і представлений як діяльність, що спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації в інформаційно-телекомунікаційних, інформаційних, телекомунікаційних, автоматизованих системах і на об'єктах інформаційної діяльності.

Економічно обґрунтовані комплекси і системи захисту інформації будуються адекватно загрозам її безпеки, що описуються у відповідних моделях.

Для захисту інформації від витоку технічними каналами на об’єктах інформаційної діяльності або в складі комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах створюються комплекси ТЗІ.

Комплекс ТЗІ – сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті інформаційної діяльності. [23]

Комплекси ТЗІ створюють на ОІД, де передбачається:

– озвучення інформації з обмеженим доступом (ІзОД) при проведенні нарад, показів зі звуковим супроводженням кіно- і відеофільмів тощо;

– здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання тощо);

– обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

Створення комплексів ТЗІ на ОІД є складним та багатогранним завданням і для досягнення головної мети (забезпечення безпеки інформації на ОІД) в інтересах суб’єктів-замовників вимагає певних кваліфікацій та зобов’язань суб’єктів-виконавців. Так для здійснення відповідних робіт зі створення комплексу ТЗІ та розподілу юридичної відповідальності виділяють таких суб’єктів створення комплексу ТЗІ:

– **установа-замовник** – установа, яка є замовником та в інтересах якого створюється комплекс ТЗІ;

– **підрозділ-заявник** – структурний підрозділ в установі, що обґрунтовує необхідність і заявляє про створення комплексу ТЗІ;

– **підрозділ ТЗІ (організатор) –** підрозділ (фахівець, група фахівців), якому доручено організацію і супроводження робіт зі створення комплексу ТЗІ в установі (можливо суб’єкт господарської діяльності);

– **виконавець спеціальних досліджень ТЗС –** підрозділ (або суб’єкт господарювання), який здійснює спеціальні дослідження ТЗС;

– **виконавець робіт –** підрозділ, який здійснює упровадження комплексу ТЗІ;

– **виконавець атестації** – підрозділ (суб’єкт господарювання), який виконує атестацію комплексу ТЗІ.

Слід відмітити, що суб’єкти господарської діяльності, які залучаються для атестації комплексів ТЗІ, повинні мати відповідну ліцензію для надання послуг у галузі ТЗІ.

Створення комплексів ТЗІ – це сукупність різноманітних та логічно пов’язаних дій та заходів із знаходження та впровадження оптимальних рішень, достатніх для забезпечення захищеності інформації від витоку технічними.

Підставою для створення комплексу ТЗІ є відповідне рішення керівника установи-замовника. При цьому, споруді, де планується створення комплексу ТЗІ, розпорядчим документом надається статус ОІД та призначається відповідальна особа для організації, супроводження та координації робіт на всіх етапах цього створення;

При цьому враховуються:

– пропозиції від заявників щодо організації створення комплексів захисту;

– відомості про діючі ОІД та створені в установі комплекси ТЗІ;

– перспективи подальших робіт з ТЗІ в установі;

– технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ.

Рішення щодо необхідності створення (модернізації) комплексу ТЗІ готує підрозділ-заявник на стадіях проектування, нового будівництва, розширення, реконструкції ОІД, а також у разі змін умов функціонування ОІД (далі будівництва ОІД).

Будівництво ОІД може виконуватися за відповідною проектно-кошторисною документацією. При цьому повинні бути враховані вимоги державних будівельних норм (ДБН А.2.2-2 і ДБН А.2.2-3).

Комплекс ТЗІ повинен створюватися, виходячи із перспектив модернізації і розвитку інших комплексів ТЗІ установи, охоронних, протипожежних або загальних систем безпеки установи, спеціальних систем енергоспоживання, життєзабезпечення тощо, а також забезпечувати виконання норм ефективності захищеності інформації, відповідати експлуатаційним вимогам щодо необхідності та періодичності перевірок цієї захищеності.

Для створення комплексу ТЗІ можуть використовуються засоби ТЗІ, які мають (або мали на момент їх виготовлення) чинний документ (сертифікат відповідності або експертний висновок у сфері ТЗІ), що підтверджує їх відповідність у сфері ТЗІ.

Застосування засобів ТЗІ іноземного виробництва можливе за умови відсутності вітчизняних аналогів при наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або державної експертизи у сфері ТЗІ.

Джерела фінансування робіт зі створення комплексу ТЗІ визначає замовник.

Витрати на проектування, будівельно-монтажні роботи, проведення випробувань щодо ТЗІ, атестації комплексу ТЗІ вносяться до кошторису на будівництво та експлуатацію (утримання) ОІД.

Дозвіл на здійснення озвучення та/або обробки технічними засобами ІзОД (окрім обробки ІзОД в ІТС) надається керівником установи-замовника за наявності Акта атестації та Паспорта на комплекс ТЗІ (з паспортами на приміщення ОІД в додатках).

Дозвіл на експлуатацію ІТС, технічні засоби яких розміщуються на ОІД, надається керівником установи-замовника за наявності Атестата відповідності на комплексну систему захисту інформації в ІТС, який оформляється за результатами проведення державної експертизи у сфері ТЗІ (окреме питання).

Створення комплексу ТЗІ передбачає три етапи:

- розроблення комплексу ТЗІ (І етап);
- упровадження комплексу ТЗІ (ІІ етап);
- атестацію комплексу ТЗІ (ІІІ етап).

Зміст та порядок робіт на етапах створення комплексу ТЗІ визначається нормативними документами системи ТЗІ.

Вимоги до захищеності інформації від витоку технічними каналами та норми захищеності інформації визначаються нормативно-правовими актами та нормативними документами системи ТЗІ.

Перелік питань для самоконтролю

1. Поняття комплексу ТЗІ.
2. Суб’єкти створення комплексу ТЗІ.
3. Визначення понять атестації комплексу ТЗІ.
4. Вимоги до засобів ТЗІ, що використовуються при створені комплексів ТЗІ.
5. Етапи створення комплексу ТЗІ.

3.2. Розроблення комплексу ТЗІ

Розроблення комплексу ТЗІ складається з передпроектних робіт та розроблення технічного проекту комплексу ТЗІ.

3.2.1. Передпроектні роботи

Передпроектні роботи передбачають такі заходи:

- категоріювання ОІД;
- обстеження ОІД;
- спеціальні дослідження ОТЗІ;
- спеціальні дослідження ОІД (проводяться у разі створення комплексу ТЗІ для захисту мовної інформації);
- інженерний аналіз ДТЗС (або спеціальні дослідження ДТЗС);
- розроблення моделі загроз для інформації;
- розроблення технічного завдання на створення комплексу ТЗІ.

Категоріювання ОІД здійснюється згідно з нормативними документами системи ТЗІ (НД ТЗІ). За результатами категоріювання складається акт категоріювання ОІД.

Обстеження ОІД передбачає аналіз ОІД та визначення характеристик (параметрів) ОІД та розміщених на ньому технічних засобів, їх комунікацій, інженерних комунікацій, побутових засобів, предметів інтер’єру, сувенірів тощо, що обумовлюють можливість створення технічних каналів витоку інформації, а також підготовку вихідних даних для розробки моделі загроз для інформації та формування вимог до комплексу ТЗІ. За результатами складається акт обстеження ОІД. Форма за зміст акта визначається НД ТЗІ.

Спеціальні дослідження ОІД передбачають комплекс аналітичних, експериментальних та вимірювальних робіт з виявлення можливості створення технічних каналів витоку інформації, що озвучується,

попереднє визначення показників захищеності мовної інформації об’єкта та спеціальних вимог до умов його експлуатації.

Спеціальні дослідження ОТЗС передбачають комплекс аналітичних, експериментальних та вимірювальних робіт з визначення можливості створення технічних каналів витоку інформації цими ОТЗС та показників захищеності інформації (зони 1 та зони 2) цих ОТЗС. За результатами складається протокол спеціальних досліджень ОТЗС та визначаються спеціальні вимоги до умов їх експлуатації.

При інженерному аналізі ДТЗС аналізується призначення, принцип дії, склад, взаємозв’язки складових ДТЗС тощо для визначення можливості (або неможливості) створення допоміжними технічними засобами та системами технічних каналів витоку інформації при розташуванні їх на ОІД. У разі недостатності інженерного аналізу здійснюються спеціальні дослідження ДТЗС.

Модель загроз для інформації розробляється та оформлюється згідно з НД ТЗІ. Модель загроз для інформації – це формалізований опис методів та засобів здійснення загроз для інформації і схематичне подання шляхів їх здійснення. Вихідними даними для розроблення моделі загроз для інформації є матеріали акта категоріювання ОІД, акта обстеження ОІД, результати спеціальних досліджень ОІД або ОТЗС, ДТЗС (інженерного аналізу ДТЗС). Модель загроз містить таки структурні елементи:

– ситуаційний план ОІД та його опис;

– генеральний план ОІД та його опис;

– схему розташування та опис ОТЗС;

– схему розташування та опис ДТЗС;

– обґрунтування можливості створення технічних каналів витоку інформації, властивих даному ОІД;

– висновки: перелік технічних каналів витоку інформації, які можуть бути утворені на даному ОІД.

На ситуаційному плані ОІД вказується (та описується) розташування на місцевості будинку, де знаходиться ОІД, та оточуючих об’єктів.

На генеральному плані вказується (та описується) об’єкт інформаційної діяльності на плані будинку, де знаходиться ОІД, суміжні приміщення, системи електроживлення, заземлення, безпеки, охорони, сигналізації, життєзабезпечення тощо.

Технічне завдання (ТЗ) на створення комплексу ТЗІ розробляється згідно з НД ТЗІ. Вихідними даними для розроблення ТЗ є результати обстеження ОІД, загрози для інформації (можливі технічні канали витоку інформації), що визначені в моделі загроз для інформації, результати спеціальних досліджень ОТЗ, результати інженерного аналізу ДТЗС (або результати спеціальних досліджень ДТЗС), результати спеціальних досліджень ОІД та спеціальні вимоги до умов експлуатації ОІД (у разі створення комплексу ТЗІ для захисту інформації, що озвучується на ОІД), а також встановлені нормативними документами з питань ТЗІ вимоги до захисту інформації від витоку відповідними технічними каналами. Технічне завдання на створення комплексу ТЗІ містить загрози для інформації (перелік технічних каналів витоку інформації, які властиві даному ОІД), технічні вимоги та вимоги до документації, яка має бути розроблена для (під час) створення комплексу ТЗІ, а також вимоги до засобів ТЗІ, їх монтажу, електроживлення та заземлення та вимоги щодо забезпечення охорони державної таємниці. Технічні вимоги містять потрібні способи (методи) захисту інформації від витоку кожним властивим даному ОІД технічним каналом та вимоги стосовно норм, яким має відповідати захищеність інформації від витоку відповідним технічним каналом.

3.2.2. Розроблення технічного проекту комплексу ТЗІ

Технічний проект комплексу ТЗІ розробляється виконавцем робіт з ТЗІ відповідно до вимог ТЗ на створення комплексу ТЗІ та НД ТЗІ.

При розробці технічного проекту обґрунтовуються і приймаються проектні рішення, які дозволяють реалізувати вимоги ТЗ на створення комплексу та НД ТЗІ щодо захисту інформації від витоку технічними каналами. Номенклатура документації технічного проекту комплексу ТЗІ визначається в ТЗ на створення комплексу ТЗІ. Зокрема розробляється пояснювальна записка з ТЗІ, яка містить призначення комплексу ТЗІ, варіант захисту інформації та його обґрунтування, специфікацію комплексу ТЗІ, креслення комплексу ТЗІ, розрахунки характеристик комплексу ТЗІ та показників захищеності інформації.

Проектування, нове будівництво або реконструкція (далі – будівництво) ОІД, де оброблятиметься технічними засобами та/або озвучуватиметься секретна інформація, здійснюються з урахуванням вимог ДБН А.2.2-2-96 та ДБН А.2.2-3-2004.

Проектно-кошторисна документація розробляється згідно з вимогами ДБН А.2.2-2 і ДБН А.2.2-3 виконавцем робіт з ТЗІ за рішенням замовника. При будівництві (реконструкції) ОІД заходи з ТЗІ відображаються за напрямами у відповідних проектно-кошторисних документах: у будівельних кресленнях, планах території, споруд, приміщень, на схемах електроживлення, зв’язку, опалення, вентиляції тощо.

Перелік питань для самоконтролю

1. Зміст першого етапу створення комплексу ТЗІ.
2. Зміст передпроектних робіт.
3. Категоріювання ОІД.

4. Обстеження ОІД.
5. Спеціальні дослідження ОІД.
6. Спеціальні дослідження ОТЗС.
7. Інженерний аналіз та спеціальні дослідження ДТЗС.
8. модель загроз для інформації.
9. Технічне завдання на створення комплексу ТЗІ.
10. Розроблення технічного проекту комплексу ТЗІ

3.3. Упровадження комплексу ТЗІ

Упровадження комплексу ТЗІ передбачає придбання (закупівлю) засобів ТЗІ та іншого обладнання, монтаж та налагодження (настроювання) засобів ТЗІ, розробку технічної та експлуатаційної документації на комплекс ТЗІ.

Упровадження комплексу ТЗІ містить такі роботи:

розробку (за рішенням замовника) та погодження із замовником плану робіт з упровадження заходів із захисту інформації на ОІД;

придбання (закупівлю) за погодженням з замовником засобів ТЗІ та іншого обладнання;

архітектурно-будівельні та монтажні роботи (за необхідності);

впровадження на ОІД заходів та встановлення і налагоджування (настроювання) засобів ТЗІ відповідно до технічного проекту комплексу ТЗІ та іншої проектної документації;

розроблення експлуатаційної та іншої технічної документації (в тому числі паспорта на комплекс ТЗІ та припису на експлуатацію ОІД).

Впровадження на ОІД заходів та встановлення і налагоджування (настроювання) засобів ТЗІ здійснюється відповідно до технічного проекту комплексу ТЗІ та іншої проектної документації, плану робіт з впровадження заходів із захисту інформації на ОІД, а також відповідно до технічної та експлуатаційної документації засобів ТЗІ.

Перелік питань для самоконтролю

1. Сутність упровадження комплексу ТЗІ.
2. Роботи з упровадження комплексу ТЗІ.

3.4. Атестація комплексу ТЗІ

Атестація комплексу ТЗІ передбачає:

– здійснення інструментального контролю захищеності інформації;

– проведення перевірки повноти і відповідності реалізованих на ОІД заходів із захисту інформації від витоку властивими конкретному ОІД технічними каналами вимогам ТЗ на створення комплексу ТЗІ та вимогам НД ТЗІ;

– оформлення, затвердження та організація реєстрації Акта атестації комплексу ТЗІ.

Атестація комплексу ТЗІ буває первинною, черговою та позачерговою.

Первинна атестація проводиться при завершенні створення комплексу ТЗІ.

Чергова атестація проводиться при завершенні строку дії акта попередньої (первинної або чергової) атестації. Термін проведення чергової атестації вказується в акті атестації та паспорті на комплекс ТЗІ.

Позачергова атестація проводиться у разі змін умов функціонування ОІД, що призводять до змін загроз для інформації. Позачергова атестація також проводитися, якщо така необхідність визначена за результатами державного контролю за станом ТЗІ.

Атестація комплексу ТЗІ включає такі роботи:

розроблення, погодження та затвердження програми та методики атестації комплексу ТЗІ;

інструментальний контроль захищеності інформації від витоку властивими даному ОІД технічними каналами та оформлення протоколу інструментального контролю захищеності інформації;

перевірку правильності встановлення категорії ОІД;

перевірку виконання етапів створення комплексу ТЗІ, що визначені НПА та НД ТЗІ (на основі перевірки наявності документів, що розробляються на етапах створення комплексу ТЗІ);

перевірку наявності, чинності та оцінку відповідності проектної, конструкторської, експлуатаційної та іншої технічної документації на комплекс ТЗІ вимогам НД ТЗІ та ТЗ на створення комплексу ТЗІ;

перевірку правильності визначення загроз інформації (технічних каналів витоку інформації, що властиві даному ОІД) в Моделі загроз для інформації;

перевірку коректності визначених в ТЗ на створення комплексу ТЗІ вимог до захисту інформації від витоку технічними каналами;

перевірку відповідності складу та реального розміщення ОТЗ, ДТЗС та сторонніх комунікацій на ОІД даним, зазначеним в моделі загроз для інформації та наведеним у паспорті на комплекс ТЗІ;

перевірку відповідності складу та розміщення комплексу ТЗІ (засобів ТЗІ, що входять до складу комплексу ТЗІ) даним, зазначеним у паспорті на комплекс ТЗІ;

перевірку наявності сертифікатів відповідності або експертних висновків у сфері ТЗІ на засоби ТЗІ, що входять до складу комплексу ТЗІ;

перевірку відповідності монтажу та умов експлуатації засобів ТЗІ вимогам проектної, конструкторської, експлуатаційної та іншої технічної документації;

аналіз результатів (протоколів) інструментального контролю захищеності інформації стосовно інструментального підтвердження відповідності показників захищеності інформації від витоку технічними каналами нормам захищеності інформації;

оцінку відповідності комплексу ТЗІ вимогам НД ТЗІ та ТЗ на створення комплексу ТЗІ;

оцінку відповідності рівня створеного комплексу ТЗІ сучасному стану науки і техніки у сфері ТЗІ;

оформлення, затвердження та організація реєстрації Акта атестації комплексу ТЗІ.

За результатами атестації складається акт атестації комплексу ТЗІ.

Акт атестації містить:

– загальні відомості про ОІД та інформаційну діяльність на ньому;

– прелік документів нормативно-правових актів та НД ТЗІ, згідно з якими проводилась атестація комплексу ТЗІ;

– перелік проектних, конструкторських, експлуатаційних та інших технічних документів, наданих для проведення атестації комплексу ТЗІ;

– результати перевірок, які здійснювалися при атестації комплексу ТЗІ;

– висновки щодо відповідності показників захищеності інформації від витоку кожним з технічних каналів, які властиві даному ОІД, нормам захищеності інформації;

– висновки за результатами атестації щодо відповідності комплексу ТЗІ вимогам ТЗ на цей комплекс та вимогам НД ТЗІ;

– термін проведення чергової атестації (строк дії акта атестації);

– рекомендації з експлуатації комплексу ТЗІ (за необхідністю);

– умови проведення позачергової атестації комплексу ТЗІ.

Перелік питань для самоконтролю

1. Сутність атестації комплексів ТЗІ.
2. Види атестації комплексів ТЗІ.
3. Роботи з атестації комплексу ТЗІ.
4. Зміст акта атестації комплексу ТЗІ.

3.5. Будівельні норми на приміщення для зберігання секретних документів та роботи з ними

3.5.1. Загальні положення та вимоги щодо розміщення режимних приміщень

Проектування режимних приміщень здійснюється з дотриманням вимог “Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях”, затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 року № 939.

При розробці проектної документації на об’єкт будівництва або реконструкції, в якому передбачається розміщення режимних приміщень, поряд з цими Нормами слід враховувати вимоги і рекомендації чинних нормативних документів у галузі будівництва, а також нормативних актів органів державного нагляду щодо приміщень з постійним перебуванням людей.

При наявності в режимних приміщеннях персональних електронно-обчислювальних машин (ПЕОМ) слід керуватись вимогами ДНАОП 0.00-1.31, якщо вони не суперечать вимогам цих Норм.

Режимні приміщення розміщуються в громадських будинках та спорудах, будівлях виробничого та адміністративного призначення I або II ступенів вогнестійкості за ДБН В.1.1-7.

Режимні приміщення в багатоповерхових будівлях слід розміщувати, як правило, не нижче другого і не вище передостаннього (не враховуючи технічного) поверху.

Взаємопов’язані за функціональними ознаками режимні приміщення повинні розміщуватись групами і мати загальні для групи входи зі сторони загального коридору.

При розміщенні режимних приміщень слід враховувати, що біля їх вікон не повинно бути пожежних драбин, водостічних труб, балконів, покрівель прибудов та інших будівельних елементів (карнизів, виступів стін тощо), з яких можливе проникнення через вікна сторонніх осіб.

Розміщення обладнання, технічних засобів в режимних приміщеннях повинно відповідати вимогам з технічного захисту інформації, безпеки праці, санітарним нормам та відповідати вимогам пожежної безпеки.

3.5.2. Вимоги до будівельних конструкцій режимних приміщень

До будівельних конструкцій приміщення відносять перегородки (стіни), перекриття (стелю, підлогу), двері та вікна.

Перегородки та перекриття, які відокремлюють режимні приміщення від інших приміщень, повинні бути бетонними, залізобетонними (монолітними або збірними) товщиною не менше ніж 80 мм або цегляними товщиною не менше ніж 120 мм.

Цегляні та бетонні конструкції армуються.

Горизонтальне армування цегляних конструкцій виконується сітками згідно СНіП 11-22, армування бетонних конструкцій – згідно вимогам СНіП 2.03.01.

У вертикальній площині бетонні та цегляні перегородки армуються зварною сіткою з арматури класу Вр-1 чарункою 50х50 мм, діаметром 4 мм, розкріпленою по периметру на суміжні конструкції через 40 мм та на анкери діаметром 12-20 мм влаштовані в тілі самої конструкції на глибину не менше ніж 120 мм, кроком 500 мм. Технологія виконання таких робіт для існуючих конструкцій рекомендована ДБН В.3.1-1.

Опорядження стін і підвісних стель (якщо вони необхідні) повинні бути із негорючих матеріалів.

Застосування для покриття підлог килимових матеріалів не допускається.

Індекс ізоляції повітряного шуму стінами, перекриттями і дверима, що відокремлюють режимні приміщення від інших приміщень, а також відокремлюють кабінет начальника режимно-секретного органу від інших приміщень, повинен бути не менше ніж 60 дБ.

Якщо конструкції дверей не забезпечують вказаної звукоізоляції – передбачати подвійні двері, які забезпечували б вказаний індекс ізоляції повітряного шуму.

Двері всіх режимних приміщень повинні бути однопільними. Вхідні двері в групу режимних приміщень з коридору повинні бути металевими або дерев'яними (із столярної плити), оббитими оцинкованим листовим залізом. Вхідні двері повинні мати сертифікат відповідності для забезпечення межі вогнестійкості 0,6 год.

Дерев'яні дверні коробки повинні бути укріплені у дверному прорізі сталевими скобами із смуги товщиною 3 мм, привареними до закладних деталей в отворі, металеві двірні коробки приварюються до цих закладних деталей. Кількість закладних деталей по висоті дверного отвору повинна бути не менше ніж 4, по ширині – не менше ніж 3.

Вхідні двері режимних приміщень обладнуються двома різними замками з не менше ніж двома комплектами ключів кожний.

Входи в режимні приміщення повинні обладнуватись внутрішніми засувами, автоматичними або кодовими замками, тощо, а також пристроями для опечатування.

Необхідність встановлення автоматичних контрольно-пропускних пунктів і турнікетів, кабін ручного обслуговування, механічних та напівавтоматичних кабін та проходів тощо встановлюється завданням на проектування.

У вікнах режимних приміщень повинні передбачатись пристрої, які не дозволяють оглядати приміщення зовні (штори, жалюзі і ін.), незалежно від поверху і наявності будівель, які розташовані напроти.

При розміщенні режимних приміщень на першому та останньому поверхах, а також за наявності конструктивних особливостей будівлі, які можуть бути використані для несанкціонованого проникнення до таких приміщень, у їх вікнах повинні бути передбачені стальні грати з прута діаметром 16 мм. Відстань між вертикальними прутами повинна бути 150 мм, між горизонтальними не більше ніж 400 мм.

Горизонтальними елементами грат допускається застосування стальної смуги, товщиною не менше ніж 5 мм.

Грати повинні бути приварені до закладних деталей у віконних прорізах. Відстань між закладними деталями повинна бути не більше ніж 600 мм.

Грати не повинні перешкоджати відчиненню вікон (фрамуг, кватирок) для провітрювання приміщень.

Проектне рішення на застосування інших конструкцій, сучасних матеріалів та пристроїв, погоджується зі Службою безпеки України.

Вікна режимних приміщень повинні бути відокремлені простінками від вікон інших приміщень. Ширина простінку між віконними прорізами, до якого примикає стіна або перегородка, що відокремлює режимне приміщення від інших приміщень, повинна бути не менше ніж 0,9 м від середини стіни (перегородки) в кожну сторону. При обладнанні режимних приміщень охоронною сигналізацією ця величина не може бути зменшена.

Через режимні приміщення забороняється прокладання транзитних трубопроводів, повітроводів та інших комунікацій без обов’язкового застосування на них вставок з ізоляційного матеріалу, або інших засобів технічного захисту, згідно з вимогами нормативних документів з технічного захисту інформації.

Режимні приміщення повинні мати природне і штучне освітлення відповідно до СНіП 11-4.

Всі режимні приміщення обладнуються аварійним освітленням.

В режимних приміщеннях забороняється встановлювати світильники з розсіювачами з горючих матеріалів.

Дотримання оптимальних параметрів повітряного середовища (температура та вологість) в режимних приміщеннях забезпечуються роботою систем опалення, вентиляції та кондиціонування повітря у відповідності з СНіП 2.04.05.

3.5.3. Вимоги щодо сигналізації в режимних приміщеннях

Режимні приміщення оснащуються охоронною сигналізацією, яка повинна бути виведена на пульт поста охорони будинку, групи приміщень, чергового по установі (підприємству) або пульт централізованого спостереження підрозділу охорони.

Типи та види охоронної сигналізації повинні відповідати встановленим Службою безпеки України вимогам.

Для живлення охоронної сигналізації у аварійних випадках повинне передбачатись автономне джерело живлення. Переключення на автономне джерело живлення повинно бути автоматичним.

Режимні приміщення повинні бути обладнанні автоматичною пожежною сигналізацією.

Необхідність встановлення спеціальних видів сигналізації, а також засобів електронного, оптичного і акустичного захисту передбачаються в завданні на проектування.

Перелік питань для самоконтролю

1. З дотриманням вимог яких документів відбувається проектування режимних приміщень?
2. Вимоги по розміщенню режимних приміщень.
3. Вимоги до будівельних конструкцій режимних приміщень.
4. Вимоги щодо сигналізації в режимних приміщеннях.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Богуш В.М., Юдин О.К. Інформаційна безпека держави. – К.: «МК-Прес», 2005.– 432с.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.
3. Проект Концепції інформаційної безпеки України. [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf. – Назва з екрану.
4. ДСТУ 3396.0-96.
5. ДСТУ 3396.1-96.
6. ДСТУ 3396.2-97.
7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
8. Закон України «Про Державну службу спеціального зв'язку та захисту інформації». [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/3475-15. – Назва з екрана.
9. Закон України «Про основи національної безпеки України».
10. Закон України «Про інформацію».
11. Закон України «Про державну таємницю».
12. Конституція України.
13. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126.
14. Основы информационной безопасности. Учебное пособие для вузов / Е.Б Белов, В.П. Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

15. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27 вересня 1999 року № 1229.

Для нотаток

Навчальне видання

Іванченко С.О., Гавриленко О.В., Липський О.А.,

Шевцов А.С.

ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. ПОРЯДОК СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

Відповідальний за випуск О.А. Липський

Комп'ютерна верстка С.О. Іванченко

Друк.арк. 3,1. Ум.-друк арк. 2,88. Обл.-вид.арк. 2,89.