МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ОЛЕСЯ ГОНЧАРА

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.

Конспект лекцій.

м. Дніпро

2022р.

Методи та засоби захисту інформації: Конспект лекцій / Укладач В.І. Стаценко.Друге навчальне видання. Дніпро

[Електронний ресурс]:

Репозиторій ФТФ ДНУ, 2022. – 132с..

Кафедра кібербезпеки та комп’ютерно-інтегрованих технологій

ПЕРЕДМОВА

Інформаційна сфера це системоутворюючий фактор життя сучасного суспільства, роль якої зростає з кожним роком. Вона. активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України, ЕС і інших країн.

У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потоками, яка загострюється на тлі глобалізаційних процесів. Вигравває той, хто не лише їх формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити розумну конфедиційність та цілісність своїх інформаційних ресурсів та доступ до необхідної інформації для прийняття важливих рішень, якість яких напряму залежить від повноти та цілісності інформації, яка була в наявності на момент прийняття рішення.

Сьогодні є дуже актуальним захист інформації у всіх сферах діяльності: в науці, бізнесі, на державній службі й навіть в особистому житті. Виходячи з аналізу властивостей інформації, стає очевидним, що при забезпеченні інформаційної безпеки об'єкта понад усе слід надійно захищати носії інформації від несанкціонованої та ненавмисної діяльності людей, пов'язаною з інформацією, що охороняється на об'єкті захисту. Серед засобів по захисту інформації важливе значення надається інженерно-технічному захисту інформації, що заснована на використанні технічних засобів та організаційних заходів.

В рамках вивчення дисципліни розглядаються загальні питання теорії інформаційної безпеки, основні положення технології збору інформації і ведення технічного знімання інформації, організаційне забезпечення інженерно-технічного захисту інформації, засоби інженерного захисту і технічної охорони об'єктів державних та комерційних структур.

Конспект лекцій передбачається для використання студентами, які цікавляться методами та засобами захисту інформації для подальшого використання в кар'єрі, розвитку власного бізнесу та створення стартапів.

1 ВИДИ, ДЖЕРЕЛА ТА НОСІЇ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЄ ЗАХИСТУ.

1.1 ІНФОРМАЦІЯ, ЯК ОБ'ЄКТ ЗАХИСТУ.

Згідно Закону України «Про інформацію», ***інформація*** **–** це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

В даному законі інформація розглядається як об'єкт правових відносин:

1) Інформація може бути об'єктом публічних, громадянських та інших правових відносин. Інформація може вільно використовуватися будь-ким та передаватися, якщо законами не встановлені обмеження доступу до інформації або інші вимоги до порядку її надання і розповсюдження.
2) Інформація в залежності від категорії доступу до неї поділяється на загальнодоступну інформацію, а також на інформацію, доступ до якої обмежується законами (інформація обмеженого доступу).
3) Інформація в залежності від порядку її надання або поширення поділяється на інформацію:
   - вільно поширювану;
   - надається за згодою осіб, що беруть участь у відповідних відносинах;
   - підлягає наданню або поширенню в Україні;
   - обмежену або заборонену до поширення в Україні.
4) Законодавством України можуть бути встановлені види інформації в залежності від її змісту або володаря.

   Система захисту інформації в Україні являє собою сукупність правових, організаційних і технічних заходів, спрямованих:
   - на забезпечення захисту інформації від незаконного втручання, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій у відношенні такої інформації;
   - дотримання конфіденційності інформації обмеженого доступу,
   - реалізацію права на доступ до інформації.

   Володар інформації відповідно до законодавства України, зобов'язаний:
   - запобігати несанкціонованому доступу до інформації і (або) передачу її особам, які не мають права на доступ до інформації;
   - своєчасно виявляти факти несанкціонованого доступу до інформації;
   - попереджати можливість несприятливих наслідків порушення порядку доступу до інформації;
   - не допускати вплив на технічні засоби обробки інформації, в результаті якого порушується їх функціонування;
   - негайно відновлювати інформацію, модифіковану або знищену внаслідок несанкціонованого доступу до неї;
   - постійно контролювати рівень захищеності інформації.

Інформація як об'єкт має особливості:

- інформація нематеріальна в тому сенсі, що не можна виміряти її параметри, наприклад масу, розміри, енергію, відомими фізичними методами і приладами;

- інформація, записана на матеріальний носій, може зберігатися, оброблятися, передаватися по різних каналах зв'язку;

- будь-який матеріальний об'єкт містить інформацію про самого себе або про інші об'єкти.

З точки зору захисту, інформація має властивості, основні з яких наступні:

1. Інформація доступна людині, якщо вона зберігається на матеріальному носії. Так як за допомогою матеріальних засобів можна захищати тільки матеріальний об'єкт, то об'єктом захисту є матеріальні носії інформації. Розрізняють носії та джерела інформації, носії-переносники і носії-одержувачі інформації. Так, креслення є джерелом інформації, а папір, на якому він намальований, - носієм інформації. Фізична природа джерела і носія в цьому прикладі одна і та ж - папір. Однак між ними існує різниця. Папір без нанесеного на неї тексту або малюнка може бути джерелом інформації про її фізичні і хімічні характеристики. Коли папір містить семантичну інформацію, їй присвоюється інше ім'я: креслення, документ і т. п.

2. Цінність інформації оцінюється ступенем корисності її для користувача. Інформація може забезпечити її власнику певну перевагу (принести прибуток, зменшити ризик діяльності в результаті прийняття більш обґрунтованих рішень). Корисність інформації завжди конкретна, немає корисної інформації взагалі. Інформація або корисна, або шкідлива для конкретного користувача.

Шкідливою є інформація, в результаті використання якої її одержувачу наноситься моральна чи матеріальна шкода. Коли така інформація створюється навмисно, то її називають дезінформацією.

Часто шкідлива інформація створюється в результаті цілеспрямованої або випадкової модифікації її при перенесенні з одного носія на інший. Якщо в якості таких носіїв виступають люди, то шкідлива інформація циркулює у вигляді чуток. Широко практикується спосіб дезінформування людей шляхом використання механізму поширення чуток.

В інтересах захисту цінної (корисної) інформації її власник (держава, організація, фізична особа) наносить на носій умовний знак корисності інформації, що міститься на ньому - гриф секретності або конфіденційності.

3. Так як інформація може бути для одержувача корисною чи шкідливою, її можна розглядати як товар.

Ціна інформації пов'язана з її цінністю, але це різні поняття. Так, при проведенні досліджень можуть бути витрачені великі матеріальні і фінансові ресурси, які завершилися негативним результатом, тобто не отримується інформація, на основі якої її власник може отримати прибуток. Але негативні результати представляють цінність для фахівців, що займаються даної проблемою, так як отримана інформація вкорочує шлях до істини.

Корисна інформація може бути створена її власником в результаті науково-дослідницької діяльності, запозичена з різних відкритих джерел, може потрапити до зловмисника випадково, наприклад в результаті ненавмисного підслуховування і, нарешті, здобута різними нелегальними шляхами. Ціна інформації, як будь-якого товару, складається з собівартості і прибутку.

Собівартість інформації визначається витратами власника інформації на її отримання:

- шляхом проведення досліджень в наукових лабораторіях, аналітичних центрах, групах;

- покупки інформації на ринку інформації;

- добування інформації протиправними діями.

Прибуток від інформації через її особливості може приймати різні форми, причому грошове її вираження не є найпоширенішою формою. У загальному випадку прибуток від інформації може бути отриманий в результаті наступних дій:

- продажу інформації на ринку;

- матеріалізації інформації в продукцію з новими властивостями або технології, які приносять прибуток;

- використання інформації для прийняття більш ефективних рішень.

Остання форма прибутку від інформації не настільки очевидна, але вона найпоширеніша. Для прийняття будь-якого рішення необхідна інформація, причому, чим вище ризик і ціна рішення, тим більшого обсягу повинна бути інформація. Роздуми перед прийняттям рішення є нічим іншим, як переробка людиною наявної у нього інформації. З власного досвіду кожен знає, як важко прийняти відповідальне рішення в умовах дефіциту інформації або часу.

4. Цінність інформації змінюється в часі. Залежно від тривалості життєвого циклу комерційна інформація класифікується наступним чином:

• оперативно-тактична (втрачає 10% вартості в день);

• стратегічна (втрачає 10% вартості в місяць).

5. Неможливо об'єктивно оцінити кількість інформації. Кількість інформації, що міститься, наприклад в підручнику, для різних читачів - різна. Навіть одна й та сама людина в різні періоди свого життя знаходить у підручнику кожен раз щось нове для себе. Кількість інформації в голові людини можна побічно оцінити по його діям, так як для прийняття обґрунтованого рішення необхідно більше інформації.

6. При копіюванні, інформаційний параметр носія не змінюється, кількість інформації не змінюється, а ціна падає.

Після зняття копії з документа на ксероксі або іншим способом кількість інформації в ньому не змінюється. В результаті цього несанкціоноване копіювання (розкрадання) інформації може залишитися непоміченим для її власника, якщо відсутні інші ознаки проникнення зловмисника до її джерела і факту розкрадання. Але якщо при копіюванні відбувається вплив на інформаційні параметри носія, що приводить до зміни їх значень, або незначні зміни накопичуються, то кількість інформації зменшується. Погіршується якість звуку і зображення відповідно на аудіо- та відеоплівку через механічне руйнування магнітного шару, книжка зачитується до дірок, знебарвлюються через вплив яскравого ультрафіолетового світла кольори зображення оригіналу при ксерокопіюванні і т.п.

Так як при кожному копіюванні збільшується число її законних і незаконних користувачів, то відповідно до законів ринку ціна знижується.

Види інформації, яка захищається технічними засобами

За змістом (мал.1.1) будь-яка інформація може бути віднесена до ***семантичної*** (в перекладі з латинської - містить сенс) або до інформації про ознаки матеріального об'єкта - ***ознаковою***. Сутність ***семантичної інформації*** не залежить від характеристик носія.

Зміст тексту, наприклад, не залежить від якості паперу, на якому він написаний, або фізичних параметрів іншого носія.

Семантична інформація - продукт абстрактного мислення людини. Вона відображає об'єкти, явища як матеріального світу, так і створювані ним образи і моделі за допомогою символів на мовах спілкування людей.

Мал. 1.1. Класифікація інформації за змістом

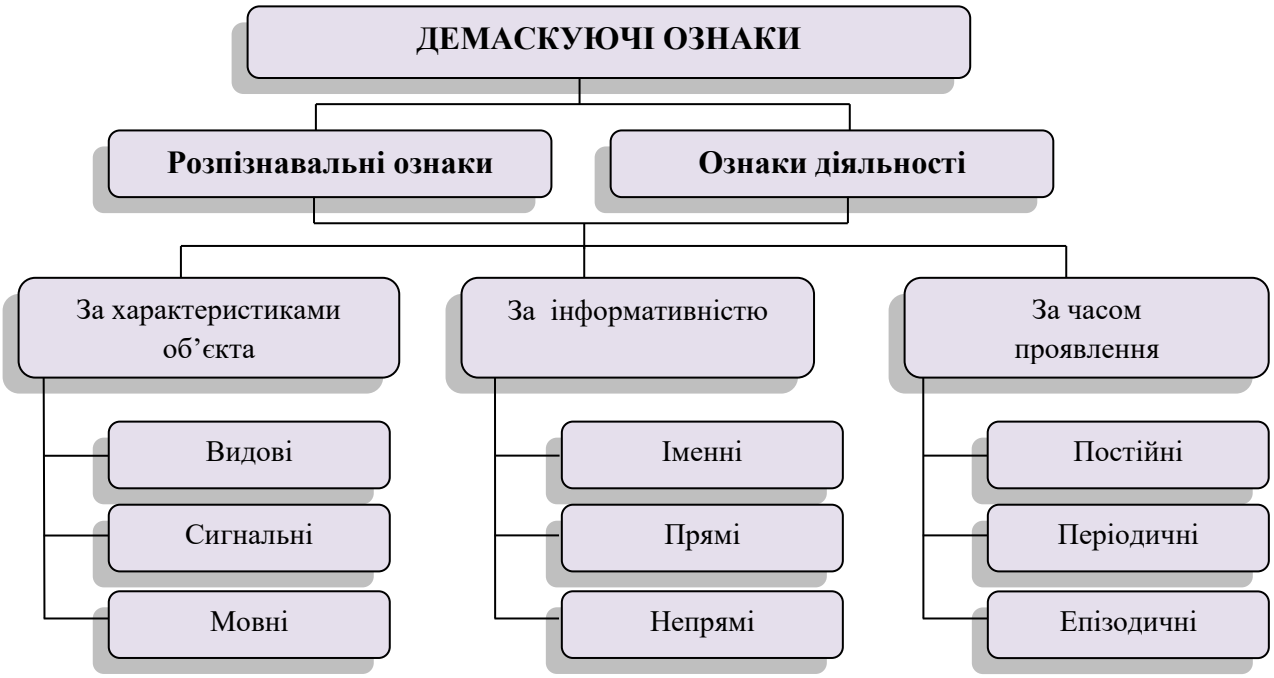
Ознакова інформація описує конкретний матеріальний об'єкт на мові його ознак. Джерелом інформації цього об'єкта є сам об'єкт. Залежно від виду опису об'єкта ознакова інформація ділиться на інформацію про зовнішній вигляд (зовнішні ознаки), про його поля (ознаки сигналів), про структуру і склад його речовин (ознак речовини).

1.2 ДЕМАСКУЮЧІ ОЗНАКИ ОБ'ЄКТІВ ЗАХИСТУ.

Ознаки, що дозволяють відрізнити один об'єкт від іншого, називаються ***демаскуючими***. Демаскуючі ознаки об'єкта становлять частину його ознак, а значення їх відрізняються від значень відповідних ознак інших об'єктів. Однакові ознаки різних об'єктів не належать до демаскуючих. Так, ознака «зріст людини» без вказівки його значення не є демаскуючим, так як вона відноситься до всіх людей.

Демаскуючі ознаки об'єкта описують його різні стани, характеристики і властивості. У загальному випадку демаскуючі ознаки об'єктів поділяються на ***розпізнавальні ознаки*** і ***ознаки діяльності*** (мал.1.2.).

Розпізнавальні ознаки описують об'єкти в статичному стані: його призначення, приналежність, параметри. ***Ознаки діяльності*** об'єктів характеризують етапи і режими функціонування об'єктів, наприклад етапи створення нової продукції: наукові дослідження, підготовка до виробництва, виготовлення нової продукції, її випробування і т.п.



Мал. 1.2.1 Класифікація демаскуючих ознак

До ***видових ознак*** відносяться форма об'єкта, його розміри, деталі об'єкта, тон, колір, структура.

Таким чином, сукупність демаскуючих ознак трьох розглянутих груп є модель об'єкта, що описує його зовнішній вигляд, поля, що їм випромінюються, внутрішню структуру, хімічний склад речовин, які в ньому містяться.

Видові демаскуючі ознаки.

Видові демаскуючі ознаки описують зовнішній вигляд об'єкта (форма, розміри, деталі, тон, колір, структура об'єкта). Основними видовими демаскуючими ознаками об'єктів у

видимому світлі є фотометричні і геометричні характеристики об'єкта (тіні, дим, сліди на ґрунті, снігу, воді), взаємне розташування елементів групового об'єкта, розташування такого об'єкта щодо інших об'єктів, що захищаються.

Демаскуючі ознаки сигналів.

Ознаки сигналів описують параметри полів і електричних сигналів, що генеруються об'єктом (потужність, частота, ширина спектра).

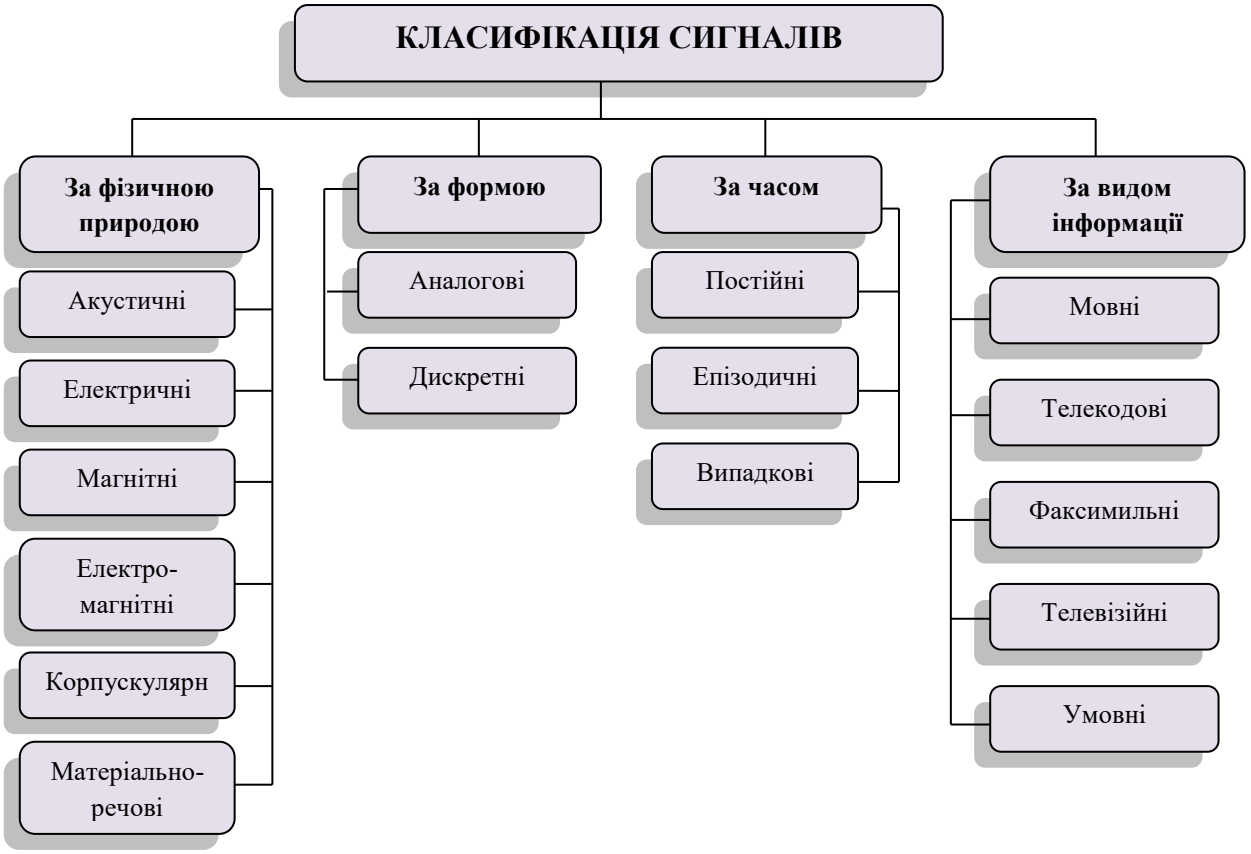
Сигнал – зміна фізичної величини (наприклад, температури, тиску повітря, світлового потоку, сили струму тощо), що використовується для пересилання даних. Саме завдяки цій зміні сигнал може нести в собі якусь інформацію. Сигнали можуть бути власні і відбиті. Класифікація сигналів представлена на мал. 1.2.2.

Власні сигнали - сигнали зумовлені фізичними процесами або станами об'єкта.

Відбиті сигнали - сигнали, зумовлені впливом навколишнього середовища.

Аналоговий сигнал може бути описаний наступними параметрами: частота / діапазон частот, фаза сигналу, тривалість сигналу, амплітуда або потужність сигналу, ширина спектру сигналу, динамічний діапазон.

У дискретних сигналах амплітуда має кінцевий, заздалегідь визначений набір значень. Дискретний сигнал характеризується амплітудою, потужністю, періодом виникнення сигналу і шириною спектру сигналу.



Мал. 1.2.2 Класифікація сигналів

Демаскуючі ознаки речовин.

Ознаки речовин визначають фізичний і хімічний склад, структуру і властивості речовин матеріального об'єкта.

Речовиною називається все, що складається із частинок одного або декількох хімічних елементів, знаходиться в твердому, рідкому, газоподібному стані, має масу і об'єм.

Для забезпечення безпеки інформації про речовини з новими властивостями важливо представляти ознаки, за якими зловмисник може відтворити речовину з новими властивостями.

Класифікація основних ознак речовин представлена на мал.1.2.3.

Ознаки, за якими можна визначити чи розпізнати (тобто визначити склад, структуру і властивості) речовини, є демаскуючими ознаками речовини. Демаскуючі ознаки нової речовини і технологія її виготовлення містяться не тільки в кінцевому продукті, а й в проміжних продуктах технологічного процесу отримання цієї речовини. Речовини, що містять демаскуючі ознаки іншої речовини, називаються демаскуючими речовинами.

Мал. 1.2.3 Класифікація основних ознак речовини

1.3 ДЖЕРЕЛА ТА НОСІЇ ІНФОРМАЦІЇ, ЩО ЗАХИЩАЄТЬСЯ ТЕХНІЧНИМИ ЗАСОБАМИ.

Джерелами інформації є суб'єкти та об'єкти, від яких інформація може надійти до несанкціонованого користувача.

Основними джерелами інформації є:

- люди (фізичні особи);
- документи;
- продукція;
- вимірювальні прилади і датчики;
- інтелектуальні засоби обробки інформації;
- чернетки і відходи виробництва;
- матеріали і технічне обладнання.

Люди, як джерела інформації, є найбільш інформативними, хоча їх інформативність істотно градуюється в залежності від соціального стану, освіти, займаної посади, доступу до відомостей, та інших чинників.

Документи - зафіксована на матеріальному носії інформація з реквізитами, що дозволяє однозначно його ідентифікувати. Тому документи відносяться до найбільш достовірних інформаційних джерел.

Більшість технічних засобів збору, обробки, передачі, зберігання інформації можна віднести до джерел інформації, так як вони представляють собою лише інструмент для перетворення вхідної інформації. Критерієм віднесення технічного засобу до джерела інформації може служити відповідь на питання споживача інформації про її джерело. Винятком є датчики різних вимірювальних систем.

Продукція без документації є джерелом ознакової інформації. Для отримання інформації про внутрішній зміст продукції її необхідно додатково дослідити і вивчити, наприклад методами зворотнього інжинірингу (вівісекції).

Вимірювальні прилади є найбільш якісним засобом отримання інформації про досліджуваний об'єкт з точністю певної похибки.

Інтелектуальні засоби обробки інформації в даний час до джерел інформації відносяться вельми умовно. Так, навіть найпотужніший комп'ютер виконує при обробці інформації лише програму, розроблену людиною. Повною мірою інтелектуальні засоби обробки можна буде віднести до джерел інформації зі створенням досконалих систем штучного інтелекту.

Відходи є джерелом обмеженого поширення, тому що містять фрагменти інформаційного портрета реальної діяльності або продукту.

Містити конфіденційну інформацію можуть також вихідні матеріали та технічне обладнання. Так, за номенклатурою матеріалу і технічного обладнання можна судити про те, що випускається на підприємстві.

Таким чином, джерелом конфіденційної інформації можуть бути як фізичні особи, так і різні об'єкти. У рідкісних випадках інформація від джерела безпосередньо передається одержувачу. Як правило, для добування інформації між джерелом і одержувачем інформації існує посередник - носій інформації, який дозволяє організувати розвідку або отримувати зловмисникові інформацію дистанційно, в більш безпечних умовах.

Носіями інформації є матеріальні об'єкти, що забезпечують запис, зберігання і передачу інформації в просторі і часі.

Відомо 4 види носіїв інформації: ***люди, матеріальні тіла, поля, елементарні частинки***.

Джерела сигналів.

Більшість систем обробки інформації в процесі своєї діяльності випромінюють сигнали, тобто містять джерела сигналів. Якщо об'єкт відбиває поля зовнішніх джерел, то він одночасно є джерелом інформації про об'єкт і джерелом сигналу. Коли на вхід джерела сигналу надходить первинний сигнал, наприклад акустична хвиля від людини, що говорить, то джерело сигналу, що переписує інформацію з одного носія (акустичної хвилі) на інший (електромагнітне поле) в зв'язку називається ***передавачем***. Джерела сигналів, що створюються і прийняті для забезпечення зв'язку між санкціонованими абонентами, називають ***функціональними джерелами сигналів***. Джерела сигналів, що несанкціоновано передають конфіденційну інформацію, називаються ***небезпечними***. Як правило, функціональні джерела також можна віднести до небезпечних.

До ***джерел функціональних сигналів*** відносяться:

- передавачі систем зв'язку;
- передавачі радіотехнічних систем;
- випромінювачі акустичних сигналів гідролокатором;
- умовні сигнали.

Серед радіотехнічних систем і засобів значну частку займають радіолокаційні станції. Радіонавігаційні засоби і системи призначені для визначення місця розташування об'єктів на суші, у воді і в космосі. Об'єктами захисту інформації (ЗІ) тут будуть характеристики радіотехнічних систем.

Передача коротких повідомлень проводиться за допомогою умовних сигналів. У якості сигналів можуть використовуватися будь-які об'єкти спостереження, останнім часом для передачі інформації застосовуються лазери оптичних систем зв'язку. Поступаючись радіосигналам по дальності поширення (особливо в несприятливих кліматичних умовах), оптичні системи зв'язку мають кращі показники по завадостійкості.

Побічні випромінювання і наводки.

Побічні випромінювання і наводки виникають при роботі апаратури і при передачі сигналів випадково. Якщо ці сигнали містять інформацію, що захищається, то їх відносять до ***небезпечних***. Всі засоби, які випромінюють побічні наводки, діляться на дві групи:

1. Основні технічні засоби і системи (ОТЗС), що забезпечують обробку, зберігання та передачу інформації, що захищається;

2. Допоміжні технічні засоби і системи (ДТЗС)

До **основних технічних засобів і систем** відносяться:

• засоби міської телефонної мережі, розміщені на території організації;
• внутрішньооб'єктова автоматична телефонна мережа;
• обчислювальна техніка (ПЕОМ, принтери, сканери, сервери);
• апаратура передачі даних;
• засоби телеграфного та факсимільного зв'язку;
• система об'єктового промислового телебачення;
• засоби аудіо- та відеозапису, які використовуються для документування інформації, що захищається.
• та ін.

Допоміжні технічні засоби і системи включають:

• міську і об'єктову радіотрансляційну мережу;
• систему електрочасофікації;
• технічні засоби охоронної та пожежної сигналізації;
• телевізійні засоби системи охорони об'єкта;
• побутову техніку
• та ін.

Незважаючи на різноманіття технічні засоби і системи можна класифікувати виходячи з їх фізичної природи наступним чином:

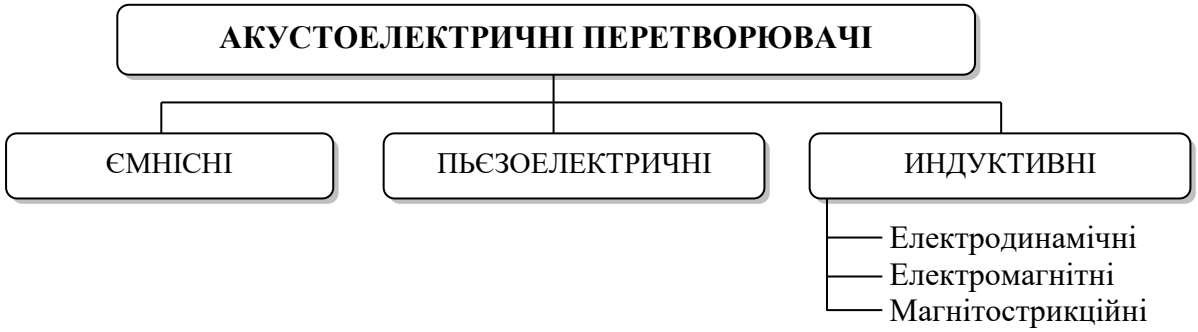
• акустоелектричні перетворювачі;

• випромінювачі низькочастотних сигналів;

• випромінювачі високочастотних сигналів;

• паразитні зв'язки і наводки.

До ***акустоелектричних*** перетворювачів відносяться фізичні пристрої, конструктивні елементи яких здатні під дією змінного тиску акустичної хвилі створювати еквівалентні електричні сигнали. (Мал. 1.3.)



Мал.1.3. Класифікація акустоелектричних перетворювачів

Перелік побутових радіоприладів, в яких виникають подібні процеси, досить великий. До них відносяться:

• телефонні апарати,

• телефонні апарати з електромеханічними дзвінками,

• електричний годинник системи єдиного часу,

• вентилятори, гучномовці.

Магнітострикція проявляється зміною магнітних властивостей феромагнітних речовин і їх сплавів при їх деформації.

Небезпечні сигнали на виході акустоелектричних перетворювачів можуть поширюватися по проводах, які виходять за межі контрольованої зони і модулювати інші більш потужні електричні сигнали, до яких можливий доступ зловмисників.

Джерелами побічних високочастотних коливань є:

• високочастотні генератори,

• підсилювальні каскади,

• нелінійні елементи.

Численні небезпечні сигнали створюють працюючі персональні ЕОМ, розташовані в неекранованих корпусах.

Орієнтовна дальність виявлення радіовипромінювань ПЕОМ в таблиці:

Паразитні зв'язки і наводки характерні для будь-яких радіоелектронних засобів і з'єднуючих їх проводів. Розрізняють 3 види паразитних зв'язків: гальванічна, індуктивна і ємнісна.

Дальність ПЕМВН персонального комп’ютера

Блоки ПЕОМ	Дальність перехвату, м	
	Електромагнітний сигнал	Електричний сигнал
Системний блок	2-40	1-30
Монітор	25-120	10-55
Клавіатура	15-50	15-30
Принтер	5-35	10-80

Дальність ПЕМВН – побічного електромагнітного випромінювання і наведень.

Гальванічний зв'язок або зв'язок через опір виникає, коли по одним і тим самим ланцюгам протікають струми різних джерел сигналів.

Паразитні індуктивні і ємнісні зв'язки являють собою фізичні фактори, що характеризують вплив електричних і магнітних полів, що виникають в ланцюзі будь-якого радіоелектронного засобу на інші ланцюги.

ПРИНЦИПИ ЗАПИСУ І ЗНІМАННЯ ІНФОРМАЦІЇ З НОСІЇВ.

Матеріалізація, або запис будь-якої інформації, проводиться шляхом зміни параметрів носія. При вивченні сутності запису інформації, як правило, розглядається хімічна і електрична природа механізмів запам'ятовування. Запис інформації на матеріальні тіла відбувається шляхом зміни їх фізичної структури і хімічного складу. На папері інформація записується шляхом фарбування елементів її поверхні друкарською фарбою, чорнилом, пастою та іншими барвниками.

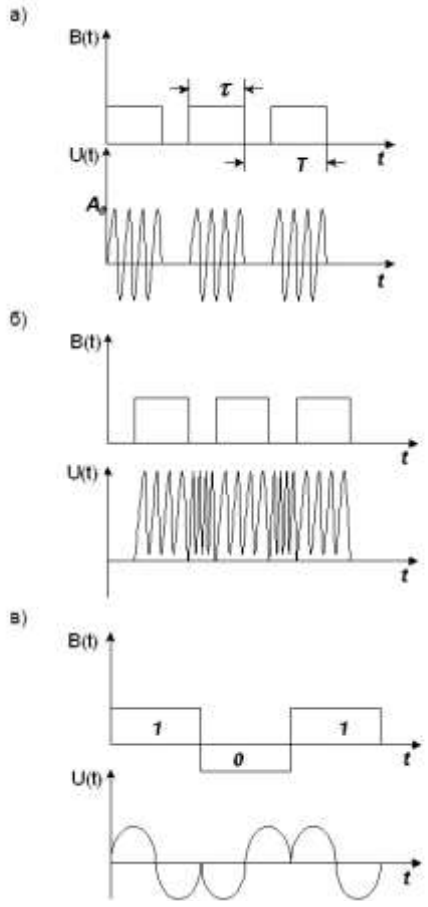
Записана на матеріальному тілі інформація зчитується при послідовному перегляді поверхні тіла зоровим аналізатором людини або автомата, виділення і розпізнавання ними знаків, символів або конфігурації точок.

Запис інформації на носії у вигляді полів і електричного струму здійснюється шляхом зміни їх параметрів. Безперервна зміна параметрів сигналів у відповідності зі значеннями первинного сигналу називається ***модуляцією***, дискретне - ***маніпуляцією***. Первинним є сигнал від джерела інформації. Якщо змінюються значення амплітуди аналогового сигналу, то модуляція називається амплітудною, частоти - частотною, фази - фазовою. Частотна і фазова модуляція мало різняться, оскільки при фазовій модуляції змінюється безпосередньо фаза, а при частотній її перша похідна за часом - частота (мал.1.4.1).

При модуляції дискретних сигналів, як модульованих застосовуються і інші параметри: тривалість імпульсу, частота його повторення і ін. Для ущільнення інформації на носії та економії тим самим енергії носія застосовують складні (з використанням різних параметрів сигналу) види модуляції.

Виділення інформації з модульованого електричного сигналу проводиться шляхом зворотних перетворень - демодуляції його в детекторі (демодуляторі) приймача. При демодуляції виділений і посилений радіосигнал, наведений електромагнітною хвилею в антені, перетворюється таким чином, що сигнал на виході детектора відповідає моделюючому сигналу передавача.

Демодуляція, як будь-яка процедура розпізнавання, забезпечується шляхом порівняння поточного сигналу з еталонним.



Мал. 1.4.1 Приклади модуляцій:
а – амплітудна; б – частотна;
в – фазова

Повної відповідності моделюючого і демодульованого сигналів через вплив перешкод домогтися неможливо. У загальному випадку будь-які перетворення сигналу погіршують якість записаної в ньому інформації, так як при цьому виявляється вплив на його інформаційні параметри, які можуть привести до втрати інформації. При достатньо великому перевищенні потужності носія над потужністю перешкод, спотворення настільки незначні, що на якість інформації перешкоди практично не впливають.

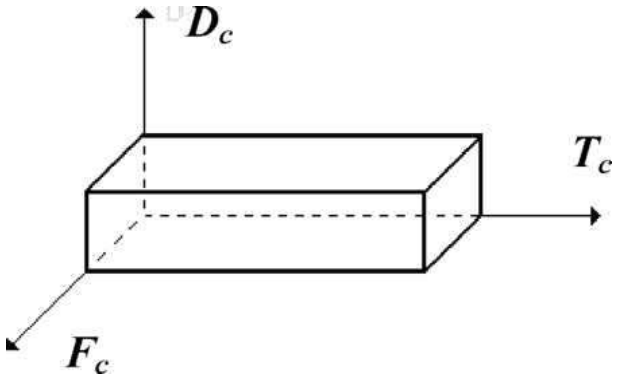
Перешкодостійкість дискретних сигналів вище, ніж аналогових, так як спотворення дискретних сигналів виникають, якщо зміни параметру сигнала перевищують половину величини інтервалу між сусідніми значеннями параметра. Якщо зміни параметрів перешкоди становлять менше половини цього інтервалу, то при прийомі такого сигналу можна відновити вихідне значення параметра сигналу. Допустимі значення відносин потужностей або амплітуд сигналу і перешкоди (відношення сигнал/ перешкода), при яких забезпечується необхідна якість прийнятої інформації, визначаються видом інформації і характером перешкод.

Для підвищення достовірності передачі інформації поряд зі збільшенням енергії передавача інформації використовують інші методи захисту дискретної інформації від перешкод, перш за все завадостійке кодування. При завадостійкому кодуванні кожному елементу дискретної інформації (букві, цифрі, будь-якому іншому знакові) ставиться у відповідність кодова комбінація, яка містить додаткові (надлишкові) символи. Ці додаткові символи дозволяють виявляти спотворення і виправляти в залежності від надмірності коду помилкові символи різної кратності. Однак слід мати на увазі, що платою за підвищення завадостійкості кодованих сигналів є зменшення швидкості їх передачі.

Будь-яке повідомлення в загальному випадку можна описати за допомогою трьох основних параметрів: динамічним діапазоном Dc, шириною спектра частот ΔFc і тривалістю передачі Tc. Добуток цих трьох параметрів називається об'ємом сигналу (формула 1.1)

$$V_c = D_c \Delta F_c T_c. \qquad (1.1)$$

У тривимірному просторі обсяг сигналу можна представити у вигляді паралелепіпеда (див. мал. 1.4.2).



Мал. 1.4.2 Графічне представлення обсягу сигналу

Для забезпечення неспотвореної передачі повідомлення обсягом Vc, необхідно, щоб характеристики середовища передавача і приймача відповідали ширині спектра і динамічному діапазону сигнала. Якщо смуга частот середовища передавача або приймача менше смуги сигнала, то для забезпечення неспотвореної передачі сигналу об'ємом Vc зменшують його ширину спектра. При цьому для збереження Vc = const відповідно збільшують час передачі Tc. Для неспотвореної передачі повідомлення в реальному масштабі часу смуга пропускання приймача повинна відповідати ширині спектра сигнала.

1.4 ВИДИ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ.

Під ***безпекою інформації*** слід розуміти умови зберігання, обробки і передачі інформації, при яких забезпечується її захист від загроз знищення, перекручення і розкрадання.

Слід розрізняти потенційну і реальну безпеку. ***Потенційна безпека*** інформації, як і будь-який інший об'єкт або суб'єкт, існує завжди. Безпека інформації оцінюється двома показниками: ймовірністю запобігання загрозам і часом, протягом якого забезпечується певний рівень безпеки. Ці показники взаємозалежні. При заданих конкретних умовах щодо захисту забезпечити більш високий рівень безпеки можливо протягом коротшого часу.

Інформація постійно піддається випадковим або навмисним загрозам: розкрадання, зміни, знищення. Ці загрози реалізуються:

- внаслідок дії зловмисників: люди, що займаються добуванням інформації в інтересах державної і комерційної розвідки, кримінальні елементи, непорядні співробітники або просто неадекватні люди;

- розголошення інформації людиною, що володіє секретною або конфіденційною інформацією;

- втратою носіїв з інформацією (документи, електронні носії, зразки матеріалу та продукції);

- несанкціоноване поширення інформації через поля і електричні сигнали, що випадково виникають в електричних і радіоелектронних приладах через їх старіння і зношування, неякісне конструювання або виготовлення і порушення правил експлуатації;

- впливу стихійних сил, перш за все вогонь під час пожежі і вода в ході гасіння пожежі і протікання в системах опалення, водопостачання, каналізація;

- збій в роботі апаратури збору, обробки, зберігання і передачі інформації, викликаний її несправністю, а також ненавмисні і навмисні помилки користувачів і обслуговуючого персоналу;

- вплив потужних електромагнітних і електричних промислових і природних перешкод.

Несанкціоноване розповсюдження (витік) інформації може відбуватися:

- внаслідок спостереження за джерелами інформації;

- підслуховування конфіденційних розмов і акустичних сигналів;

- перехоплення електричних, магнітних і електромагнітних полів, електричних сигналів і радіаційних випромінювань;

- несанкціоноване поширення матеріальних носіїв за межі організації.

Здійснюються такі види спостереження: візуально, візуально-оптично (за допомогою оптичних приладів) телевізійно і радіолокаційно, фотографуванням об'єктів в оптичному і інфрачервоному діапазонах.

Підслуховування – мовна інформація. Одна з найчастіших загроз безпеки інформації - її копіювання. Підслуховування звуків, що видаються механізмами під час випробувань або

експлуатації, дозволяє фахівцям зробити припущення про конструкції, нові вузли і технічне рішення механізмів, які випромінюють ці звуки. Перехоплення електричних сигналів, що містять інформацію, здійснюється шляхом їх прийому технічними засобами зловмисника і зйому з них інформації або сигналів.

Загроза безпеки інформації створює також умови і дії, що забезпечує доступ зловмисників до паперових носіїв (начерки, чернетки і ін.). Бракована продукція або її окремі вузли і деталі, сировина і матеріали, що містять демаскуючі речовини та інші джерела інформації.

Спостереження, перехоплення і підслуховування інформації, що проводяться з використанням технічних пристроїв, призводять до її витоку технічними каналами.

Для забезпечення ефективного захисту інформації необхідно оцінювати величину загрози. Величину конкретної загрози C_{yi} для розглядаємого і-го елемента інформації в загальному випадку можна представити у вигляді добутку потенційних збитків від реалізації загрози в і-му елементі інформації $C_{пуі}$ і ймовірності реалізації загрози P_{yi}, т. е. $C_{yi} = C_{піу} \times P_{yi}$.

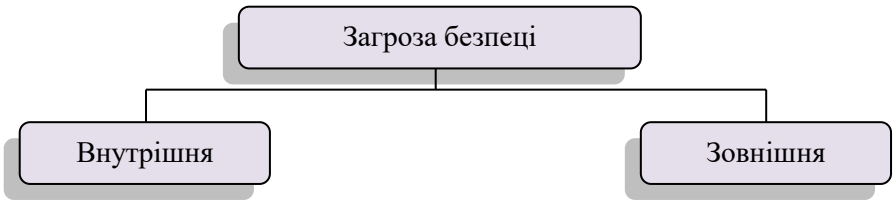
Отримати точні кількісні значення співмножників не представляється можливим. Наближена оцінка загрози можлива при наступних обмеженнях і умовах.

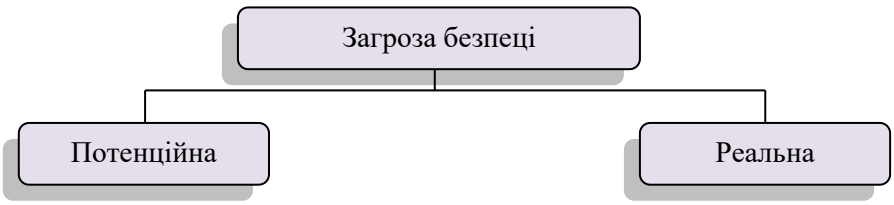
По-перше, можна припустити, що максимальний збиток від розкрадання інформації відповідає її ціні. Дійсно, при попаданні інформації до конкурента власник інформації може втратити не тільки очікуваний прибуток, але і не компенсувати її собівартість.

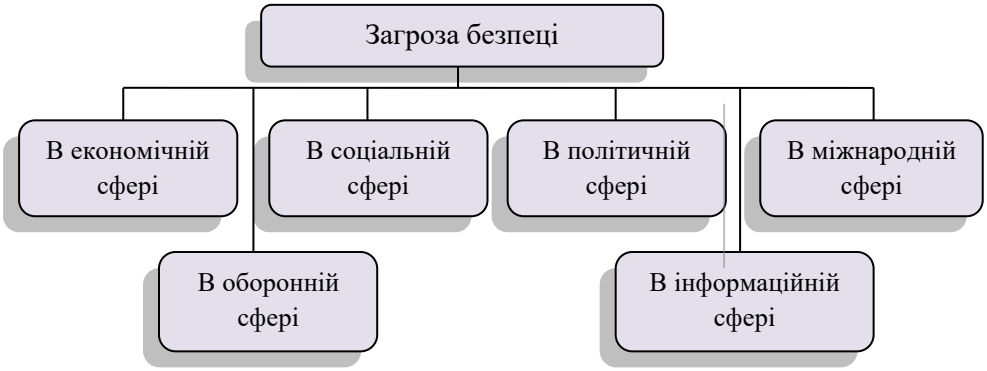
По-друге, в умовах повної невизначеності намірів зловмисника по добуванню інформації помилка прогнозу мінімальна, якщо прийняти величину ймовірності реалізації загрози протягом аналізованого періоду часу (наприклад, 1 року) рівною 0,5.

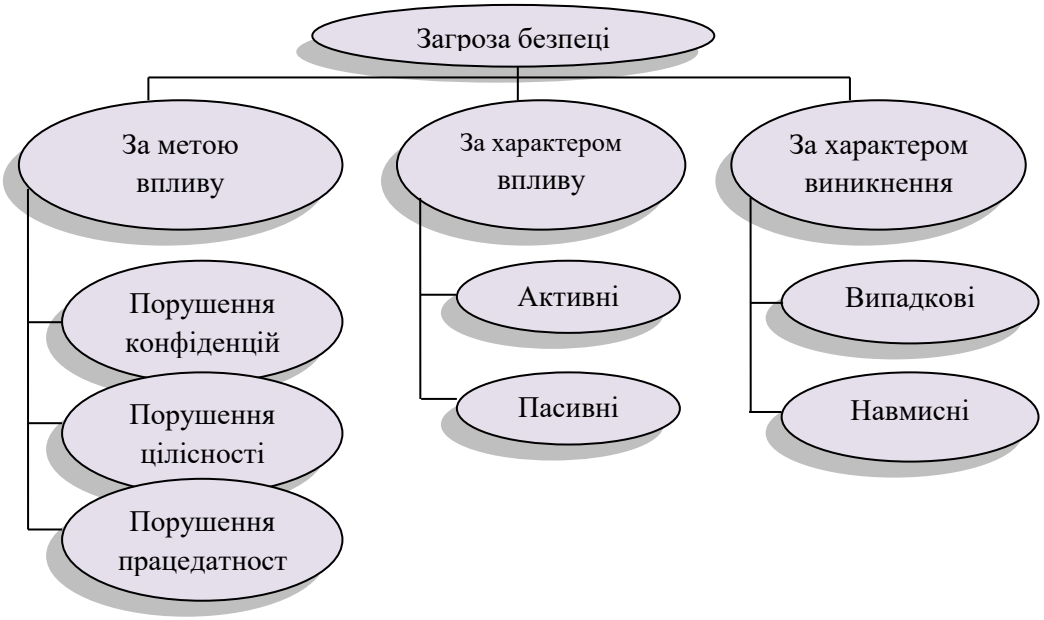
В результаті усереднення по всім я-м елементам інформації верхньої межі загроза складе половину ціни, що захищається. Очевидно, що чим вища ціна інформації та більше загроза її безпеці, тим більше ресурсів буде потрібно для захисту цієї інформації.

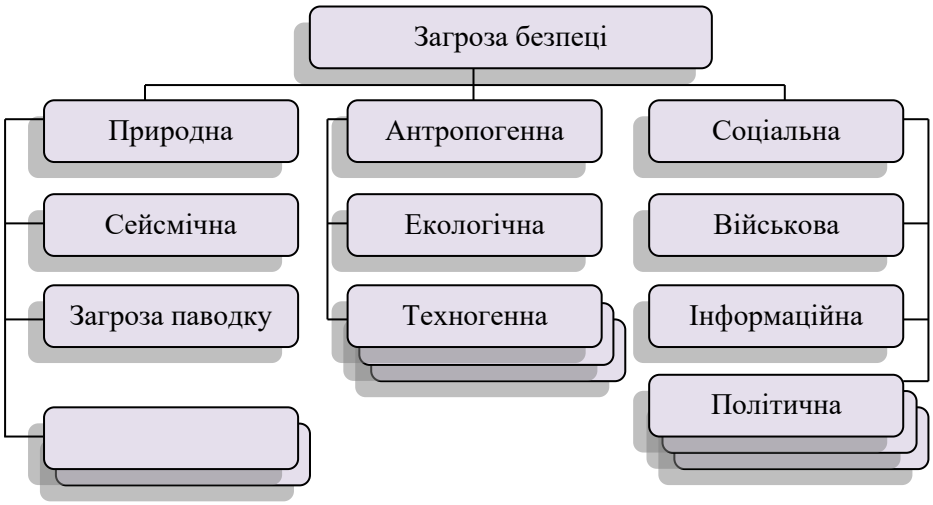
Існують декілька методів класифікації загроз по різним чинникам, нижче наведені приклади (мал. 1.5.1 та мал. 1.5.2):



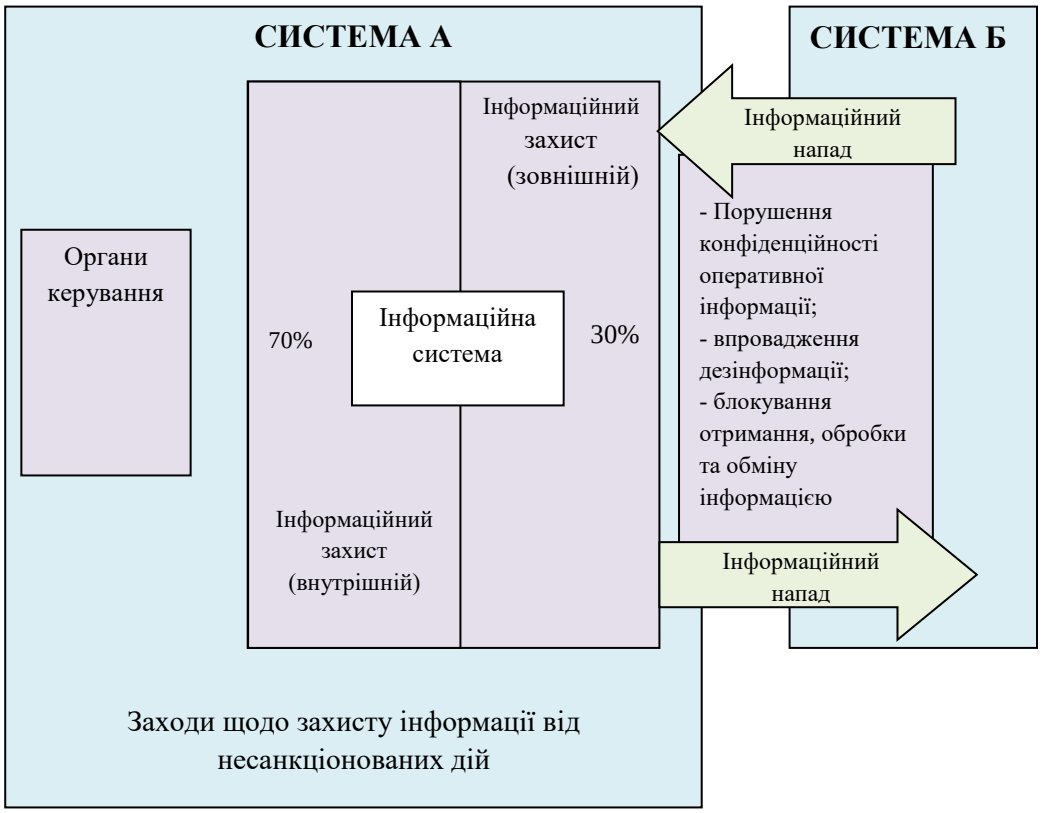








Мал. 1.5.1. Приклади класифікацій загроз інформаційної безпеки



Мал. 1.5.2. Структура інформаційної боротьби

1.5 ПРИНЦИПИ ДОБУВАННЯ І ОБРОБКИ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ.

1.5.1 ОРГАНИ ДОБУВАННЯ ІНФОРМАЦІЇ.

Необхідність в інформації для будь-яких структур, що діють в конкуруючих умовах, змушує їх витрачати ресурси (і чималі) на її постійне добування. При цьому створюються спеціалізовані органи, призначені для добування інформації. Такими органами є органи державної та комерційної розвідки.

Будь-яка держава створює органи розвідки, що забезпечують керівництво країни інформацією для прийняття ним політичних, економічних, військових, науково-технічних рішень в умовах жорсткої міждержавної конкуренції. Залежно від цілей держави, його зовнішня політика і можливості структури органів розвідки істотно відрізняються.

Основні сфери інтересів державної розвідки:

- військово-економічний і науково-технічний потенціали інших держав, і прогнозування їх розвитку;

- військово-технічних об'єктів та підприємств, їх розміщення, виробничі потужності, характер і розподіл продукції, що випускається;

- роботи, що ведуться в області створення нових видів озброєння і військової техніки;

- склад і дислокація угруповань збройних сил;

- озброєння і військова техніка, тактико-технічні характеристики;

- графік проведення навчань, які залучаються сили і засоби, які вирішуються завдання;

- побудова та технічне оснащення систем державного і військового управління та зв'язку;

- інженерне обладнання стратегічних об'єктів зв'язку та навігаційно-гідрографічне забезпечення;

- паливно-енергетичні, рудні, водні, рослинні та інші природні ресурси;

- метеорологічна обстановка, клімат;

- виконання умов міжнародних договорів, наприклад, про обмеження озброєнь.

Крім цих глобальних завдань органи розвідки добувають великий обсяг різноманітної інформації, аж до стану здоров'я, характеру, звичок, стилю мислення політичних і військових керівників зарубіжних держав.

Розвідка комерційних структур (комерційна розвідка) видобуває інформацію в інтересах їх успішної діяльності на ринку в умовах гострої конкурентної боротьби. Завдання органів комерційної розвідки, їх склад і можливості залежать від цілей власників і капіталу фірми, але принципи добування інформації істотно не відрізняються, але необхідно враховувати, що державні органи діють в інтересах держави в цілому, а комерційні діють в інтересах власників і відповідно регламентація їх діяльності відрізняється.

Області, які представляють інтерес для комерційної розвідка:

- стратегічні та оперативні плани вищого керівництва фірм-конкурентів;

- комерційна філософія і ділова стратегія (місія) фірм конкурентів, особисті та ділові якості керівників і ключових співробітників;

- відомості, що становлять комерційну таємницю, наприклад, технологічні, науково-дослідні та конструкторські роботи;

- технологічні процеси при виробництві нової продукції, результати випробувань;

- фінансовий стан і фінансові операції;

- організаційна та виробнича інформація;

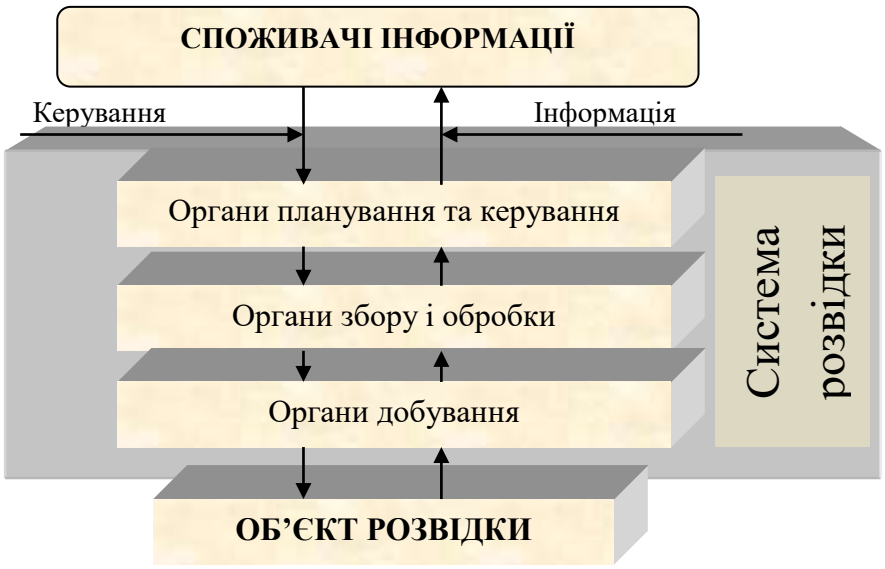
- введення в дію нового обладнання, розширення і модернізація існуючих виробничих потужностей, кооперація з іншими підприємствами;

- маркетинг фірми, в тому числі режими поставок, відомості про замовників і угоди, що укладаються, показники реалізації продукції.

Дані переліки не є вичерпними, збір і аналіз даних проводиться з багатьох інших питань, наприклад зі сфери психології та соціальної інженерії.

Організація органів комерційної розвідки різних фірм можуть відрізнятися за формою. Вона залежить від завдань, покладених на комерційні розвідки, дохід, цінність інформації, розташування території, будівлі та приміщенн фірми і інші фактори. Однак незалежно від кількісного складу органів комерційної розвідки вони об'єктивно повинні вирішувати завдання з інформаційного забезпечення керівництва організації інформацією, необхідною для успішної діяльності в умовах безперервної конкуренції.

Таким чином, органи розвідки утворюють систему розвідки з багаторівневою ієрархічною структурою (мал. 1.6.1).



Мал. 1.6.1. Структура розвідки

Умовно розвідку поділяють на агентурну і технічну. Відмінності - в співвідношенні людського або технічного фактору.

Агентурна розвідка є найбільш давнім видом розвідки. Добування інформації проводиться шляхом проникнення агента (резидента) безпосередньо до джерела інформації на відстань доступності його органів почуттів або використовуючи ним технічні засоби копіювання та передачі інформації.

Технічна розвідка пов'язана, перш за все, з розвитком технічних засобів і технологій знімання інформації по різних каналах і підвищенням технічних можливостей, для забезпечення:

- зниження ризику (неможливості) фізичного затримання агента органами контррозвідки або служби безпеки підприємства, шляхом збільшення дистанції до джерел інформації;

- добування інформації шляхом знімання її з носіїв, які не впливають на органи чуття людини (ПЕМВН, інфрачервоний і ультрафіолетовий діапазони).

Технічний класифікують по розвідці різних ознак. Найбільш широко застосовуються дві класифікації: по фізичній природі носіїв інформації і видам носіїв технічних засобів добування.

Технічна розвідка (по фізичній природі носіїв) інформації підрозділяється:

• оптична (носій - електромагнітне поле у видимому, інфрачервоному та ультрафіолетовому діапазонах);

• радіоелектронна (носій - електромагнітне поле в радіодіапазоні або електричний струм);

• акустична або акусто-вібраційний (носій - акустична хвиля і вібрація);

• хімічна (носій - частинки речовини);

• радіаційна (носій - випромінювання радіоактивних речовин);

• магнітометричних (носій - магнітне поле).

У свою чергу, оптична, радіоелектронна і акустична розвідка підрозділяється на підвиди технічної розвідки.

Оптична розвідка включає:

- візуально-оптичний;

- фотографічний;

- інфрачервоний;

- телевізійний;

- лазерний.

Наведена послідовність видів оптичної розвідки відповідає етапам розвитку оптичної розвідки в міру технічного прогресу в області засобів оптичного спостереження. Останні три види, які використовує електронна техніка, утворюють оптико-електронну розвідку.

Радіоелектронна розвідка в залежності від характеру видобутої інформації підрозділяється:

- на радіорозвідку;

- радіотехнічну розвідку;

- радіолокаційну розвідку;

- радіотеплову розвідку.

Радіорозвідка добуває семантичну інформацію шляхом перехоплення радіовипромінювання з конфіденційною інформацією, *радіотехнічна* - інформація про параметри (ознаки) радіотехнічні сигнали, *радіолокаційна* - інформація про видові ознаки радіолокаційного зображення об'єкта на екрані радіолокатора, і нарешті, *радіотеплова* - інформація про ознаки об'єктів, що виявляються через їх власні електромагнітні випромінювання в радіодіапазоні.

Акустична розвідка в залежності від середовища поширення акустичної хвилі поділяється на повітряно-акустичну (акустична), гідроакустичну (середа поширення - вода) і сейсмічну (середа - земна поверхня).

Хімічна розвідка добуває інформацію про склад, структуру та властивості речовин шляхом взяття проб і аналізу.

Радіаційна розвідка призначена для виявлення, локалізації, визначення характеристик і вимірювання рівнів випромінювань радіоактивних речовин.

Магнітометрична розвідка дозволяє по зміні магнітного поля Землі виявляти тіла, які мають власне магнітне поле, наприклад підводні човни в зануреному стані, деякі види корисних копалин і об'єктів промислового та військового призначення.

Класифікація розвідки по виду носіїв (апаратури засобів добування):

-сухопутна;

-повітряна;

-космічна;

-морська.

1.5.2 ВЕДЕННЯ РОЗВІДКИ. ПРИНЦИПИ

Основні принципи ведення розвідки:

1. Системність і цілеспрямованість - визначення завдань і об'єктів розвідки у відповідності зі стратегічними цілями і завданнями, ведення її за єдиним планом з різних напрямків і зосередження зусиль розвідки на виконанні поставлених завдань.

2. Активність - активні дії всіх елементів системи розвідки, постійний пошук оригінальних способів вирішення завдань з урахуванням конкретних умов.

3. Безперервність - постійний характер добування інформації і незалежність цих дій від пори року, доби, погоди і будь-яких інших умов. При зміні обстановки і умов міняються способи і засоби добування (принцип активності).

4. Прихованість - проведення заходів з підготовки та добування інформації в таємниці, що дозволяє забезпечити безпеку органів добування і приховування фактів витоку чи внесення змін до інформації. Це дає можливість виграти час для більш ефективного застосування добутої інформації в умовах конкуренції.

Зробити висновки про факти витоку конфіденційної інформації можна за ***непрямими ознаками***:

- зниження доходів або посилення позицій конкурента у зв'язку з виходом на ринок аналогічних товарів конкурента, але з кращими споживчими властивостями або за нижчими цінами;

- поява публікацій у періодичній пресі та реєстрація патентів за результатами досліджень, що ведуться в лабораторіях фірми;

- перерозподіл традиційної клієнтури на користь конкурента.

Скритність досягається застосуванням пасивних технічніх засобів, маскування і камуфлювання апаратури, легендування і засекречування заходів по добуванню інформації.

З огляду на різноманіття способів і форм відображення інформації, ефективність різних способів і засобів її добування, залежить від конкретних умов. Таким чином, не існує універсальних методів. Тому ефективне добування інформації проводиться шляхом комплексного використання різних способів і засобів добування інформації. При цьому забезпечується дублювання даних і їх перехресна перевірка, що є основним способом підвищення достовірності даних.

Технологія добування інформації включає наступні етапи:

- організація добування;

- добування даних і відомостей;

- інформаційна робота.

Організація добування інформації передбачає:

- декомпозиція (структуризація) поставленого завдання;

- розробка задуму операції по добуванню інформації;

- планування;

- постановка задачі виконавцю;

- нормативне і оперативне управління діями виконавців і режимами роботи технічних засобів.

Первісна постановка задач, як правило, здійснюється в досить загальному вигляді, тому необхідна конкретизація з урахуванням наявних даних про можливі джерела інформації, їх місцезнаходження, можливі способи доступу і перешкоди, можливі наявні технічні засоби добування і т. п. В результаті аналізу завдань і наявних попередніх даних і припущень розробляється задум операції, в якому намічаються шляхи вирішення поставлених завдань.

На результативність добування інформації впливають численні перешкоди і випадкові чинники - протидія контррозвідки і служби безпеки, недостатність інформації про джерела видобування відомостей і даних, відмови апаратури, погодні умови, пильність громадян і співробітників організації та інші. Ці фактори необхідно враховувати при плануванні із зазначенням місця і часу дій всіх суб'єктів і технічних засобів, що беруть участь в операції.

Відомості та дані одержують за допомогою пошуку джерел інформації і її носіїв, їх виявлення, встановлення розвідувального контакту з ними. Відомості та дані представляють фрагменти інформації і відрізняються один від одного тим, що дані знімаються безпосередньо з носія (первинна інформація) а відомості - проаналізовані дані (вторинна інформація).

Основу процесів виявлення об’єктів складає процедура ідентифікації – порівняння поточних ознакових структур, що формуються у процесі пошуку, з еталонною ознаковою структурою об’єкта розвідки.

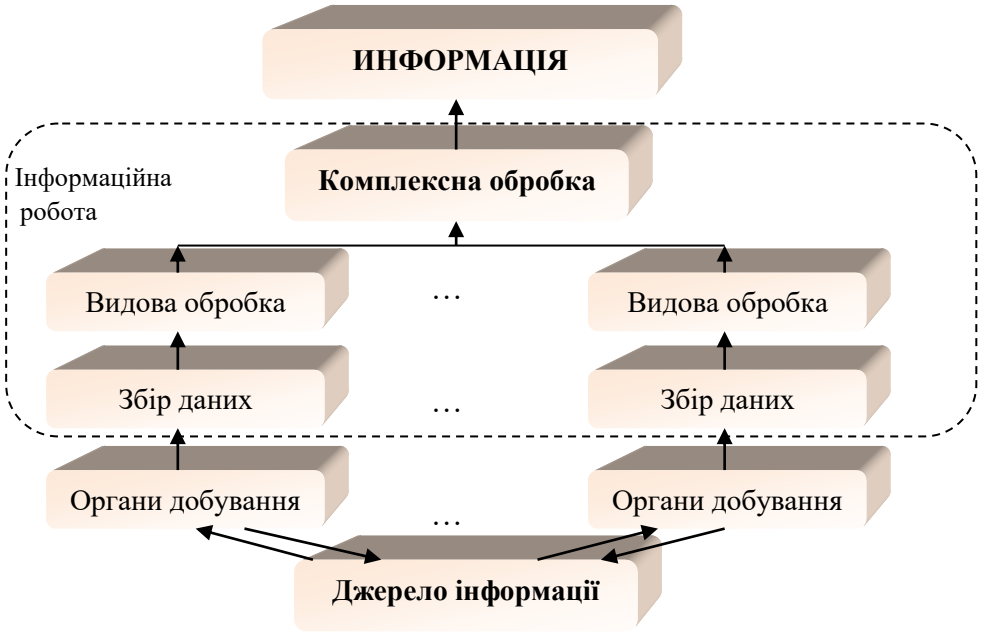
Здобуті дані, як правило, розрізнені. Вони перетворюються в корисну інформацію, відповідно до поставлених завдань, в ході накопичення та обробки інформації.

Інформаційний або аналітична робота включає наступні процеси (мал. 1.6.2):

- збір даних і відомостей від органів добування;

- видова обробка;

- комплексна обробка.



Мал. 1.6.2. Структура роботи з інформацією.

Необхідно пам’ятати, що методи розвідки (збору інформації) бувають легальні та нелегальні. При цьому необхідно враховувати правове регулювання і можливі наслідки, так як сучасне законодавство передбачає жорстке покарання за порушення інформаційних прав та свобод які мають місце при нелегальних методах.

Легальне добування інформації проводиться шляхом вивчення і обробки відкритих джерел, публікацій в засобах масової інформації, періодичних наукових та популярних журналах, праці ВУЗів і науково-виробничих підприємств, урядових виданнь, навчальних посібників і тому подібні. Інформацію можна знайти в матеріалах, що мають безпосереднє відношення до діяльності фірми: в угодах про ліцензії, статтях та доповідях, річних звітах фірм, звітах комівояжерів, оглядах ринків і доповідях інженерів-консультантів, внутрішніх друкованих виданнях, телефонних довідниках, рекламній літературі та проспектах. Цей перелік неповний.

Однак найбільшу небезпеку по заподіянню шкоди несе ***нелегальний шлях*** в результаті проведення таємних заходів спецслужб і комерційних розвідок, або так званий промисловий шпіонаж - "комерційна розвідка".

Добування інформації в загальному випадку представляє собою процес, який починається з моменту постановки завдання її користувачами (військово-політичне керівництво країни або окремі відомства, керівництво фірми) до моменту надання користувачам інформації, яка відповідає поставленим завданням та вимогам.

Показники ефективності збору інформації

Загальним критерієм ефективності збору інформації, що включає органи управління, добування і обробки, є ступінь виконання поставлених перед нею завдань. Але цей критерій не є конструктивним і не досить об'єктивний, оскільки рівень відповідності добутої інформації, відповідно до тої, що необхідна, оцінює її споживач. Для більш об'єктивного визначення можливостей використовується група загальносистемних показників кількості і якості інформації:

- повнота;
- своєчасність;
- достовірність;
- точність вимірювання демаскуючих ознак;
- сумарні витрати на отримання інформації.

Найбільш достовірним показником ефективності ведення збору інформації є успішна реалізація тієї операції, яка планувалася на основі отриманої інформації.

Контрольні питання

1. Назвіть закони України, які визначають поняття «інформація» і класифікують її в залежності від порядку розповсюдження.
2. Дайте визначення поняття «захист інформації».
3. Які обов'язки власника інформації відповідно до законодавства.
4. Перерахуйте особливості інформації як об'єкта захисту.
5. Назвіть види інформації, що захищається технічними засобами.
6. Що таке демаскуючі ознаки?
7. Наведіть класифікацію демаскуючих ознак.
8. Назвіть основні носії інформації.
9. Наведіть класифікацію сигналів.
10. Наведіть класифікацію основних ознак речовин.
11. Назвіть і дайте характеристики основних джерел інформації.
12. Назвіть основні джерела функціональних сигналів.
13. Перерахуйте принципи запису інформації на носії.
14. Що розуміють під безпекою інформації?
15. Назвіть причини виникнення загроз безпеки інформації.
16. Перелічіть основні сфери інтересів державних органів добування інформації.
17. Наведіть структуру системи збору інформації.
19. Перелічіть види технічних розвідок.
20. Назвіть основні принципи збору інформації.
21. Які етапи включає технологію добування інформації.
22. Які процеси містить інформаційно-аналітична робота.
23. Що розуміють під контактом, внаслідок якого можлива втрата інформаційного ресурсу?

2 ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

2.1 ОСОБЛИВОСТІ ВИТОКУ ІНФОРМАЦІЇ ОСНОВНІ ПОКАЗНИКИ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ.

Під ***витоком інформації*** розуміється несанкціонований процес перенесення інформації від джерела до зловмисника.

Витік інформації можливий шляхом її розголошення людьми, втрата ними носіїв з інформацією, перенесення інформації за допомогою полів, потоків елементарних частинок, речовини в газоподібному, рідкому або твердому вигляді. Наприклад, надмірне бажання співробітників поділитися останніми новинами про роботу з рідними або близькими створює можливості витоку конфіденційної інформації. Переносниками інформації можуть бути будь-які її носії.

Способи доступу до конфіденційної інформації можна поділити на дві групи в залежності від способів доступу її органів добування - агентів або технічних засобів - до джерел інформації та забезпечення розвідувального контакту з ними.

Розвідувальний контакт між зловмисником або його технічним засібом і джерелом інформації передбачає встановлення фізичного контакту між зловмисником (технічний засіб) і носієм інформації. Фізичний контакт передбачає, що зловмисник має можливість взяти носій з інформацією в руки з метою його викрадення, копіювання, знищення або модернізації або за допомогою своїх рецепторів і використовуваних технічних засобів добування - зняти з носія інформацію дистанційно.

Дистанційне добування інформації передбачає знімання її з носія, що поширюється за межі області фізичного контакту зловмисника з джерелом інформації. Часто розглядається варіант, коли інформація знімається за межами контрольованої зони, але можливі інші варіанти. Дистанційне добування інформації можливе в результаті спостереження, підслуховування, перехоплення, збір носіїв інформації у вигляді матеріальних тіл - браковані вузли, деталі, демаскуючі речовини та поля за межами організації чи контрольованої зони, наприклад - акустичних, електричних, магнітних і електромагнітних полів, в тому числі в оптичному діапазоні; електричний струм, що поширюється по дротах електроживлення, телефонна мережа, радіотрансляція, охоронна і пожежна сигналізація.

Витік інформації ***технічними каналами*** має ряд особливостей, які необхідно враховувати:

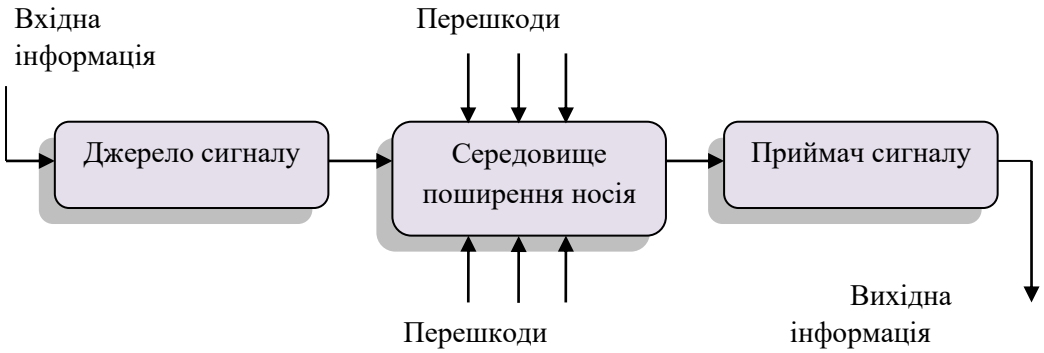
- витік інформації може відбуватися тільки при попаданні її до зацікавленого в ній несанкціонованого одержувача;
- при витоку інформації відбувається її тиражування, яке не змінює характеристики носія інформації (кількість аркушів документа, число пікселів зображення, розміри, вага, колір та інші демаркуючі ознаки продукції залишаються в тій же кількості, що і до витоку);
- ціна інформації при її витоку зменшується при тиражуванні;
- витік інформації, як правило, виявляється через деякий час, за наслідками, коли заходи щодо забезпечення її безпеки можуть виявитися неефективними.

Фізичний шлях перенесення інформації від її джерела до несанкціонованого одержувача (зловмисника) називається ***каналом витоку***. Канал, в якому здійснюється

несанкціонований процес перенесення інформації з використанням технічних засобів, називається ***технічним каналом витоку інформації***.

Характеристики технічних каналів витоку інформації

Для передачі інформації носіями у вигляді полів і мікрочастинок по будь-якому технічному каналу сам канал повинен містити три основних елементи: джерело сигналу, середовище поширення носія і приймач. Узагальнена типова структура каналу передачі інформації наведена на мал.2.1.1.



Мал. 2.1.1 Типова структура каналу передачі інформації

На вхід каналу надходить інформація у вигляді первинного сигналу. Первинний сигнал являє собою носій з інформацією від її джерела або з виходом попереднього каналу. Як ***джерело сигналу*** можуть бути:

- об'єкт спостереження, що відображає електромагнітні та акустичні хвилі;
- об'єкт спостереження, що випромінює власні (теплові) електромагнітні хвилі в оптичному і радіодіапазоні;
- передавач функціонального каналу зв'язку;
- закладний пристрій;
- джерело небезпечного сигналу;
- джерело акустичних хвиль, модульованих інформацією.

Так як інформація від джерела надходить на вхід каналу на мові джерела (у вигляді тексту, символів, знаків, звуків, сигналів і т.п.), то передавач перетворює ці форми подання інформації у форму, що забезпечує запис її на носій інформації, відповідно середовищу поширення. У загальному випадку він виконує наступні функції:

- створює (генерує) поля (акустичне, електромагнітне) або електричний струм, які переносять інформацію;
- проводить запис інформації на носій (модуляцію інформаційних параметрів носія);
- підсилює потужність сигналу (носія з інформацією);
- забезпечує передачу (випромінювання) сигналу в середу поширення в заданому секторі простору.

Середовище поширення носія - частина простору, в якому переміщується носій. Воно характеризується набором фізичних параметрів, що визначають умови переміщення носія з інформацією. Основні параметри, які необхідно враховувати при описі середовища поширення, є:

- фізичні перешкоди для суб'єктів і матеріальних тіл;
- ступінь ослаблення (або пропускання енергії) сигналу на одиницю довжини;
- частотна характеристика (нерівномірність ослаблення частотних складових спектра сигналу);
- вид і потужність перешкод для сигналу.

Приймач виконує функції, зворотні функції передавача. Він здійснює:
- вибір (селекція) носія з необхідною одержувачу інформацією;
- посилення прийнятого сигналу до значень, що забезпечує знімання інформації;
- знімання інформації з носія (демодуляція, декодування):
- перетворення інформації в форму сигналу, доступного одержувачу (людина, технічний пристрій) і посилення сигналів до значень, необхідних для безпомилкового їх сприйняття.

Канал витоку інформації відрізняється від функціонального каналу передачі одержувачем інформації. Якщо одержувач санкціонований, то канал **функціональний**, в іншому випадку - **канал витоку**.

2.2. КЛАСИФІКАЦІЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ.

Основною класифікаційною ознакою технічних каналів витоку інформації є фізична природа носія. За цією ознакою вони діляться:
- на оптичні;
- радіоелектронні;
- акустичні;
- матеріально-речові.

Носієм інформації в оптичному каналі є **електромагнітне поле** в діапазоні 0,46 до 0,76 мкм (видиме світло) і від 0,76 до 13 мкм (інфрачервоне випромінювання).

У **радіоелектронному каналі** витоку інформації в якості носіїв використовуються електричні, магнітні та електромагнітні поля в радіодіапазоні, а також електричний струм (потік електронів), що поширюється по металевих дротах. Діапазон коливань носія цього виду надзвичайно великий: від звукового діапазону до десятків ГГц.

Відповідно ***радіоелектронний канал*** доцільно розділити на 2 підвиди: ***електромагнітний***, носіями інформації в якому є електричне, магнітне і електромагнітне поля, і ***електричний канал***, носій інформації в якому - електричний струм.

Носіями інформації в ***акустичному каналі*** є механічні пружні акустичні хвилі в інфразвуковому (менш 16Гц), звуковому (16Гц - 20кГц) і ультразвуковому (понад 20 кГц) діапазоні частоти, що поширюється в атмосфері, воді та твердому середовищі.

У ***матеріально-речовинному каналі*** витік інформації проводиться шляхом несанкціонованого поширення за межі організації речових носіїв з інформацією, яка захищається, наприклад, чернетки документів і використана копіювальна стрічка та папір, забраковані деталі і вузли, демаскуючі речовини, брухт, технологічні відходи.
Кожен з технічних каналів має свої особливості, які необхідно знати і враховувати для забезпечення ефективного захисту інформації.

За своєю інформативністю канали витоку діляться на **інформативні** та **неінформативні**. Інформативність каналу оцінюється цінністю інформації, яка передається по каналу.

За часом прояву канали діляться на постійні, періодичні та епізодичні. У ***постійному каналі*** витік інформації носить досить регулярний характер. Так, наявність в кабінеті джерела небезпечного сигналу може передбачати передачу з кабінету мовної інформації до моменту виявлення цього джерела. ***Періодичний канал*** витоку може виникнути за умови, наприклад, розміщення у дворі не прикритої продукції, демаскуючі ознаки про яку складають таємницю, під час прольотів розвідувальних космічних апаратів. До ***епізодичних каналів*** належать канали, витік інформація в яких має випадковий разовий характер.

Канал витоку інформації, що складається з передавача, середовища поширення і приймача, є **одноканальним**. Однак можливі варіанти, коли витік інформації відбувається більш складним шляхом - за кількома послідовними або паралельними каналами.

2.3. СТРУКТУРА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ.

Структура технічних каналів витоку інформації має наступний вигляд (мал. 2.3.1):

Мал.2.3.1 Класифікація технічних каналів витоку інформації

Різноманіття каналів витоку інформації надає зловмисникові великий вибір шляхів, способів і засобів добування інформації. На основі результатів аналізу кожного з каналів можна зробити наступні висновки:

1. Витік семантичної інформації можливий за всіма технічними каналами. По можливості витоку, а отже, за загрозою безпеки інформації їх можна ранжувати в наступній послідовності: радіоелектронний, акустичний і оптичний канали. Однак в деяких конкретних умовах можливі інші ранги каналів, наприклад, коли є реальна передумова для спостереження або фотографування документів.
2. Найбільшими потенційними можливостями з добування інформації про видові демаскуючі ознаки є оптичний канал, в якому інформація добувається шляхом фотографування. Це обумовлено наступними особливостями фотозображення:

- має найвищу роздільну здатність навіть на великій відстані від об'єкта спостереження, наприклад при детальній фотозйомці з космосу воно досягає 10 - 15 см на місцевості;

- має найвищу інформаційну ємність, обумовлену максимумом демаскуючих ознак, в тому числі наявністю такоїінформативної ознаки як колір;
- забезпечує відносно низький рівень геометричних спотворень.

Інформаційні ємності телевізійних зображень приблизно на порядок нижче фотозображень. Телевізійні зображення мають гіршу роздільну здатність, підвищений рівень яскравості спотворень через нерівномірність спектральних характеристик яскравості фотокатода передавальних телевізійних трубок або приладів із зарядним зв'язком, підвищений рівень геометричних спотворень через додаткові спотворення при формуванні електронного растра.

Зображення в ІЧ-діапазоні володіють ще більш низькими інформаційними параметрами. Крім низької роздільної здатності і великих спотворень для зображень в ІЧ-діапазоні характерна крайня мінливість яскравості протягом доби. Однак, як уже зазначалося при розгляді каналів витоку інформації, зображення в кожному з них містить додаткові ознаки через різну природу походження.

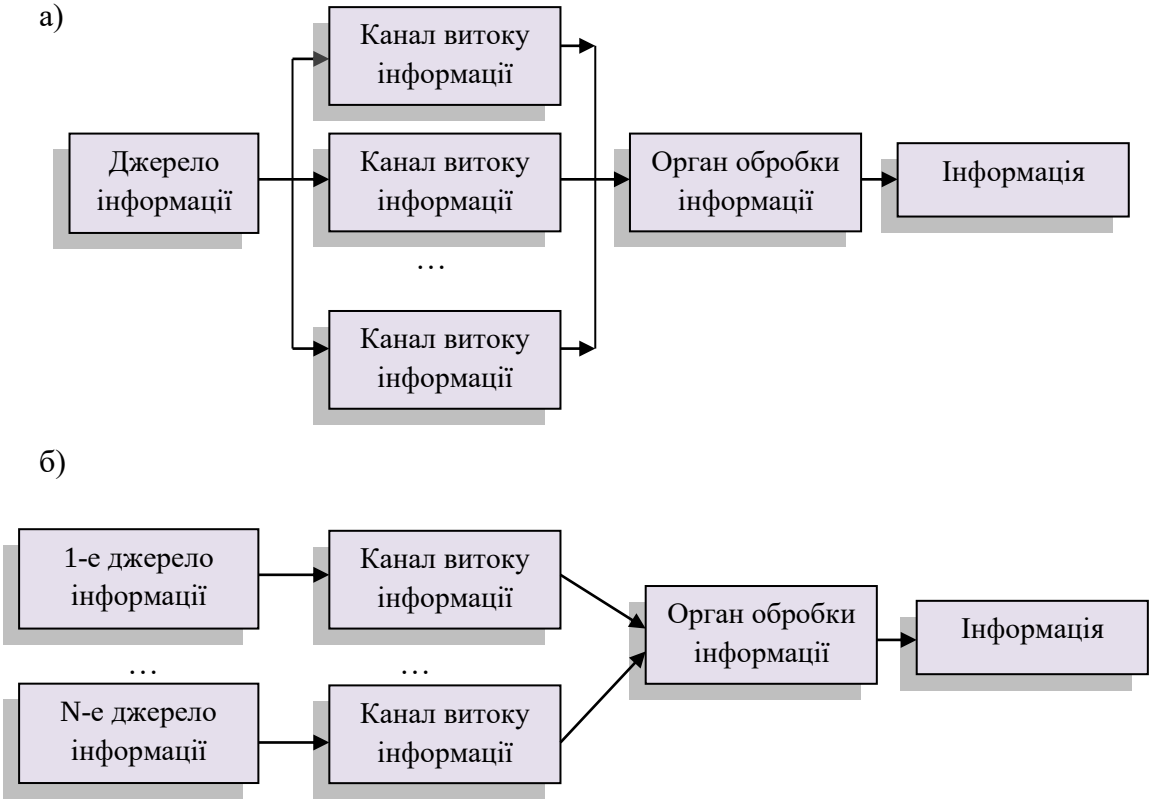
3. Основним каналом отримання сигнальних демаскуючих ознак є радіоелектронний. В значно меншому обсязі витік інформації про сигнальні демаскуючі ознаки можливий в акустичному каналі.

Для добування інформації зловмисник, як правило, використовує кілька каналів її витоку. Комплексне використання каналів витоку інформації зумовлюється наступними принципами:
- комплексні канали доповнюють один одного за своїми можливостями;
- ефективність комплексування підвищується при зменшенні залежності між джерелами інформації та демаскуючими ознаками в різних каналах. Комплексування каналів витоку інформації забезпечує:
- збільшення ймовірності виявлення і розпізнавання об'єктів через розширення їх поточних ознакових структур;
- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо при добуванні інформації з недостатньо надійних джерел.

Коли виникають сумніви в достовірності інформації, то для виключення дезінформації, отримані відомості і дані перевіряють по іншому каналу.

Можливі 2 основних види комплексування каналів витоку інформації: забезпечення витоку інформації від одного джерела з кількох паралельно функціонуючих каналів (мал. 2.3.2 а) і від різних джерел (мал.2.3.2 б).

У першому варіанті одна і та сама інформація поширюється по різних напрямках одним або різними носіями. Так, мовна інформація розмовляючих людей може бути підслухана через двері або стіну, знята з небезпечних сигналів або перехоплена в вигляді текстових документів.



Мал. 2.3.2. Варіанти комплексного використання каналів витоку

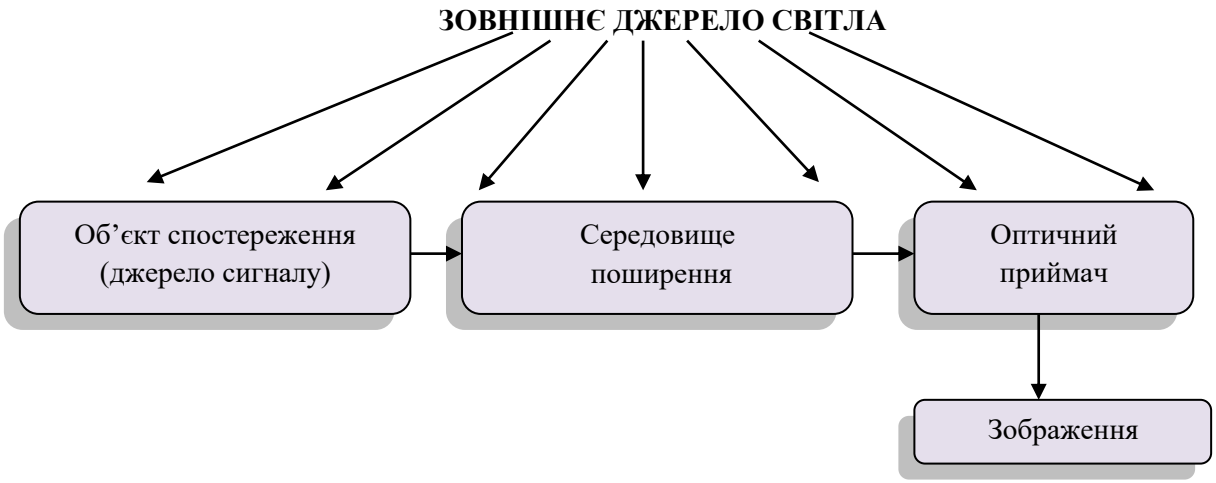
У другому варіанті одна і та ж інформація добувається від декількох джерел, наприклад документів і перехоплених телефонних переговорів. Цей варіант реалізується, якщо є ймовірність отримання дезінформації від одного ненадійного джерела.

2.4. ОСНОВНІ СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ СПОСТЕРЕЖЕННЯ ОБ'ЄКТІВ.

2.4.1 ОПТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

Структура оптичного каналу витоку інформації має вигляд, показаний на мал.2.4.1.

Об'єкт спостереження в оптичному каналі витоку інформації є одночасно джерелом інформації і джерелом сигналу, тому що світлові промені, що несуть інформацію про видові ознаки об'єкта, являють собою відображені об'єктом промені зовнішнього джерела або його власні випромінювання.



Мал. 2.4.1 Структура оптичного каналу витоку інформації

Відбите від об'єкта світло містить інформацію про його зовнішній вигляд (видові ознаки), а випромінюване об'єктом світло - про параметри випромінювань (ознаки сигналів). Запис інформації відбувається в момент відбиття падаючого світла шляхом зміни його яскравості і спектрального складу. Випромінююче світло містить інформацію про рівень і спектральний склад джерел видимого світла, а в інфрачервоному діапазоні за характеристиками випромінювань можна також судити про температуру елементів випромінювання.

В інфрачервоному діапазоні потужність випромінювання об'єкта залежить від температури тіла або його елементів, потужності падаючого на об'єкт світла і коефіцієнта відображення об'єкта в цьому діапазоні.

Довжина (протяжність) каналу витоку залежить від потужності світла, об'єкта, властивостей середовища розповсюдження і чутливості фотоприймача. Середовище поширення в оптичному каналі витоку інформації можлива трьох видів:

- безповітряний (космічний) простір;
- атмосфера;
- оптичні світловоди.

Оптичний канал витоку інформації, середовище поширення якого містить ділянки ***безповітряного простору***, виникає при спостереженні за наземними об'єктами з космічних апаратів. Кордон між космічним простором і атмосферою

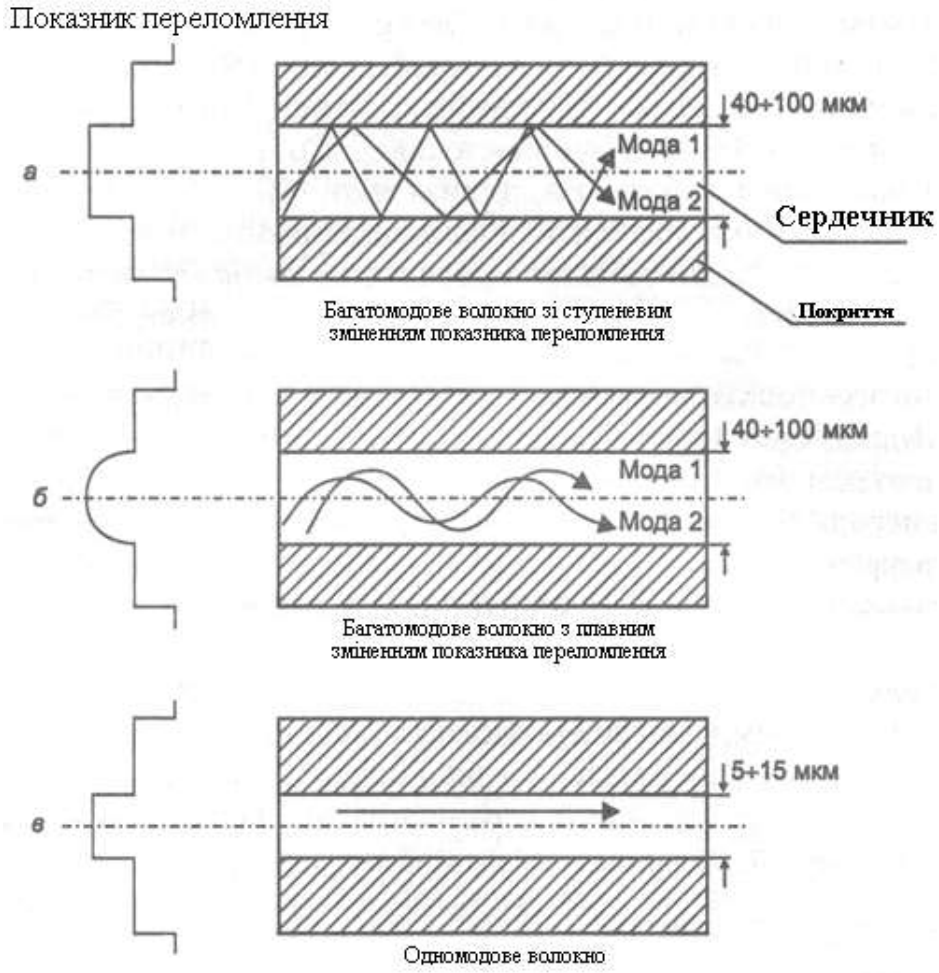
досить умовний. На висотах 200 - 300 км існують ще залишки газів, які проявляють гальмуючу дію на космічні апарати.

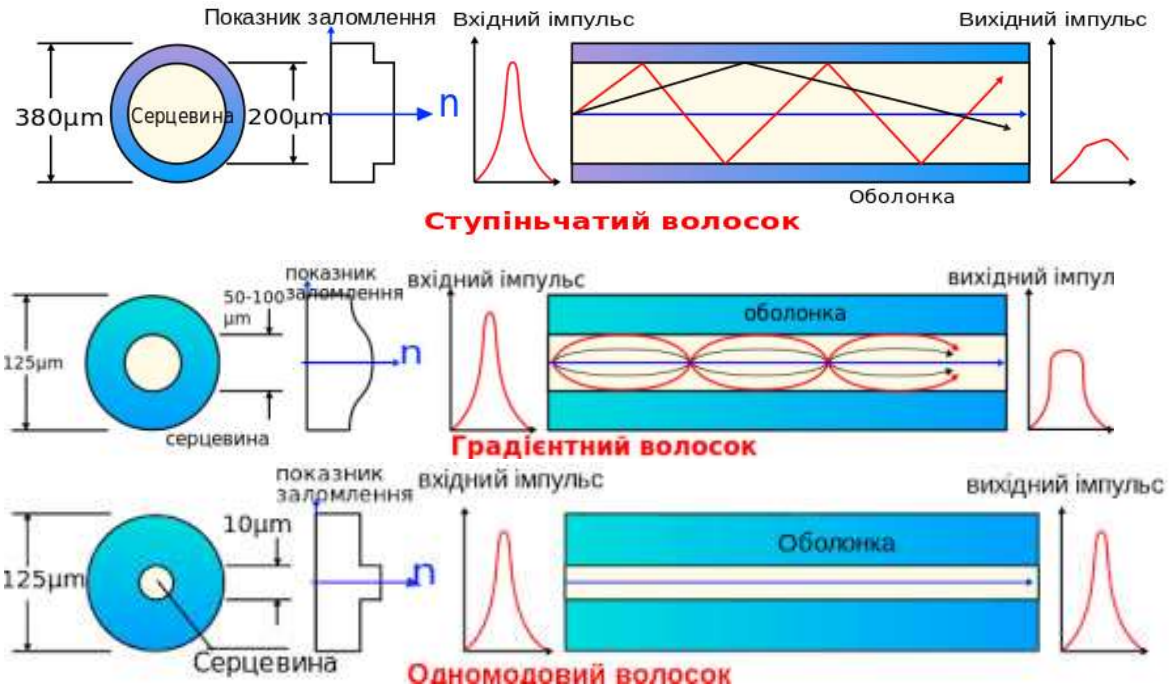
Метеорологічна видимість залежить від наявності в атмосфері зважених часток пилу і вологи, що утворюють імлу і туман, крапельок і кристалів води у вигляді дощу і снігу, а також аерозолів і димів, що містять тверді частинки. Все це викликає помутніння атмосфери і погіршує видимість. Прозорість атмосфери як каналу поширення світла оцінюється метеорологічної дальністю видимості.

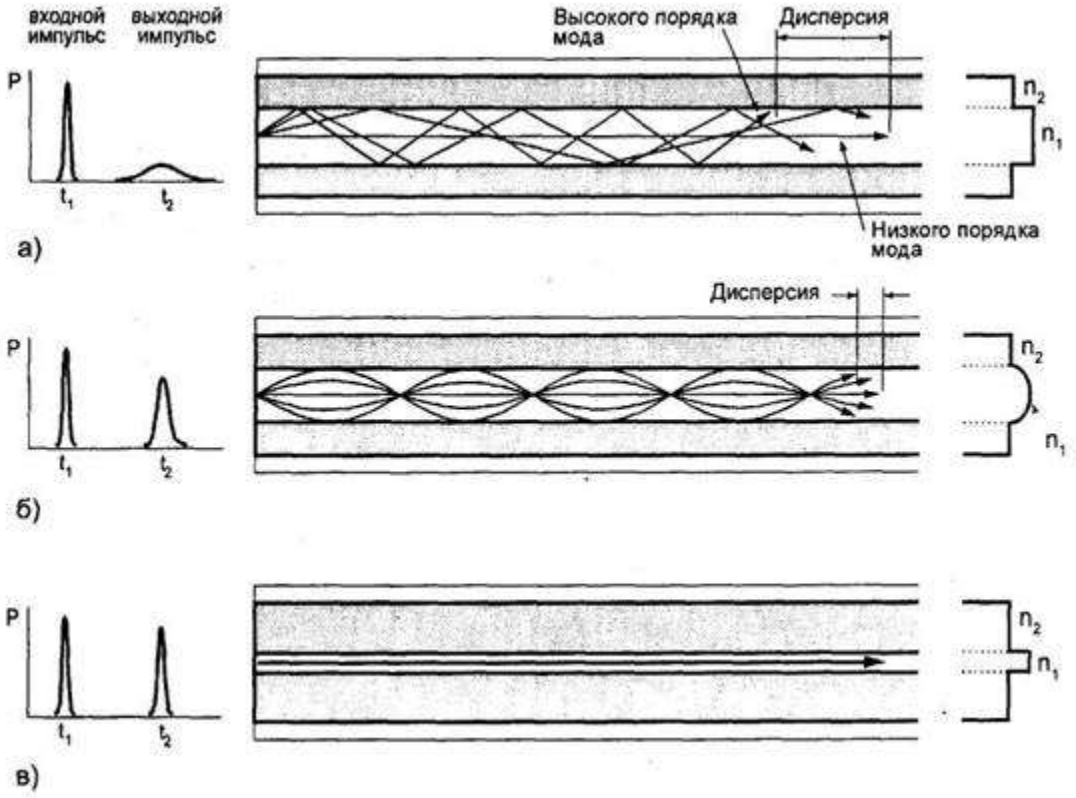
До недавнього часу атмосфера і безповітряний простір були єдиним середовищем поширення світлових хвиль. З розробкою **волоконно-оптичної технології** з'явилися направляючі лінії зв'язку в оптичному діапазоні, які через свої великі переваги по відношенню до традиційних електричних провідників розглядаються як більш досконалі фізичні середовища для передачі великих обсягів інформації. Лінії зв'язку, що використовують оптичне волокно, стійкі до зовнішніх перешкод, мають мале загасання, довговічні, забезпечують значно більшу безпеку переданої по волокну інформації.

Волокно являє собою нитку діаметром близько 100 мкм, виготовлену з кварцу на основі двоокису кремнію. Волокно складається з серцевини (світоводної жили) і оболонки з різними показниками заломлення.

Волокно з постійним показником заломлення серцевини називається ступінчастим, із змінним - градієнтним. Для передачі сигналів застосовуються 2 види волокна: одномодове і багатомодове (мал. 2.4.2).







Мал 2.4.2 Оптоволокно: а)звичайне; б)багатомодове градієнтне; в) одномодове

У одномодовому волокні світоводна жила має діаметр 8 - 10 мкм, по якій може поширюватися один промінь (одна мода). У багатомодовому волокні діаметр світоводної жили становить 50 - 60 мкм, що робить можливим поширення в ньому великої кількості променів.

Волокно характеризується двома основними параметрами: **загасанням** і **дисперсією**. Загасання вимірюється в децибелах на кілометр (дБ/км) і визначається втратами на поглинання і розсіювання світла в оптичному волокні. Втрати на поглинання залежать від чистоти матеріалу, а втрати на розсіювання - від неоднорідності показника заломлення. Кращі зразки волокна мають згасання 0,15 - 0,2 дБ/км, розробляються ще більш «прозорі» волокна з теоретичними значеннями загасання 0,02дБ/км для хвилі довжиною 2,5 мкм. При такому загасанні сигнали можуть передаватися на відстань в сотні км без ретрансляції (регенерації).

Дисперсія обумовлена відмінністю фазових швидкостей окремих мод оптичного сигналу, направляючими властивостями волокна і властивостями його матеріалу. Вона призводить до спотворення (розширення та зглаження фронтів) форми сигналу при його поширенні в волокні, що обмежує дальність передачі і верхнє значення частоти спектра сигналу, що обмежує максимальну швидкість передачі даних. Дисперсія волокна оцінюється величиною збільшення на 1 км довжини тимчасового параметра оптичного сигналу або еквівалентною смугою частот пропускання.

Волокна об'єднують в волоконно-оптичні кабелі, покриті захисною оболонкою. За умовами експлуатації кабелі поділяються на **монтажні**, **станційні**, **зонові** і **магістральні**. Кабелі перших двох типів використовуються всередині будівель і споруд. Зонові і магістральні кабелі прокладаються в колодязях кабельних комунікацій, в грунтах, на опорах, під водою.

Хоча можливість витоку інформації з волоконно-оптичного кабелю істотно нижче, ніж з електричного, але за певних умов такий витік можливий. Для знімання інформації руйнують захисну оболонку кабелю, притискають фотодетектор приймача до очищеної частини волокна і згинають кабель під кутом, при якому частина світлової енергії спрямовується на фотодетектор приймача.

2.5. ОСНОВНІ СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ ПІДСЛУХОВУВАННЯ СИГНАЛІВ.

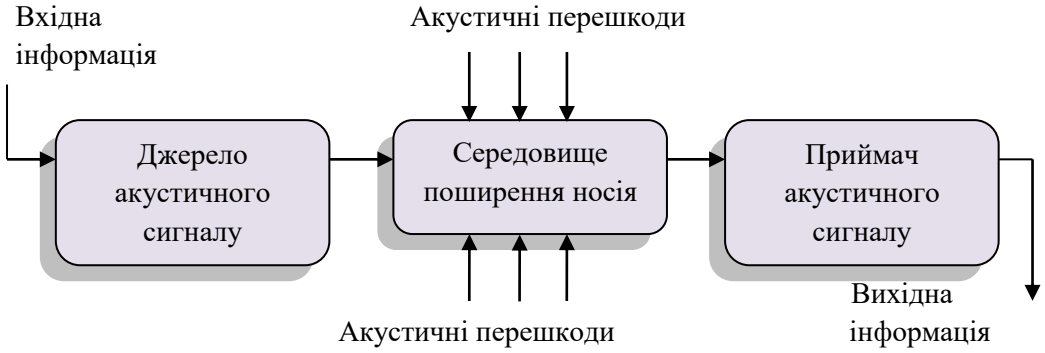
2.5.1 АКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

В акустичному каналі витоку носієм інформації від джерела до несанкціонованого одержувача є акустична хвиля в атмосфері, воді і твердому середовищі. Джерелами її можуть бути:

- розмова людини підслуховується в реальному масштабі часу або озвучується звуковідтворюючим пристроєм;
- механічні вузли механізмів і машин, які при роботі видають акустичні хвилі.

Структура цього каналу витоку інформації принципово не відрізняється від структури розглянутих каналів витоку інформації на (мал. 2.5.1).

Середовище поширення носія інформації від джерела до приймача може бути однорідним (повітря, вода) і неоднорідним, утвореними послідовними ділянками різних фізичних середовищ: повітря, деревини дверей, скляних вікон, бетону або цегли стін, різними породами земної поверхні і т. п. Але і в однорідному середовищі її параметри не постійні, а можуть істотно відрізнятися в різних точках простору.



Мал. 2.5.1 Структура акустичного каналу витоку інформації

Акустичні хвилі, як носії інформації, характеризуються такими показниками і властивостями:

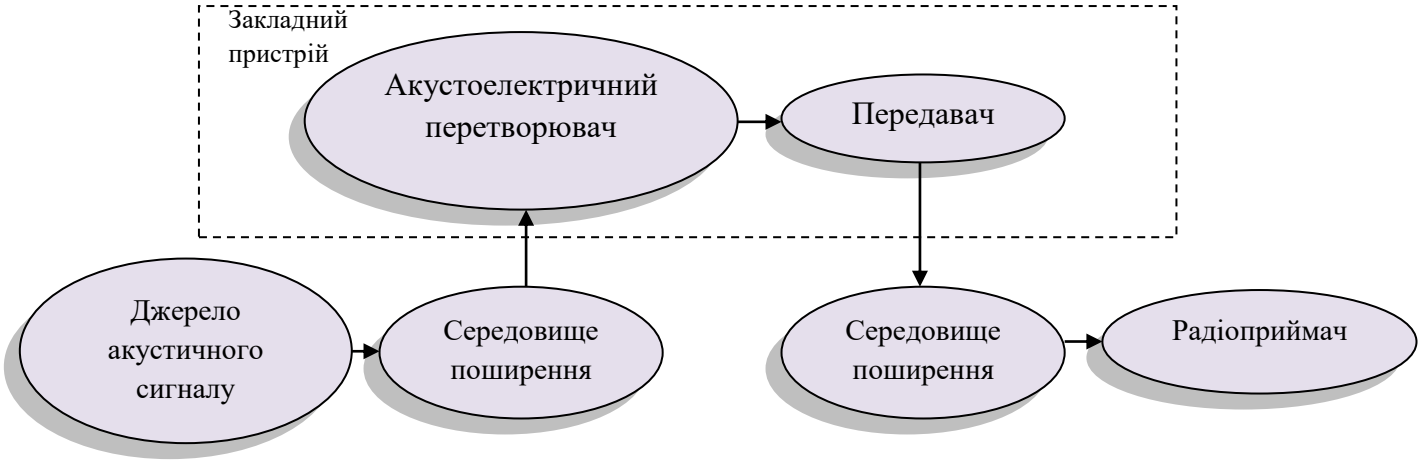
- швидкістю поширення носія;
- величиною (коефіцієнтом) загасання або поглинання;
- умовами поширення акустичної хвилі (коефіцієнтом відбиття від кордонів різних середовищ, дифракцією).

Акустична хвиля, на відміну від електромагнітної, значною мірою поглинається в середовищі поширення. Тому дальність акустичного каналу витоку інформації, особливо від такого малопотужного джерела як людина, мала і, як правило, не забезпечує можливість її знімання за межами території організації. Мова людини при звичайній гучності може бути безпосередньо підслухана зловмисником на відстані одиниць і в рідкісних випадках - десятків метрів, що вкрай мало.

Пошуки шляхів підвищення дальності добування мовної інформації привели до появи складових каналів витоку інформації. Застосовуються 2 види складеного каналу витоку інформації: акусто-радіоелектронний і акусто-оптичний.

Акусто-радіоелектронний (мал. 2.5.2) канал витоку інформації складається з двох послідовно сполучених каналів: акустичного і радіоелектронного каналів витоку інформації.

Приймачем акустичного каналу є функціональний або випадково утворений акустоелектричний перетворювач. Електричний сигнал з його виходу надходить на вхід радіоелектронного каналу витоку інформації - джерела електричних або радіосигналів.

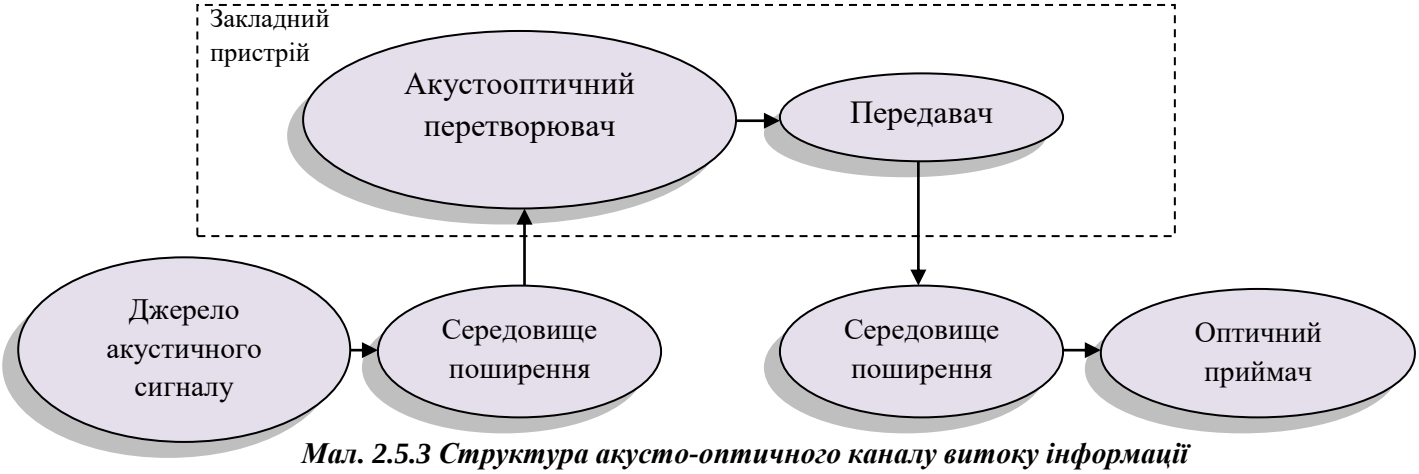


Мал. 2.5.2 Структура акусто-радіоелектронного каналу витоку інформації

Пара акусто-електричний перетворювач – джерело сигналу, утворюють джерело небезпечних сигналів або реалізуються в закладному пристрої, що розміщується зловмисником в приміщенні. Закладні пристрої створюються спеціально для підслуховування мовної інформації і забезпечують підвищення дальності складеного акустичного каналу до одиниць км і можливість знімання інформації зловмисником за межами контрольованої зони.

Закладний пристрій як ретранслятор є більш надійним елементом каналу витоку, ніж джерело небезпечного сигналу, тому що процес утворення каналу витоку інформації на основі закладки керується зловмисником. Інший спосіб підвищення дальності акустичного каналу витоку інформації реалізується шляхом створення складеного акусто-оптичного каналу витоку інформації. Схема його вказана на мал.2.5.3.

Складовий акусто-оптичний канал витоку інформації утворюється шляхом знімання інформації з плоскої поверхні, що коливається під дією акустичної хвилі з інформацією, лазерним променем в інфрачервоному (ІЧ) діапазоні. В якості такої поверхні використовується зовнішнє скло закритого вікна в приміщенні, в якому циркулює секретна (конфіденційна) інформація.



Мал. 2.5.3 Структура акусто-оптичного каналу витоку інформації

Для створення оптичного каналу скло опромінюється лазерним променем з зовнішньої сторони, наприклад з вікна протилежного будинку. Промінь лазера в ІЧ-діапазоні для сторонніх осіб і осіб, що знаходяться в приміщенні – невидимий. У місці зіткнення лазерного променя зі склом відбуваються акустооптичні перетворення, тобто модуляція лазерного променя акустичними сигналами від розмовляючих в приміщенні людей.

Модульований лазерний промінь приймається оптичним приймачем апаратури лазерного підслуховування, перетворюється в електричний сигнал, який посилюється, фільтрується, демодулюється і подається в головні телефони для прослуховування оператором або в аудіомагнітофон для консервації.

2.6 ОСНОВНІ СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ ПЕРЕХОПЛЕННЯ СИГНАЛІВ.

2.6.1 РАДІОЕЛЕКТРОННІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

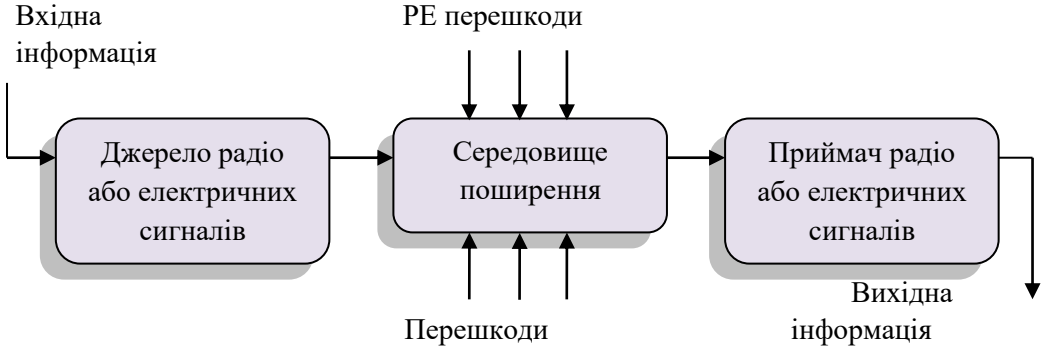
У радіоелектронному каналі передачі носієм інформації є електричний струм і електромагнітне поле з частотами коливань від звукового діапазону до десятків ГГц.

Радіоелектронний канал відноситься до найбільш інформативних каналів витоку завдяки таким особливостям:

- незалежність функціонування каналу від часу доби і року, істотно менша залежність його параметрів у порівнянні з іншими каналами від метеоумов:
- висока достовірність видобуваємої інформації, особливо при перехопленні її в функціональних каналах зв'язку (за винятком випадків дезінформації);
- великий обсяг видобутої інформації;
- оперативність отримання інформації, аж до реального масштабу часу;
- скритність перехоплення сигналів і радіотеплового спостереження.

У радіоелектронному каналі відбувається перехоплення радіо і електричних сигналів, радіолокаційне та радіотеплове спостереження. Отже, в рамках цього каналу витоку добувається семантична інформація, видові і сигнальні демаскуючі ознаки. Радіоелектронні канали витоку інформації використовують радіо, радіотехнічна, радіолокаційна і радіотеплова розвідка.

Структура радіоелектронного каналу витоку інформації в загальному випадку включає джерело сигналу, або передавач, середу поширення електричного струму або електромагнітної хвилі і приймач сигналу (мал. 2.6.1).



Мал. 2.6.1 Структура радіоелектронного каналу витоку інформації

У радіоелектронних каналах витоку інформації джерела сигналів можуть бути чотирьох видів:

- передавачі функціональних каналів зв'язку;
- джерела небезпечних сигналів;
- об'єкти, що відображають електромагнітні хвилі в радіодіапазоні;
- об'єкти, що випромінюють власні (теплові) радіохвилі в радіодіапазоні.

Середовищем поширення радіоелектронного каналу витоку інформації є атмосфера, безповітряний простір і направляючі – електричні дроти різних типів та хвилеводи. Носій у вигляді електричного струму поширюється по дротах, а електромагнітне поле – в атмосфері, в безповітряному просторі або по направляючим – волноводам. У приймальнику відбувається виділення (селекція) носія з інформацією, що цікавить одержувача по частоті, посилення виділеного слабкого сигналу і знімання з нього інформації – демодуляція.

При перехопленні сигналів функціональних каналів зв'язку передавачі цих каналів є одночасно джерелами радіоелектронних каналів витоку інформації. У загальному випадку напрямок поширення електромагнітної хвилі від передавача до санкціонованого одержувача і зловмисника відрізняється. У функціональних каналах зв'язку максимум випромінювання енергії електромагнітної хвилі орієнтують в напрямку розташування приймача санкціонованого одержувача. Тому потужність джерела сигналів радіоелектронного каналу витоку інформації, як правило, істотно менше потужності випромінювання в функціональному каналі зв'язку.

Залежно від способу перехоплення інформації розрізняють 2 види радіоелектронного каналу витоку інформації.

У каналі витоку першого виду виробляється перехоплення інформації, що передається по функціональному каналу зв'язку. Для цього приймач сигналу каналу витоку інформації налаштовується на параметри сигналу функціонального радіоканалу або підключається (контактно або дистанційно) до проводів відповідного функціонального каналу. Такий канал витоку має спільне з функціональним каналом джерело сигналів – передавач. Так як місця розташування приймачів функціонального каналу і каналу витоку інформації в загальному випадку не збігаються, то середовище поширення сигналів в них від загального передавача різні або збігаються, наприклад до місця підключення приймача зловмисника до проводів телефонної мережі.

Радіоелектронний канал витоку другого виду має власний набір елементів: передавач сигналів, середу поширення і приймач сигналів. Передавач цього каналу витоку інформації утворюється випадково (без участі джерела або одержувача інформації) або спеціально встановлюється в приміщенні зловмисником. В якості такого передавача застосовуються джерела небезпечних сигналів і закладні пристрої.

Електричні сигнали як носії інформації можуть бути аналоговими або дискретними, їх спектр може містити частоти від десятків Гц до десятків ГГц.

Найбільш широко застосовуються сигнали, ширина спектра яких відповідає ширині спектра стандартного телефонного каналу. Такі сигнали передають мовну інформацію за допомогою телефонних апаратів і поширюються по направляючих лініях зв'язку, що зв'язують абонентів як всередині організації, так і всередині населеного пункту, міста, країни, земної кулі в цілому.

У загальному випадку направляючі лінії зв'язку створюються для передачі сигналів в заданому напрямку з належною якістю і надійністю. Способи і засоби передачі електричних

сигналів по дротах розглядаються прикладної областю електрозв'язку, так званим проводним зв'язком.

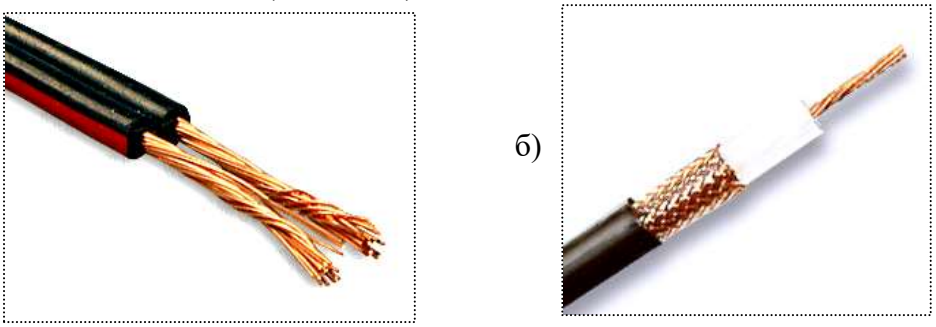
Розрізняють повітряні і кабельні провідні лінії зв'язку. ***Повітряні лінії*** зв'язку відносяться до симетричних ланцюгів, відмінною рисою яких є наявність двох провідників з однаковими електричними властивостями.

Залежно від типу несучих конструкцій вони діляться на стовпові і стійкі. ***Стовповими*** називаються лінії, несучими конструкціями яких є дерев'яні або залізобетонні опори. Опорами стовпових ліній служать металеві стійки, встановлені, наприклад, на дахах будівель. Для ізоляції проводів повітряних ліній один від одного і щодо землі їх зміцнюють на порцелянових ізоляторах.

Більш широко застосовуються кабельні лінії зв'язку. Кабельні лінії зв'язку отримали домінуючий розвиток при організації об'єктової, міського та міжміського телефонного зв'язку. Вони складають 65% телефонних ліній України. Кабелі бувають симетричними і коаксіальними.

Якщо обидві жили ланцюга, утвореного кабелем, виконані з дроту однакового діаметра, мають однакову ізоляцію і розташовані так, що між ними можна провести площину симетрії, то кабель називається ***симетричним***. Якщо ж обидва провідника ланцюга виконані у формі співвісних циліндрів, в поперечному перерізі мають форму концентричних кіл, то такий кабель – ***коаксіальний*** (мал. 2.6.2).

а) б)

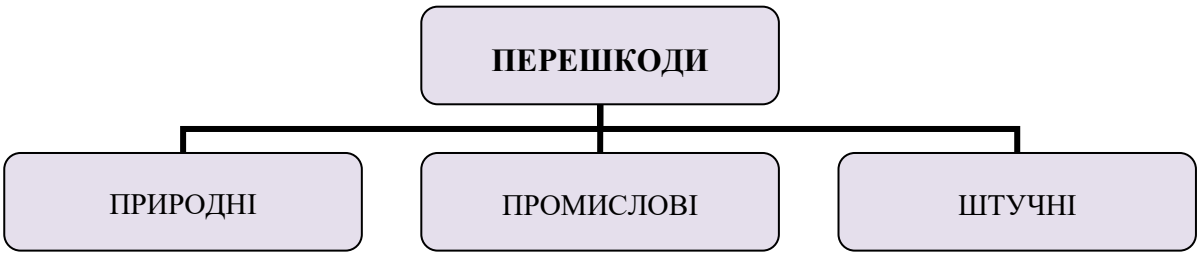


Мал. 2.6.2 Зовнішній вигляд а) симетричного і б) коаксіального кабелю

Основними параметрами провідних ліній зв'язку є ширина спектру частот, що пропускається ними, потужність сигналу на вході і виході ланцюга відповідно.

Радіохвилі в залежності від умов поширення діляться на земні (поверхневі), прямі, тропосферні і іоносферні (просторові).

Різноманіття природних і штучних джерел випромінювань в радіодіапазоні породжує проблему електромагнітної сумісності радіосигналів з певною інформацією з іншими радіосигналами – перешкодами з співпадаючими частотами. Класифікація перешкод представлена на мал.2.6.3.



Мал.2.6.3 Класифікація перешкод в технічних каналах витоку

Природні перешкоди можуть бути викликані наступними природними явищами:

- електричними грозовими розрядами, як правило, на частотах менше 30 МГц;
- переміщенням електрично заряджених частинок хмар, дощу, снігу та ін.,
- виникненням резонансних електричних коливань між землею і іоносферою;
- тепловим випромінюванням Землі і будівель в діапазоні понад 30 – 40 МГц;
- сонячною активністю в основному на частотах понад 20 МГц;
- електромагнітними випромінюваннями неба, Місяця, інших планет (на частотах понад 1 МГц);
- тепловими шумами в елементах і ланцюгах радіоприймачів.

Так як електромагнітні хвилі в радіодіапазоні є основними носіями інформації, то для порушення управління були створені різноманітні засоби генерування перешкод.

За ефектом впливу радіоелектронні перешкоди діляться на маскуючі та імітуючі. ***Маскуючі перешкоди*** створюють перешкоджаючий фон, на якому ускладнюється або виключається виявлення і розпізнавання корисних сигналів. ***Імітуючі перешкоди*** по структурі близькі до корисних сигналів і при прийомі можуть ввести в оману одержувача.

За співвідношенням спектра перешкод і корисних сигналів перешкоди підрозділяються на загороджувальні і прицільні. ***Загороджувальні перешкоди*** мають ширину спектра частот, що значно перевищує ширину спектру корисного сигналу, що дозволяє пригнічувати сигнал без точної настройки на його частоту.

Прицільна перешкода має ширину спектра, порівняну (що дорівнює або перевищує в 1,5 – 2 рази) з шириною спектра сигналу, і створює високий рівень спектральної щільності потужності в смузі частот сигналу при невисокій середній потужності передавача перешкод. По часовій структурі випромінювання перешкоди бувають безперервні і імпульсні (у вигляді немодульованих або модульованих радіоімпульсів).

Контрольні питання:

1. Що розуміють під витоком інформації?
2. Назвіть особливості витоку інформації технічними каналами.
3. Наведіть структуру каналу витоку інформації.
4. Наведіть класифікацію технічних каналів витоку інформації.
5. Наведіть структуру оптичного каналу витоку інформації.
6. Охарактеризуйте радіоелектронний канал витоку інформації.
7. Дайте класифікацію перешкод в каналах передачі інформації.
8. Охарактеризуйте акустичні канали витоку інформації.
9. Наведіть структуру акусто-радіоелектронного каналу витоку інформації.
10. Наведіть структуру акусто-оптичного каналу витоку інформації.
11. Назвіть основні способи реалізації комплексного каналу витоку інформації.

3. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

3.1 МЕТОДОЛОГІЯ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

3.1.1 ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ.

Об'єкт посягань інженерно-технічної розвідки противника - це інформація, витік якої здатний завдати шкоди безпеці об'єкту. Для раціонального забезпечення захисту інформації та скорочення витрат на реалізацію конкретних заходів, необхідно враховувати наступні принципи, що характеризують професійний підхід до цих питань:

• відповідність рівня захисту ступеню цінності інформації;

• гнучкість захисту;

• багатозональність засобів захисту (тобто розміщення джерел інформації в зонах з контрольованим рівнем її безпеки);

• багаторубіжність засобів захисту інформації на шляху руху ворожого агента (або технічного засобу розвідки).

Відповідність рівня захисту цінності інформації. Цей принцип визначає економічну доцільність тих чи інших заходів захисту. Він полягає в тому, що витрати на захист не повинні перевищувати ціну, що захищається. В іншому випадку захист нерентабельний.

Гнучкість захисту проявляється в можливості зміни ступеня захищеності відповідно до зміни вимог до безпеки об'єкту захисту в цілому та інформації зокрема. Захист повинен бути гнучким тому, що ціна інформації - величина змінна, що залежить як від джерела інформації, так і від часу.

Ступінь захищеності інформації визначає рівень її безпеки. Необхідний рівень безпеки інформації досягається багатозональністю і багаторубіжністю захисту.

Багатозональність забезпечує диференційований санкціонований доступ різних категорій співробітників і відвідувачів до джерел інформації.

Даний принцип реалізується шляхом поділу простору, займаного об'єктом захисту.

Типовими зонами є:

• територія, яку займає організацією і обмежена огорожею або умовними зовнішніми кордонами;

• будівлі та інші споруди на цій території;

• коридори, сходові марші, шахти ліфтів;

• приміщення (кабінети, кімнати, зали, технічні приміщення, склади і т.п.);

• шафи, сейфи, сховища.

Зони можуть бути незалежними (будівлі, приміщення в будинках), що перетинаються і вкладеними (кімнати всередині будівлі, сейфи всередині кімнат).

Для перешкоджання проникненню агента противника в зону, на її кордоні створюються один чи кілька рубежів захисту. Особливістю захисту кордону зони є вимога рівної міцності рубежів на кордоні, а також наявність контрольно-пропускних пунктів (постів), що забезпечують керований доступ людей і автотранспорту в зону.

Додамо, що своєрідними рубежами захисту є також негласні помічники служби безпеки. Вони знаходяться в контрольованих зонах у зв'язку зі своїми основними службовими обов'язками і одночасно відстежують ситуацію. При необхідності вони негайно повідомляють в підрозділ служби безпеки про виявлені порушення або інших значущих фактах.

Рубежі захисту створюються і всередині зон на можливих шляхах руху агентів або поширення носіїв інформації (перш за все, електромагнітних і акустичних полів). Так, для захисту від підслуховування може бути встановлений кордон захисту у вигляді акустичного екрану.

Кожна зона характеризується рівнем безпеки для інформації, що в ній знаходиться. Безпека інформації в зоні залежить від наступних чинників:

• відстані від джерела інформації (сигналу) до шпигуна або його засобів добування інформації;

• числа і рівня захисту рубежів (агентурних і технічних) на шляху руху шпигуна або носія інформації (наприклад, поля);

• ефективності способів і засобів управління допуском людей і автотранспорту в зону;

• заходів щодо захисту інформації всередині зони.

Чим далі знаходиться джерело інформації від місця знаходження суб'єкта розвідки противника (або його технічного засобу добування інформації) і чим більше рубежів захисту, тим більше часу займає просування шпигуна до цього джерела (тим сильніше слабшає енергія носія у вигляді поля або сили електричного струму).

Число зон і рубежів захисту, їх просторове розташування слід вибирати таким чином, щоб забезпечити необхідний рівень безпеки інформації, що захищається як від зовнішніх загроз (що знаходяться поза територією), так і внутрішніх (агентів, що проникли на територію, встановлених там технічних засобів знімання інформації). Чим більш цінною є інформація, що захищається, тим більшим числом рубежів і зон доцільно оточувати її джерело.

При створенні інженерно-технічної системи захисту доцільно, крім того, враховувати принципи:

• надійність агентурних і технічних засобів системи, що виключають як пропуск загроз, так і помилкові дії;

• обмежений і контрольований доступ до інженерно-технічних елементів системи забезпечення безпеки інформації;

• безперервність роботи системи в будь-яких умовах функціонування об'єкта захисту (наприклад, при короткочасній відсутності електроенергії);

• адаптованість (пристосованість) системи до змін навколишнього середовища.

Сенс зазначених принципів очевидний, слід лише доповнити останній з них. Справа в тому, що закриті відомості про способи і засоби захисту інформації в конкретній організації з часом стають відомими все більшій кількості людей, в результаті чого збільшується ймовірність отримання цієї інформації агентами противника. Тому доцільно періодично змінювати структуру системи захисту або ж робити це при виникненні реальної загрози витоку інформації, наприклад при звільненні інформованого співробітника служби безпеки.

Реалізація зазначених принципів в системі контррозвідувального захисту дозволяє наблизити її до абсолютної. Останню можна визначити як систему, що володіє всіма можливими способами захисту, здатну в будь-який момент прогнозувати наступ загрозливої події з випередженням її за часом, достатнім для застосування адекватних заходів.

3.1.2 ОСНОВНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ.

При захисті інформації технічними засобами (технічна контррозвідка) необхідно враховувати вимоги:

• джерело та носій інформації локалізуються в межах кордонів об'єкта захисту;

• забезпечується механічна перешкода від контакту з ними шпигуна, від дистанційного взаємодії з ними його технічних засобів добування;

• співвідношення енергії носія і перешкод на виході приймача каналу витоку таке, що шпигунові не вдається зняти інформацію з носія або забезпечити необхідну для користувача якість;

• шпигун не в змозі виявити джерело або носій інформації;

• замість правдивої інформації шпигун отримує неправдиву (завдяки діям контррозвідки).

Для реалізації цих вимог використовуються методи:

• перешкоджання за допомогою інженерних конструкцій і технічних засобів охорони безпосередньому проникненню шпигуна до джерела інформації;

• приховування достовірної інформації;

• дезінформація - «підкидання» противнику неправдивої інформації.

Способи захисту інформації на основі інженерних конструкцій, в поєднанні з технічними засобами охорони і за участю негласних можливостей служби безнеки досить поширені. Сукупність цих способів утворює так званий фізичний захист, надійність якого постійно «висвітлює», а в ряді випадків і забезпечує, агентура служби безпеки.

Але цей термін невдалий, так як інші методи захисту за допомогою технічних засобів теж засновані на фізичних законах. З огляду на те, що основу даного методу складають інженерні конструкції і технічні засоби охорони, його доцільно визначити як інженерний захист і технічна охорона об'єктів (ІЗТОО).

Основним завданням ІЗТОО є недопущення (запобігання) безпосереднього контакту суб'єкта розвідки противника, а також сил природи з об'єктами захисту. Під об'єктами захисту розуміються як люди і матеріальні цінності, так і носії інформації, локалізовані в просторі.

До числа таких носіїв відноситься папір, машинні носії, фото- і кіноплівка, продукція, матеріали і т.п., тобто все те, що має певні розміри і вагу. Носії інформації у вигляді електромагнітних і акустичних полів, електричного струму не мають чітких меж і для захисту інформації на цих носіях методи інженерного захисту неприйнятні. Так, електромагнітне поле з інформацією можна зберігати в сейфі. Для захисту інформації на таких носіях застосовують методи захисту інформації технічними засобами (мал. 1.1.1).

Приховування інформації передбачає такі зміни структури і енергії її носіїв, при яких шпигун не може як безпосередньо, так і за допомогою технічних засобів виявити інформацію, що володіє якостями, достатніми для використання її у власних інтересах.

Мал. 1.1.1 Методи захисту інформації технічними засобами

Розрізняють інформаційне та енергетичне приховування. ***Інформаційне приховування*** досягається зміною портрета (або створенням помилкового) семантичного повідомлення, фізичного об'єкта або сигналу.

Інформаційний портрет - це сукупність елементів і зв'язків між ними, що відображають зміст повідомлення (мовного або данних), ознаки об'єкта або сигналу. Елементами семантичного повідомлення, наприклад, є літери, цифри та інші знаки, а зв'язки між ними визначають їх послідовність. Інформаційні портрети об'єктів спостереження, сигналів і речовин є їх еталонними ознаковими структурами.

Можливі такі способи зміни інформаційного портрета:

• видалення частини елементів і зв'язків, що утворюють інформаційний вузол, (найбільш інформативну частину);

• зміна частини елементів інформаційного портрета при збереженні незмінності зв'язків між рештою елементами;

• видалення або зміна зв'язків між елементами інформаційного портрета при збереженні їх загального числа.

При зміні інформаційного портрета об'єкта відбувається зміна зображення його зовнішнього вигляду (видових ознак), характеристик випромінюваних ним полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення ознакових структур об'єкта і фону, що його оточує, в результаті чого знижується контрастність зображення об'єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання.

В умовах ринку, коли виробник змушений рекламувати свій товар, найбільш доцільним способом інформаційного приховування є виключення з реклами та відкритих публікацій найбільш інформативних відомостей або ознак, тобто інформаційних вузлів, які містять таємницю, що охороняється.

До інформаційних вузлів відносяться принципово нові технічні, технологічні та образотворчі рішення та інші досягнення, які складають «ноу-хау». Вилучення з технічної документації інформаційних вузлів не дозволяє конкурентам користуватися інформацією, що міститься в рекламі або публікаціях.

Цей поширений спосіб дає можливість:

• суттєво зменшити обсяг інформації, що захищається і тим самим спростити проблему захисту інформації;

• використовувати в рекламі нової продукції відомості про неї, не побоюючись розголошення. Так, замість захисту інформації в сотнях і тисячах аркушів технічної документації, яка розробляється для виробництва нової продукції, захисту підлягають лише кілька десятків листів з інформаційними вузлами.

Інший метод інформаційного приховування полягає в перетворенні вихідного інформаційного портрета в новий, такий, що відповідає помилковій семантичній інформації або помилковій ознаковій структурі, і «нав'язуванні» нового портрета органу ворожої розвідки. Такий метод захисту називається ***дезінформуванням***.

Принципова відмінність інформаційного приховування шляхом зміни інформаційного портрета від дезінформування полягає в тому, що перший метод спрямований на ускладнення виявлення об'єкта з інформацією серед інших об'єктів (фону), а другий - на створення ознак помилкового об'єкта на цьому тлі.

Дезінформування відноситься до числа найбільш ефективних способів захисту інформації і застосовується контррозвідкою з наступних причин. По-перше, воно дає власнику, що захищається запас часу, обумовлений перевіркою розвідкою достовірності отриманої інформації. По-друге, наслідки рішень, прийнятих опонентом на основі неправдивої інформації можуть виявитися для нього гіршими у порівнянні з рішеннями, прийнятими при відсутності видобутої інформації.

Однак цей метод досить складно реалізувати. Основна проблема полягає в забезпеченні достовірності помилкового інформаційного портрета. Дезінформування тільки тоді досягає мети, коли у розвідки протилежної сторони не виникає сумнівів в істинності неправдивої інформації, що їй підкидається. В іншому випадку може вийти протилежний ефект, так як розкриття розвідкою факту дезінформування скоротить сферу пошуку правдивої інформації.

Тому підрозділ контррозвідки служби безпеки повинен дуже серйозно підходити до організації процесу дезінформації. Дезінформування здійснюється шляхом підгонки ознак інформаційного портрета об'єкта захисту під ознаки інформаційного портрета помилкового об'єкта. Тут все вирішують продуманість вихідної версії і бездоганність її реалізації. Вихідна версія повинна передбачати комплекс заходів, розподілених у часі і в просторі, і спрямованих на імітацію ознак помилкового об'єкта. Причому чим менше при цьому використовується неправдивих відомостей і ознак, тим важче розкрити помилковий характер інформаційного портрета.

Розрізняють наступні способи дезінформування:

1. Заміна реквізитів інформаційних портретів, які захищаються (якщо інформаційний портрет об'єкта захисту схожий на інформаційні портрети інших «відкритих» об'єктів і не має специфічних інформаційних ознак). В цьому випадку обмежуються розробкою і підтримкою версії про інший об'єкт, видаючи в якості його ознак ознаки об'єкта, що захищається. Так, в даний час велика увага приділяється розробкам продукції подвійного застосування – військового і цивільного. Поширення інформації про виробництво продукції суто цивільного використання є надійним прикриттям її варіантів військового призначення.

2. Підтримка помилкової версії з ознаками, запозиченими від інформаційних портретів декількох різних реальних об'єктів. Шляхом різних поєднань ознак, що відносяться до різних тем, можна нав'язати противнику помилкове уявлення про роботи, що ведуться, не імітуючи додаткові ознаки.

3. Поєднання справжніх і несправжніх ознак, причому помилковими замінюється незначна, але найцінніша частина інформації, що відноситься до об'єкта захисту.

4. Зміна одних тільки інформаційних вузлів зі збереженням незмінною іншої частини інформаційного портрета.

Як правило, використовуються різні комбінації цих варіантів.

Енергетичне приховування. Іншим ефективним методом захисту інформації є ***енергетичне приховування***. Воно полягає в застосуванні способів і засобів захисту інформації, що виключають або ускладнюють дотримання енергетичної умови розвідувального контакту. Енергетичне приховування досягається шляхом зменшення співвідношення енергії (потужності) сигналів, тобто носіїв інформації (електромагнітного або акустичного поля, електричного струму) і перешкод.

Це досягається наступним чином. Якщо носієм інформації є амплітудно-модульована електромагнітна хвиля, а в середовищі поширення носія інформації присутня перешкода у вигляді електромагнітної хвилі, що має однакову з носієм частоту, але випадкову амплітуду і фазу, то відбувається інтерференція цих хвиль.

В результаті значення інформаційного параметра (амплітуди сумарного сигналу) випадковим чином змінюється і інформація спотворюється. Чим менше відношення потужностей амплітуд, сигналу і перешкоди, тим в більшій мірі значення амплітуди сумарного сигналу будуть відрізнятися від вихідних (встановлюються при модуляції) і тим більше буде спотворюватися інформація.

Якість прийнятої інформації погіршується із зменшенням співвідношення сигнал/перешкода. Ступінь залежності якості прийнятої інформації від співвідношення сигнал/перешкода відрізняється для різних видів інформації (аналогової, дискретної), носіїв і перешкод, способів запису на носій (виду модуляції), параметрів засобів прийому та обробки сигналів.

Так як технічний засіб розвідки зазвичай наближений до кордонів контрольованої зони об'єкта захисту, значення співвідношення сигнал/перешкода вимірюється на межі цієї зони. Необхідно забезпечити на цій межі значення співвідношення сигнал/перешкода нижче мінімально допустимої величини.

3.2 СИСТЕМНИЙ ПІДХІД ДО ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

СИСТЕМНИЙ ПІДХІД (англ. ***Systems thinking*** — системне мислення) — напрям методології досліджень, який полягає в дослідженні об'єкта як цілісної множини елементів в сукупності відношень і зв'язків між ними, тобто розгляд об'єкта як модель системи. В англомовній літературі це поняття холізму.

Остання домінуюча модель системного підходу мала назву експертного методу, який в рамках системного підходу вичерпно використовував метод аналога чи прототипу.

Ефективність системного підходу залежить від характеру застосовуваних загальносистемних закономірностей, що встановлюють зв'язок між системними параметрами. На сучасному етапі на основі узагальнення різних варіантів системного підходу створюються умови для побудови загальної теорії про системи — системології. Виникнення і поширення системного підходу зумовлено кризою елементаризму і механіцизму у зв'язку з ускладненням завдань науки і практики.

Системний підхід розвиває і конкретизує такі категорії діалектики, як зв'язок (філософія), відношення, зміст і форма, частина і ціле та ін.

Основні принципи системного підходу:

- **Цілісність**, яка дозволяє розглядати систему одночасно і як єдине ціле, і як підсистему вищестоячих рівнів.
- **Ієрархічність** побудови, тобто наявність множини (принаймні двох) елементів, які розташовані на основі підпорядкування елементів нижчого рівня елементам вищого рівня. Реалізація цього принципу добре видна на прикладі будь-якої конкретної організації, яка являє собою взаємодію двох підсистем: керуючої і керованої. Одна підпорядковується іншій.
- **Структуризація**, яка дозволяє аналізувати елементи системи і їх взаємозв'язки в рамках конкретної організаційної структури. Як правило, процес функціонування системи обумовлений не стільки властивостями її окремих елементів, скільки властивостями самої структури.
- **Множинність**, яка дозволяє використовувати множину кібернетичних, економічних і математичних моделей для опису окремих елементів і системи в цілому.
- **Системність** — властивість об'єкта володіти всіма ознаками системи.

Розгорнуте визначення системного підходу полягає в тому, що це підхід, при якому будь-яка система (об'єкт) розглядається як сукупність взаємозв'язаних елементів (компонентів), що має вихід (ціль), вхід (ресурси), зв'язок із зовнішнім середовищем, зворотний зв'язок. Це найскладніший підхід. Системний підхід є формою накладення теорії пізнання і діалектики з дослідженням процесів, що відбуваються в природі, суспільстві, мисленні. Його суть полягає в реалізації вимог загальної теорії систем, згідно з якою кожен об'єкт у процесі його дослідження повинен розглядатися як велика і складна система і, одночасно, як елемент загальнішої системи.

Це визначення системного підходу включає також обов'язковість вивчення і практичного використання таких восьми його аспектів:

1. ***системно-елементного*** або **системно-комплексного**, який полягає у виявленні елементів-складових даної системи. У всіх соціальних системах можна виявити речові компоненти (засоби виробництва і предмети споживання), процеси (економічні, соціальні, політичні, духовні, управлінські і т. д.) і ідеї, науково-усвідомлені інтереси людей і їх спільнот;
2. ***системно-структурного***, який полягає у з'ясуванні компонентів і елементів, внутрішніх зв'язків і залежностей між елементами даної системи, що дозволяє отримати уявлення про внутрішню організацію (будову) досліджуваної системи;
3. ***системно-функціонального***, який потребує виявлення функцій, для виконання яких створені і існують відповідні системи;
4. ***системно-цільового***, який означає необхідність наукового визначення завдань і підзавдань системи, їхніх взаємних зв'язків між собою;
5. ***системно-ресурсного***, який полягає в ретельному виявленні ресурсів, потрібних для функціонування системи, для вирішення системою тієї або іншої проблеми;
6. ***системно-інтеграційного***, який полягає у визначенні сукупності якісних властивостей системи, що забезпечують її цілісність і особливість;
7. ***системно-комунікаційного***, який означає необхідність виявлення зовнішніх зв'язків даної системи з іншими, тобто, її зв'язків з навколишнім середовищем;

8. ***системно-історичного***, який дозволяє з'ясувати умови в часі, які вплинули на виникнення досліджуваної системи, пройдені нею етапи, сучасний стан, а також можливі перспективи розвитку.

Елементом називається технічний об'єкт, що входить до складу системи або підсистеми, і який при вирішенні конкретної сукупності задач недоцільно далі розбивати на частини. Наприклад, в складі підсистем приводу виконавчих органів в багатьох випадках доцільно виділити такі основні елементи: електродвигуни, зубчаті колеса, вали, осі, підшипники,, виконавчий орган.

Під зовнішнім середовищем розуміють сукупність об'єктів технічного або природного характеру, що не входять до складу системи і володіють певними властивостями і параметрами, взаємодія з якими повинна враховуватися при вирішенні поставлених задач. Наприклад, для очисного вузькозахопного комбайна як зовнішнє середовище виступає людина-оператор, що безпосередньо керує вийманням вугільного пласта, шар породи, який вміщає вугільний пласт, вибійний конвеєр і мережа електропостачання.

При зміні масштабу задач, що ставляться, система, що вивчається може розглядатися як підсистема або елемент більш складної системи, а підсистема або навіть елемент – як система. Відповідно змінюється і сукупність об'єктів зовнішнього середовища.

На даний час існує багато різних підходів до захисту інформації, але системний підхід, гарантує цілісність і послідовність застосованих методів захисту інформації при проектуванні комплексних засобів захисту інформації. Дослідження проблеми захисту інформації базується на принципах системного підходу, які сформульовані як основні принципи захисних заходів від несанкціонованого доступу в автоматизовану систему (АС).

Головна відмінність сучасних концепцій в тому, що сьогодні не говорять про якийсь один універсальний засіб захисту, а мова йде про комплексні засоби захисту інформації (КЗЗІ), що включають:

- нормативно-правовий базис захисту інформації;
- засоби, способи і методи захисту;
- органи і виконавців.

Захист інформації є комплексом регулярно використовуваних засобів і методів, запобіжних заходів, що приймаються, і здійснюваних заходів з метою систематичного забезпечення необхідної надійності інформації, що генерується, зберігається і обробляється в автоматизованій системі, а також передається по каналах. Захист повинен носити системний характер, тобто для отримання якнайкращих результатів всі розрізнені види захисту інформації повинні бути об'єднані в одне ціле і функціонувати у складі єдиної системи, що є злагодженим механізмом взаємодіючих елементів, призначених для виконання завдань з забезпечення безпеки інформації . КЗЗІ призначений забезпечувати, з одного боку, функціонування надійних механізмів захисту, а з іншого - управління механізмами захисту інформації. У зв'язку з цим повинна передбачатися організація чіткої і відлагодженої системи управління захистом інформації та підготовка кваліфікованих фахівців

Для кожної конкретної інформаційно-телекомунікаційної системи (ІТС) склад, структура і вимоги до КЗЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи і умовами її експлуатації.

Класи автоматизованих систем:

1) **одномашинний однокористувальницький** комплекс, який обробляє інформацію однієї або декількох категорій конфіденційності;

2) **локалізований багатомашинний** багатокористувальницький комплекс, який обробляє інформацію різних категорій конфіденційності.

3) **розподілений багатомашинний** багатокористувальницький комплекс, який обробляє інформацію різних категорій конфіденційності.

У загальному випадку, послідовність і зміст науково-дослідної розробки КЗЗІ можна заздалегідь **розділити на 4 етапи**:

1) **Розробка технічного завдання**:
   - аналіз стану інформаційної системи;
   - розробка інформаційної моделі КЗЗІ;
   - аналіз уражень інформаційної системи;
   - визначення вимог до системи захисту.
2) **Визначення технічного рішення**:
   - опис технічного рішення;
   - визначення детального переліку устаткування, програмного забезпечення і змісту робіт;
   - визначення вартості.
3) **Реалізація КЗЗІ:**
   - побудова повного комплексу засобів захисту;
   - тестування КЗЗІ;
   - отримання експертного висновку (атестату);
   - експлуатація КЗЗІ;
   - підтримка актуальності КЗЗІ протягом життєвого циклу.

Даний алгоритм – це лише основа проектування. Кожен представлений етап відображає безліч рівнів в ході проектування залежно від структури АС – вимоги, що пред'являються до її системи захисту.

Однією з вимог забезпечення захисту інформації в АС є те, що обробка в АС конфіденційної інформації повинна здійснюватись з використанням захищеної технології, яка містить програмно-технічні засоби захисту і організаційні заходи, які забезпечують виконання загальних вимог з захисту інформації.

Загальні вимоги передбачають:

- **наявність переліку конфіденційної інформації**, яка підлягає автоматизованій обробці; у разі потреби можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів і іншими класифікаційними ознаками;

- **наявність певного (створеного) відповідального підрозділу**, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації (служба захисту в АС, СЗІ);

- **створення КСЗІ** (комплексної системи захисту інформації), яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, направлених на забезпечення захисту інформації під час функціонування АС;

- **розробку плану захисту інформації в АС**;

- **наявність атестату відповідності КСЗІ** в АС нормативним документам із захисту інформації;

- **можливість визначення засобами КСЗІ декількох ієрархічних рівнів** повноважень користувачів і декількох класифікаційних рівнів інформації;

- **обов'язковість реєстрації в АС** всіх користувачів і їх дій щодо конфіденційної інформації;

- **можливість надання користувачам** тільки за умови службової необхідності **санкціонованого і контрольованого доступу** до конфіденційної інформації, яка обробляється в АС;

- **заборона несанкціонованій і неконтрольованій модифікації** конфіденційної інформації в АС;

- **здійснення за допомогою СЗІ обліку вихідних даних**, отриманих під час рішення функціональної задачі, у формі віддрукованих документів, які містять конфіденційну інформацію, відповідно до керівних документів;

- **заборона несанкціонованого копіювання**, розмноження, розповсюдження конфіденційної інформації, в електронному вигляді;

- **забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням**, розмноженням, розповсюдженням конфіденційної інформації, в електронному вигляді;

- **можливість здійснення однозначної ідентифікації і аутентифікації** кожного зареєстрованого користувача;

- **забезпечення КСЗІ можливості своєчасного доступу** зареєстрованих користувачів АС до конфіденційної інформації.

Приведені вимоги є базовими і застосовуються при захисті інформації від НСД (несанкціонованого доступу) у всіх типах АС.

Умовно розділивши АС на найважливіші підсистеми забезпечення захисту інформації (мал. 1.2.1), можна перелічити також вимоги, що пред'являються для захисту комп'ютерної інформації від НСД в АС кожній окремій підсистемі.

Мал. 3.2.1 Підсистеми управління та забезпечення захисту інформації в автоматизованих системах

Підсистема управління доступом повинна задовольняти наступним вимогам:

- ідентифікувати і перевіряти достовірність суб'єктів доступу при вході в систему. Причому це повинно здійснюватися по ідентифікатору (коду) і паролю умовно-постійної дії довжиною не менше шести літеро-цифрових символів;

- ідентифікувати термінали, ЕОМ, вузли комп'ютерної мережі, канали зв'язку, зовнішні пристрої ЕОМ за їх логічними адресами (номерами);

- за іменами ідентифікувати програми, томи, каталоги, файли, записи і поля записів;

- здійснювати контроль доступу суб'єктів до ресурсів, що захищаються, відповідно до матриці доступу;

Підсистема реєстрації і обліку повинна:

- реєструвати вхід (вихід) суб'єктів доступу в систему (з системи), або реєструвати завантаження і ініціалізацію операційної системи і її програмної зупинки. При цьому в параметрах реєстрації указуються:

а) дата і час входу (виходу) суб'єкта доступу в систему (з системи) або завантаження (зупинки) системи;

б) результат спроби входу — успішна або неуспішна (при НСД);

в) ідентифікатор (код або прізвище) суб'єкта, пред'явлений при спробі доступу;

г) код або пароль, пред'явлений при неуспішній спробі.

- реєстрація виходу з системи або зупинки не проводиться в моменту апаратурного відключення АС;

- реєструвати видачу печатних (графічних) документів на «тверду» копію. При цьому в параметрах реєстрації указуються:

а) дата і час видачі (звернення до підсистеми виводу);

б) короткий зміст документа (найменування, вигляд, код, шифр) і рівень його конфіденційності;

в) специфікація пристрою видачі (логічне ім'я зовнішнього пристрою);

г) ідентифікатор суб'єкта доступу, що запитав документ;

- реєструвати запуск (завершення) програм і процесів (завдань, задач), призначених для обробки файлів, що захищаються. При цьому в параметрах реєстрації указується:

а) дата і час запуску;

б) ім'я (ідентифікатор) програми (процесу, завдання);

в) ідентифікатор суб'єкта доступу, що запитав програму (процес, завдання);

г) результат запуску (успішний, неуспішний - несанкціонований).

- реєструвати спроби доступу програмних засобів (програм, процесів, завдань, задач) до файлів, що захищаються. У параметрах реєстрації указується:

а) дата і час спроби доступу до файлу, що захищається, з вказівкою її результату (успішна, неуспішна - несанкціонована);

б) ідентифікатор суб'єкта доступу;

в) специфікація файлу, що захищається.

- реєструвати спроби доступу програмних засобів до додаткових об'єктів доступу, що захищаються (терміналам ЕОМ, вузлам мережі ЕОМ, лініям (каналам) зв'язку, зовнішнім пристроям ЕОМ, програмам, томам, каталогам, файлам, записам, полям записів). При цьому в параметрах реєстрації указується:

а) дата і час спроби доступу до файлу, що захищається, з вказівкою її результату: успішна, неуспішна, несанкціонована;

б) ідентифікатор суб'єкту доступу;

в) специфікація об'єкту, що захищається [логічне ім'я (номер)].

- проводити облік всіх носіїв інформації, що захищаються, за допомогою їх маркування із занесенням облікових даних в журнал (облікову картку);

- реєструвати видачу (приймання) носіїв, що захищаються;

- здійснювати очищення (обнулення, знеособлення) областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів, що звільняються. При цьому очищення повинне проводитися одноразовим, довільним записом в область пам'яті, що звільняється, раніше використану для зберігання даних, що захищаються (файлів).

Підсистема забезпечення цілісності повинна:

- забезпечувати цілісність програмних засобів системи захисту інформації від НСД

(СЗІ НСД), оброблюваної інформації, а також незмінність програмного середовища. При цьому:

а) цілісність СЗІ НСД перевіряється при завантаженні системи по контрольних сумах компонент СЗІ;

б) цілісність програмного середовища забезпечується використанням трансляторів з мови високого рівня і відсутністю засобів модифікації об'єктного коду програм в процесі обробки і зберігання інформації, що захищається;

- здійснювати фізичну охорону пристроїв і носіїв інформації. При цьому повинні передбачатися контроль доступу в приміщення АС сторонніх осіб, а також наявність надійних перешкод для несанкціонованого проникнення в приміщення АС і сховище носіїв інформації, особливо в неробочий час;

- проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища і персоналу АС за допомогою тест-програм, що імітують спроби НСД;

- мати в наявності засоби відновлення СЗІ НСД. При цьому передбачається ведення двох копій програмних засобів СЗІ НСД, а також їх періодичне оновлення і контроль працездатності.

Провівши оцінку необхідності захисту інформації від НСД, стає питання про подальший напрям проектування системи захисту інформації. Адже саме по отриманих результатах можна судити про складність проектованої системи. Маючи такі результати, необхідно оцінити вірогідність погроз, що проявляються, на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів. Спираючись на вимоги із захисту інформації від НСД, можна привести основні принципи захисних заходів від НСД в АС.

Принцип перший – обґрунтованість доступу. Даний принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню «форму допуску» для отримання інформації потрібного ним рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. У сфері автоматизованої обробки інформації як користувачі можуть виступати активні програми і процеси, а також носії інформації різного ступеня складності. Тоді система доступу припускає визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій.

Принцип другий – достатня глибина контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип третій – розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

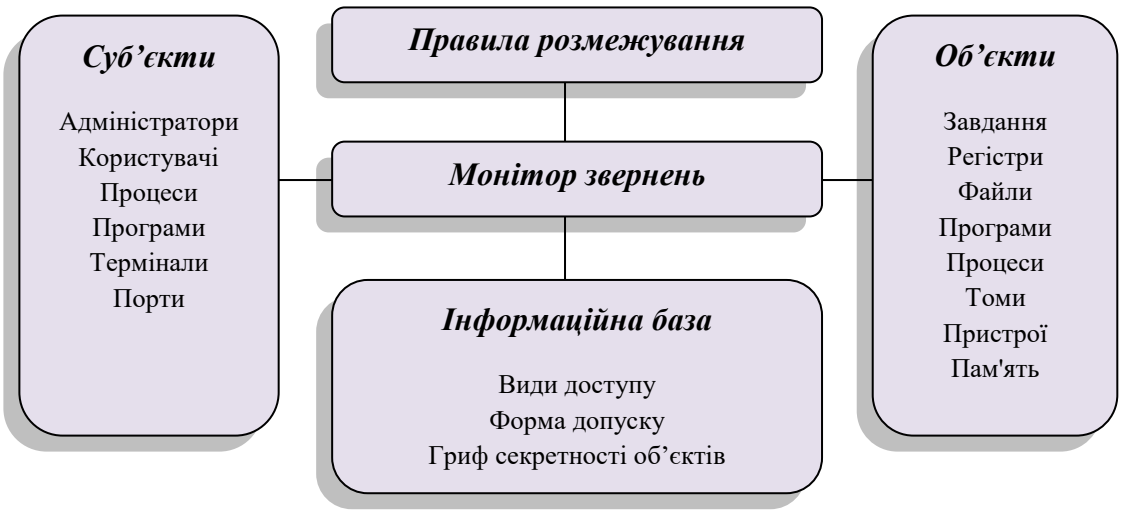
Принцип четвертий – чистота повторно використовуваних ресурсів. Даний принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип п’ятий – персональна відповідальність. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, а також за випадкові або умисні дії, які можуть привести до несанкціонованого ознайомлення з конфіденційною

інформацією, її спотворенню або знищенню, або виключенню можливості доступу до такої інформації законних користувачів.

Принцип шостий – цілісності засобів захисту. Даний принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі.

Реалізація перерахованих принципів здійснюється за допомогою «монітора звернень», контролюючого будь-які запити до даних або програм з боку користувачів (або їх програм) з встановлених для них видах доступу до цих даних і програм. Схематично такий монітор можна представити у вигляді, показаному на мал. 1.2.2.



Мал. 3.2.2 Структура монітора звернень

Практичне створення монітора звернень, як видно з приведеного малюнка, припускає розробку конкретних правил розмежування доступу у вигляді моделі захисту інформації.

Спроектувавши модель захисту інформації, необхідно виконати аналіз ефективності захисних заходів. Головна функція системи безпеки – протидія загрозам за допомогою людей і техніки. Кожна загроза спричиняє за собою збиток, а протидія покликана понизити його величину, в ідеалі – повністю. Вдається це далеко не завжди. Здатність системи безпеки виконувати свою головну функцію завжди повинна оцінюватися кількісно.

Основні виводи і рекомендації очевидні. Одночасна протидія буде достатньою для високоефективного захисту від загрози, якщо реакція на неї буде швидкою. Це завдання цілком реальне для об'єктів великого бізнесу. Кооперативні ж форми протидії в умовах повільної реакції на погрози не принесуть ефекту, якщо відсутні засоби затримки і блокування погроз. Кажучи про тактичні питання системи безпеки бізнесу в частині технічних каналів зв'язку, перш за все мають на увазі швидкість її реакції, надійність рішень, блокування розвитку погроз і їх ліквідацію. Особливо важливо забезпечити жорсткі вимоги до надійності всіх систем захисту, які залежать від часу їх функціонування і періодичності оновлення ресурсів. Якщо цей час перевищує 5 років, то вимога надійності реалізується декількома способами, серед яких – резервування рішень, багаторубіжність захисту, автоматизація первинних рішень, централізоване управління ресурсами в кризових ситуаціях і тому подібне Перш ніж визначитися в питаннях тактики, треба пам'ятати, що вони повинні відповідати стратегії і спиратися на точний кількісний аналіз. Для об'єктів

середнього і малого бізнесу такий аналіз цілком реальний навіть без засобів автоматизації. Проте, необхідно привернути фахівців і експертів, які б проаналізували обстановку і властивості об’єкту захисту, розробили модель погроз, вивчили ринок існуючих засобів і методів. Ці дані і допомогли б оцінити саму систему і при необхідності модернізувати її.

3.3 ОСНОВНІ ЕТАПИ ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ.

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних і інженерно-технічних заходів, які направлені на забезпечення захисту інформації від розголошування, витоку і несанкціонованого доступу.

Об'єктами захисту КСЗІ є інформація, в будь-якому її вигляді і формі видображення.

У побудові КСЗІ можна виділити наступні етапи:

1. Підготовка організаційно-розпорядливої документації.
2. Обстеження інформаційної інфраструктури Замовника.
3. Розробка «Плану захисту інформації».
4. Розробка «Технічного завдання на створення КСЗІ».
5. Розробка «Технічного проекту на створення КСЗІ».
6. Приведення інформаційної інфраструктури Замовника у відповідність з «Технічним проектом на створення КСЗІ».
7. Розробка «Експлуатаційної документації на КСЗІ».
8. Впровадження КСЗІ.
9. Випробування КСЗІ.
10. Проведення державної експертизи КСЗІ і здобуття «Атестата відповідності».
11. Підтримка і обслуговування КСЗІ.

У побудові КСЗІ беруть участь наступні сторони: Виконавець і Замовник, які связанни безпосередньо з кожним етапом розробки. Також потрібна участь третьої незалежної сторони - Організатора експертизи при проведенні державної експертизи. Етапи 4 (розробка ТЗ) та 10 (держекспертиза) потребують залучення фахівців уповноваженого Контролюючого органу. Виконавець і Замовник повинні скласти договір, в якому детально описати порядок, терміни і вартість робіт по створенню КСЗІ. При складанні договору треба приділити увагу відповідності змісту статей договору вимогам чинного законодавства, правам та обов’язкам сторін, можливим форс мажорним обставинам та іншим розділам. Зазвичай до складання договору долучають юристів з досвідом роботи в сфері ЗІ.

Насамперед проводиться дослідження і аналіз документів, підприємства і приміщення Замовника.

1. **Підготовка організаційно-розпорядливої документації**

На цьому етапі фахівці Виконавця проводять аналіз організаційно-розпорядливих документів Замовника і нормативно-правових документів в області захисту інформації, що впливають на діяльність Замовника.

До організаційно-розпорядливих документів зазвичай відносяться: організаційна структура, штатний розклад, положення про відділи і посадові інструкції співробітників, пов'язаних з експлуатацією ІТС, документи, що регламентують доступ до ІТС і так далі. До нормативно-правових документів в області захисту інформації відносяться Закони України, постанови Кабінету Міністрів України, накази ДССЗІУ (Держспецзв’язку) , роботи з інформацією, що встановлюють правила. За результатами виконання цього етапу Виконавець готує проекти документів, які визначають організаційну складову КСЗІ (проект

наказу про створення КСЗІ, проект положення про службу захисту інформації, проекти посадових інструкцій і процедур та ін.), які затверджуються Замовником.

2. Обстеження інформаційної інфраструктури Замовника

На цьому етапі фахівці Виконавця проводять обстеження (аудит) ІТС Замовника. Аналізується архітектура системи, її топологія і складові елементи. Визначаються типи користувачів системи, типізується інформація, що обробляється в ІТС. За результатами виконання етапу Виконавець розробляє наступні документи: - акт обстеження ІТС (містить опис, принципи побудови і архітектуру ІТС); - перелік об'єктів ІТС що підлягають захисту, які затверджуються Замовником.

Після закінчення обстеження, спираючись на дані отримані при цьому, можна приступити до розробки.

3. Розробка "Плану захисту інформації"

За результатами виконання другого етапу, а саме, грунтуючись на переліку об'єктів ІТС, що підлягають захисту, Виконавець розробляє пакет документів

"План захисту інформації" :

- документ "Модель загроз інформації";
- документи "Завдання на створення КСЗІ" та «Політику Безпеки»,які затверджуються Замовником**.**

4. Розробка "Технічного завдання на створення КСЗІ"

На цьому етапі фахівці Виконавця розробляють і погоджують із Замовником документ "Технічне завдання на створення КСЗІ", який визначає усі основні вимоги до КСЗІ і можливі шляхи реалізації її складових елементів. Після узгодження "Технічного завдання на створення КСЗІ" із Замовником, документ узгоджується з Контролюючим органом.

5. Розробка "Технічного проекту на створення КСЗІ"

Після узгодження "Технічного завдання на створення КСЗІ" з Контролюючим органом Виконавець розробляє пакет документів "Технічний проект на створення КСЗІ". "Технічний проект на створення КСЗІ" є комплектом документів, в який входить частина документів розроблених на попередніх етапах і ряд нових документів, в яких описано, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься КСЗІ.

6. Приведення інформаційної інфраструктури Замовника у відповідність з "Технічним проектом на створення КСЗІ"

Особливістю цього етапу є те, що на момент ухвалення рішення про створення КСЗИ вартість цього етапу є невідомою як для Замовника, так і для Виконавця. Також, зважаючи на великий можливий спектр виконання робіт, на цьому етапі існує велика вірогідність підключення до його виконання Підрядників. На цьому етапі можуть виконуватися монтажні, будівельні, пуско-налагоджувальні роботи, роботи, пов'язані з установкою необхідних технічних або криптографічних засобів захисту інформації, засобів фізичного захисту елементів ІТС (встановлюється необхідне устаткування і програмне забезпечення, засоби контролю доступу, охоронна і пожежна сигналізації) і таке інше.

7. Розробка "Експлуатаційної документації на КСЗИ"

На цьому етапі Виконавець КСЗИ створює пакет документів "Експлуатаційна документація на КСЗИ", який включає: - інструкції експлуатації КСЗИ і її елементів; - процедури регламентного обслуговування КСЗИ; - правила і положення по проведенню тестування і аналізу роботи КСЗИ. Після закінчення розробки, при її твердженні ми можемо перейти безпосередньо до побудови системи захисту інформації.

8. Впровадження КСЗИ

На цьому етапі Виконавець (чи Підрядник під авторським наглядом Виконавця) проводить усі пуско-налагоджувальні роботи, навчає і інструктує персонал Замовника правилам і режимам експлуатації КСЗИ. Після реалізації цього етапу впроваджена КСЗИ готова до подальшого випробування.

9. Випробування КСЗИ

Замовник за участю та підтримці Виконавця проводить попередні випробування КСЗІ, з метою підтвердження результативності її роботи і відповідності положенням та вимогам, визначеним в "Технічному завданні на створення КСЗІ". В процесі випробувань виконуються тестові завдання і контролюються отримані результати, які і є індикатором працездатності спроектованої КСЗІ. По результату випробування КСЗИ робиться висновок о відповідності та можливості представлення КСЗИ на державну експертизу, або необхідності вдосконалення КСЗІ.

10. Проведення експертизи КСЗИ і отримання "Атестата відповідності"

На цьому етапі Контролюючий орган призначає Організатора державної експертизи, який проводить незалежний аналіз (експертизу) відповідності КСЗІ вимогам, викладеним в документі "Технічне завдання на створення КСЗІ", нормативній документації по технічному захисту інформації, а також визначає можливість введення КСЗИІ в промислову експлуатацію. Залучення незалежного експерта (Організатора експертизи) до проведення державної експертизи підвищує об'єктивність оцінки проведених робіт і зменшує ризик порушень і зловживань у сфері захисту інформації. Будь-яка організація, що входить в Реєстр Організаторів експертиз у сфері ТЗИ, може проводити експертизи знову створених КСЗИ або КСЗИ, "Атестат відповідності" на які необхідно подовжувати. Реєстр Організаторів експертиз веде Контролюючий орган.

Контролюючий орган за результатами проведення державної експертизи КСЗИ видає документ "Атестат відповідності", що підтверджує якість і надійність побудованої КСЗИ.

"Атестат відповідності" є обов'язковим для введення КСЗИ в промислову експлуатацію.

Після успішного запуску і функціонування КСЗИ залишається лише підтримувати її працездатність і необхідний рівень захисту.

11. Підтримка і обслуговування КСЗИ

На цьому етапі Виконавець може проводити авторський нагляд і надавати консультаційну допомогу Замовникові в експлуатації КСЗИ, аналізі її роботи, виробленні рекомендацій, і, при необхідності, її модернізації і розвитку.

Слід зазначити, що цей етап дуже важливий для збору статистичної інформації про роботу КСЗІ, аналізу реалізованих сценаріїв атак на ІТС з метою подальшого вдосконалення КСЗІ.

4 ПРИНЦИПИ РОБОТИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ.

4.1 СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД СПОСТЕРЕЖЕННЯ.

Захист інформації від спостереження в оптичному діапазоні грунтується на загальних принципах, але з урахуванням особливостей даного каналу. Для захисту інформації про об'єкт необхідно зменшувати ступінь контрастності об'єкта і фону, знижувати яскравість об'єкта, не допускати спостерігача близько до об'єкта.

Заходи, спрямовані на зменшення величини контраст/фон називаються маскуванням. Застосовуються наступні способи маскування:

• використання маскувальних властивостей місцевості (нерівностей ландшафту, складок місцевості, пагорбів, стовбурів і крон дерев і т.п.);

• маскувальна обробка місцевості: посів трави, створення огорож з живою рослинністю, хімічна обробка ділянок місцевості і т.п.);

• маскувальне фарбування (нанесення на поверхню об'єкта фарб, підібраних за кольором і яскравістю, близьких до фону);

• застосування штучних масок (навіси – від спостереження зверху, вертикальні стінки – від спостереження з поверхні землі, похилі площини – для приховування тіней об'ємних об'єктів);

• нанесення на об'єкт повітряної піни (світлонепроникні кольорові піни забезпечують ефективне маскування об'єктів до кількох годин).

Енергетичне приховування демаскуючих ознак об'єктів досягається шляхом зменшення яскравості об'єкта і фону нижче чутливості ока людини або технічного фотоприймача, а також їх засліплення. Найбільш природним способом такого приховування є проведення заходів, що вимагають захисту інформації про них, вночі. Яскравість об'єктів, що мають штучні джерела світла, знижується шляхом їх відключення, екранування світлонепроникними шторами і щитами. Енергетичне приховування об'єктів, які спостерігаються у відбитому світлі, забезпечують штучні маски, а також природні та штучні аерозолі (піни) в середовищі поширення.

На яскравість об'єкта з власним джерелом тепла (отже, на його контраст з фоном в інфрачервоному діапазоні) впливає температура об'єкта. Для його інформаційного захисту застосовуються різні теплоізолюючі екрани (брезент, пісок та ін.). Добрими теплоізоляційними властивостями володіють повітряні піни.

4.2 СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПІДСЛУХОВУВАННЯ.

Способи і засоби протидії підслуховуванню спрямовані, перш за все, на запобігання витоку інформації в акустичному (гідроакустичному, сейсмічному) каналах.

Слід пам'ятати, що для підвищення дальності підслуховування широко застосовуються комбіновані пристрої, що поєднують акустичні, радіоелектронні та оптичні (лазерні сканери) прилади. Тому захист інформації від підслуховування включає способи і засоби блокування будь-яких каналів витоку акустичної інформації.

Відповідно до загальних принципів для захисту від підслуховування застосовують способи:

1) інформаційне приховування, що передбачає:

• технічне закриття і шифрування мовної інформації в функціональних каналах зв'язку;

• дезінформування;

2) енергетичне приховування:

• шляхом ізоляції акустичного сигналу;

• поглинання акустичної хвилі;

• глушіння акустичних сигналів;

• зашумлення приміщення (або середовища поширення звукових хвиль) іншими звуками (шумами, перешкодами);

3) виявлення та вилучення заставних пристроїв.

Виявлення електронних засобів підслуховування – завдання досить складне, тому що включає фізичний і електронний огляд приміщень. Оперативні працівники служби безпеки (СБ) повинні постійно орієнтувати свою внутрішню агентуру на виявлення підслуховуючих пристроїв. В цьому плані метою діяльності контррозвідки СБ є:

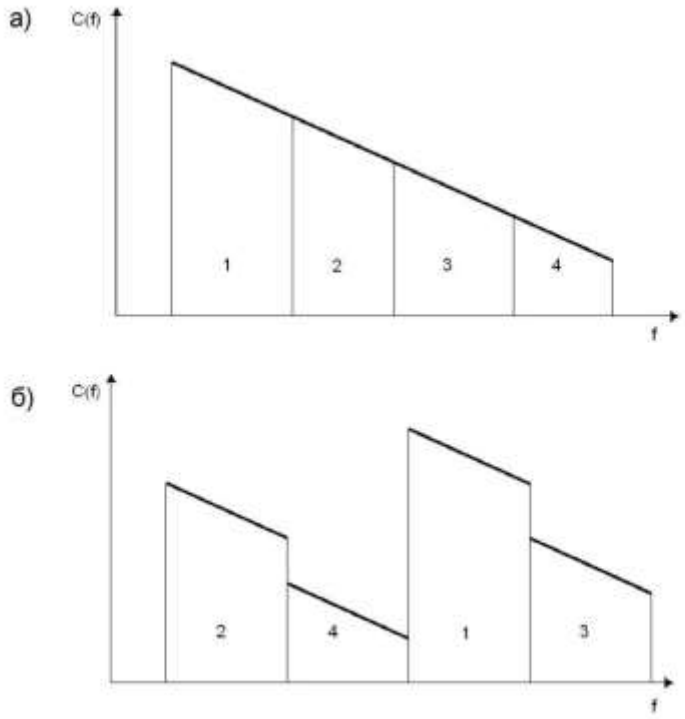
• пошук і відключення підслуховуючої апаратури;

• підкидання через апаратуру неправдивої інформації;

• збір доказів для порушення кримінальної справи проти суб'єктів розвідки противника.

Мовна інформація, що передається по каналах зв'язку захищається від прослуховування з використанням методів аналогового скремблювання і дискретизації мови з подальшим шифруванням. Під ***скремблюванням*** розуміється зміна характеристик мовного сигналу таким чином, що отриманий модульований сигнал, володіючи властивостями нерозбірливості і невпізнання, займає таку ж смугу частот спектра, як і вихідний відкритий. Аналогові скремблери перетворюють вихідний мовний сигнал шляхом зміни його частотних і часових характеристик (мал. 1.2.1).

Спосіб частотних перестановок полягає в поділі спектра вихідного сигналу на піддіапазони рівної ширини з наступним перемішуванням відповідно до деякого алгоритму. При часовому скремблюванні кадр мовної інформації перед відправленням запам'ятовується і розбивається на сегменти однаковою тривалості. Сегменти перемішуються аналогічно частотним перестановкам.



Мал. 1.2.1 Частотна перестановка:

а - вихідний сигнал; б – перетворений

Дискретизація мовної інформації з подальшим шифруванням забезпечує найбільший ступінь захисту інформації у каналах зв'язку. В процесі дискретизації мовна інформації представляється у цифровій формі. У такому вигляді вона перетворюється у відповідності до певного алгоритму шифрування і передається по каналах зв'язку.

4.3 СПОСОБИ І ПРИНЦИПИ РОБОТИ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПЕРЕХОПЛЕННЯ.

Призначення і характеристики закладного пристрою проводяться в результаті аналізу технічних і конструктивних рішень. Але вже зовнішній вигляд закладки та способи її застосування дозволяють приблизно визначити приналежність агента (установника закладки) до спецслужби, конкурента або злочинного угруповання.

Звичайними ознаками мікрофонної закладки є:

• тонкий провід, прокладений від малогабаритного мікрофона закладки в інше приміщення;

• наявність в кожусі закладки одного або декількох отворів.

Ознаками некамуфльованої радіозакладки є:

• радіовипромінювання (яке модулює радіосигнали від акустичних сигналів, що циркулюють в приміщенні);

• зовнішній вигляд – мініатюрний предмет незрозумілого призначення, що має форму плоского паралелепіпеда або циліндра;

• одне або кілька отворів малого діаметра в кожусі;

• наявність (не завжди) невеликого відрізка проводу, що виходить з кожуха;

• присутність напівпровідникових елементів, що виявляються при опроміненні обстежуваних предметів нелінійним радіолокатором;

• наявність в пристрої металевих провідників або інших деталей, що виявляються металодетектором або рентгенівськими променями.

Камуфльовані радіозакладки за зовнішнім виглядом не відрізняються від об'єктів імітації, особливо якщо закладка встановлена в корпусі побутового предмета без зміни його зовнішнього вигляду. Так, на поверхні закладки у вигляді конденсатора є заводські реквізити (тип, величина ємності, номер серії і т.п.). Виявити такі закладки можна лише шляхом розбирання або просвічування їх рентгенівськими променями.

У той же час закладки, камуфльовані під малогабаритні предмети, знижують функціональні можливості цих предметів. Тому ознаки обмеження функцій засобів оргтехніки, електропобутових приладів і т.п. служать ознаками установки в них закладних пристроїв. Так, у кульковій авторучці закладка займає половину її довжини, в результаті чого різко коротшає стрижень для письма і скорочується час нормальної роботи ручки. У такій ручці не можна замінити стрижень, тому що розбірні частини склеєні. Неможливо застосовувати для освітлення електролампочки типу РК-520 з встановленою в цоколь закладкою. Однак електролампочки типу РК-560-S позбавлені цього недоліку. Візуально виявити в них радіозакладки не можна.

Засобами боротьби з радіозакладками є, по-перше, прилади радіоконтролю приміщення, які призначені для виявлення закладних пристроїв, що випромінюють радіохвилі під час їх пошуку. На ринку переважають радіовипромінювальні закладки, отже, застосовуються різноманітні засоби радіоконтролю приміщень: починаючи від найпростіших індикаторів електромагнітного поля «Сигнал-5» (мал. 1.3.1) і закінчуючи складними автоматизованими комплексами «Філін».

По-друге, це прилади, що реагують не стільки на радіовипромінювання, а на якісь інші демаскуючі ознаки. Дистанційно керовані радіозакладки, а також закладки, що передають інформацію по проводам, апаратура радіоконтролю не може виявити. Для їх пошуку використовують прилади, що реагують на демаскуючі ознаки матеріалів конструкції і елементів схеми закладного пристрою, а також на сигнали, що розповсюджуються по дротах – нелінійний локатор «Коршун».

По-третє, це засоби «подавлення» закладних пристроїв, які забезпечують енергетичне приховування їх сигналів, порушення працездатності або їх фізичне руйнування – це генератори перешкод «Соната» і аналоги. Для ефективного придушення сигналу закладки рівень перешкоди в смузі спектра сигналу повинен в кілька разів перевищувати рівень сигналу. Подавлення електричних і радіосигналів забезпечує превентивний захист інформації без попереднього виявлення і локалізації закладних пристроїв.

Мал. 1.3.1 Індикатор поля «Сигнал-5»

Можливі 3 способи подавлення сигналів:

- зниження співвідношення сигнал / шум до безпечних для інформації значень шляхом просторового і лінійного зашумлення;
- вплив на закладні пристрої електричними сигналами, такими, що порушують задані режими роботи цих пристроїв;
- вплив на закладні пристрої, що викликають їх руйнування.

Захист ліній зв'язку, що виходять за межі приміщень, що охороняються або за межі всього об'єкта, являє собою дуже серйозну проблему, так як ці лінії найчастіше виявляються безконтрольними і до них можуть підключатися різні засоби знімання інформації.

Екранування інформаційних ліній зв'язку між пристроями технічних засобів передачі інформації (ТЗПІ) здійснюють головним чином, захист ліній від наведень, створюваних лініями зв'язку в навколишньому просторі. Найбільш економічним способом екранування є групове розміщення інформаційних кабелів в екранувальному ізольованому коробі. Коли такий короб відсутній, доводиться екранувати окремі лінії зв'язку.

Для захисту ліній зв'язку від наведень необхідно розмістити лінію в екранованому обплетенні або фользі, заземлену в одному місці, щоб уникнути протікання по екрану струмів, викликаних нееквіпотенціальностю точок заземлення. Для захисту ліній зв'язку від наведень необхідно мінімізувати площу контуру, утвореного прямим і зворотним проводом лінії. Якщо лінія є одиночним проводом, а поворотний струм тече по деякій заземляючій поверхні, то необхідно максимально наблизити провід до поверхні. Якщо лінія утворена двома проводами, має велику протяжність, то її необхідно скрутити, утворивши біфіляри (кручену пару). Лінії, виконані з екранованого проводу або коаксіального кабелю, по обплетенню якого протікає поворотний струм, також повинні відповідати вимогам мінімізації площі контуру лінії.

Найкращий захист одночасно від змін напруженості електричного і магнітного полів забезпечують інформаційні лінії зв'язку типу екранованого біфіляра, тріфіляра (трьох скручених разом проводів, з яких один використовується в якості електричного екрана), тріаксіального кабелю (ізольованого коаксіального кабелю, поміщеного в електричний екран), екранованого плоского кабелю (плоского багатопровідного кабелю, покритого з однієї або з обох сторін мідною фольгою).

Для зменшення магнітного і електричного зв'язку між проводниками необхідно зробити наступне:

• зменшити напругу джерела сигналу або струму;

• зменшити площу петлі;

• максимально рознести ланцюги;

• передавати сигнали постійним струмом або на низьких частотах;

• використовувати провід в магнітному екрані з високою проникністю;

• включити в ланцюг диференційний підсилювач.

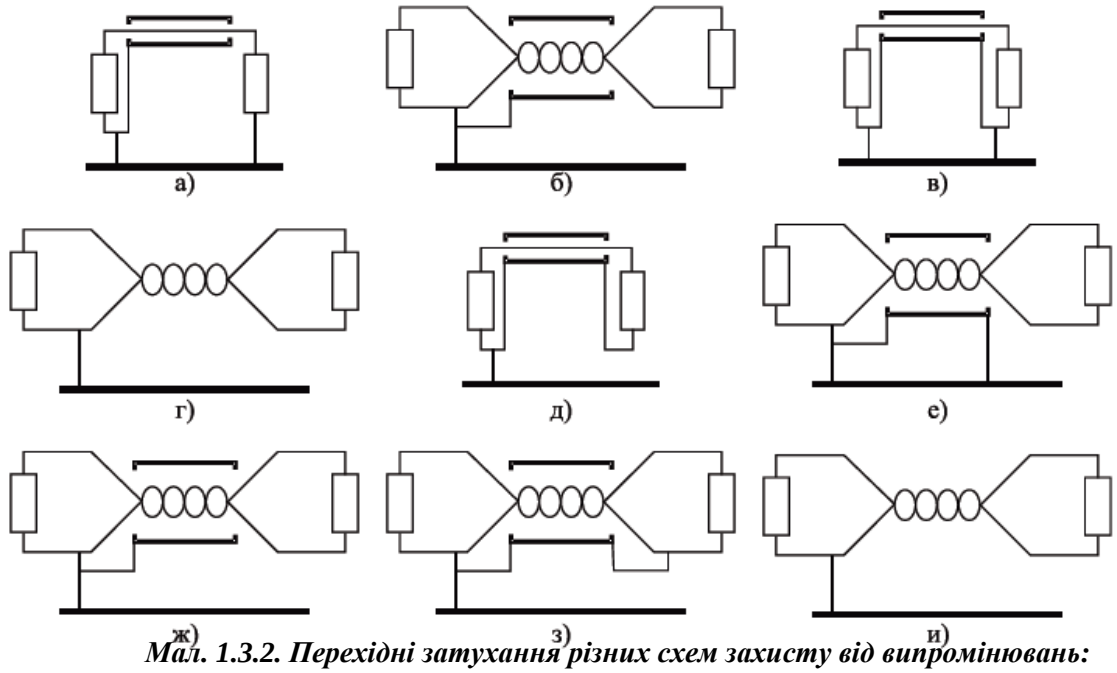
Розглянемо кілька схем захисту від випромінювання (мал. 1.3.2). Ланцюг, показаний на мал. 1.3.2, а, має велику петлю, утворену "прямим" проводом і "землею". Цей ланцюг піддається, насамперед, магнітному впливу. Екран заземлений на одному кінці і не захищає від магнітного впливу. Перехідне загасання для цієї схеми приймемо рівним 0 дБ для порівняння з загасанням, забезпечуваним схемами, представленими на мал. 1.3.2, б-і.

Схема, представлена на мал. 1.3.2, б, практично не зменшує магнітний зв'язок, оскільки зворотний провід заземлений з обох кінців, і в цьому сенсі вона аналогічна попередній схемі (мал. 1.3.2, а). Ступінь поліпшення порівнянна з похибкою розрахунку (вимірювання) і становить 2 -4 дБ. Наступна схема (мал. 1.3.2, в) відрізняється від першої схеми (мал. 1.3.2, а) наявністю зворотного проводу (коаксіального екрану), проте екранування магнітного поля погіршено, так як ланцюг заземлений на обох кінцях, в результаті чого з "землею" утворюється петля більшої площі. Схема, представлена на мал. 1.3.2, г, дозволяє істотно підвищити захищеність ланцюга (49дБ) завдяки скрутці проводів. У цьому випадку (у порівнянні зі схемою, наведеною на мал. 1.3.2, б) петлі немає, оскільки правий кінець ланцюга не заземлений. Подальше підвищення захищеності досягається застосуванням схеми, представленої на мал. 1.3.2, д, коаксіальний ланцюг якої забезпечує краще магнітне екранування, ніж скручена пара (мал. 1.3.2, г). Площа петлі схеми (мал. 1.3.2, д), не більше, ніж в схемі на мал. 1.3.2, г, так як продольна вісь екрану коаксіального кабелю збігається з його центральним проводом. Схема, наведена мал. 1.3.2, е, дозволяє підвищити захищеність ланцюга завдяки тому, що скручена пара заземлена лише на одному кінці. Наступна схема (мал. 1.3.2, ж), має ту саму захищеність: ефект заземлення екрана на одному і тому ж кінці такий же, що і при заземленні на обох кінцях, оскільки довжина ланцюга і екрану істотно менше робочої довжини хвилі. Причини покращення захищеності схеми, представленої на мал. 1.3.2, з, в порівнянні зі схемою, представленою на мал. 1.3.2, ж, фізично пояснити важко. Можливо, причиною є зменшення площі еквівалентної петлі. Більш зрозуміла схема зі скручуванням, показана на мал. 1.3.2, і, яка дозволяє додатково зменшити магнітний зв'язок. Крім того, при цьому зменшується і електричний зв'язок.

Канали витоку інформації з обмеженим доступом, що виникають внаслідок наведень в технічних засобах передачі інформації і лініях, що їх сполучають, а також в проводах, кабелях, металоконструкціях та інших провідниках, що мають вихід за межі контрольованої зони, можуть виникати при спільному розміщенні (в одному або суміжних приміщеннях) ТЗПІ і допоміжних технічних засобів і систем, а саме:

• при розміщенні сторонніх провідників в зоні дії інформаційних наведень від ТЗПІ;

• при спільному прокладанні інформаційних ліній ТЗПІ з лініями допоміжних технічних засобів на порівняно великій довжині паралельного пробігу (невиконання вимог по розносу між лініями ТЗПІ і допоміжних технічних засобів).



Мал. 1.3.2. Перехідні затухання різних схем захисту від випромінювань:

а - 0 дБ; б - 2 дБ; в - 5 дБ; г - 49 дБ; д - 57 дБ; е - 64 дБ; *ж - 64 дБ; з - 71 дБ; і - 79 дБ*

Виявлення наведених сигналів проводиться на кордоні контрольованої зони або на комутаційних пристроях, в кросах або розподільних шафах, розташованих в межах контрольованої зони об'єкта. Вимірювання напруги сигналів, наведених від технічних засобів, мовної інформації виконується при подачі на вхід ТЗПІ або в їх з'єднувальні лінії контрольного сигналу синусоїдальної форми з частотою F = 1000 Гц.

Залежно від категорії оброблюваної ТЗПІ (переданої по спеціальних лініях) інформації ефективність захисту ліній (схильних до впливу), що виходять за межі контрольованої зони, визначається шляхом порівняння вимірюваних значень з нормами. Норми визначаються виходячи з амплітуди подаваного контрольного сигналу. Якщо виконується умова $U_{конт} \leq U_{н}$, то можна зробити висновок, що досліджувана лінія достатньо захищена від витоку мовної інформації за рахунок наведень. Якщо зазначена умова не виконується, то необхідно вжити додаткових заходів захисту (наприклад, зашумить досліджувані лінії).

Для контролю стану лінії зв'язку використовуються пасивні і активні індикатори. Вони дозволяють визначити як паралельне підключення до лінії, так і послідовне.

5. ОРГАНІЗАЦІЙНІ ЗАХОДИ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ДЕРЖАВНИХ СТРУКТУРАХ.

Сучасна технологія забезпечення безпеки зв'язку рекомендує всю роботу по захисту інформації з врахуванням розглянутих стратегій протидіючої сторони проводити по наступних напрямках:

· вдосконалення організаційних і огранізаційно-технічних заходів;

· блокування несанкціонованого доступу до оброблюваної інформації, що передається;

· блокування несанкціонованого отримання інформації з допомогою технічних засобів.

На сьогодні успішно розвиваються не тільки методи і засоби закриття інформації, але і проводиться активна робота протилежного напрямку, спрямована на несанкціонований доступ і перехоплення цінної комерційної інформації. Тому користувачів технічних засобів забезпечення безпеки зв'язку в першу чергу цікавлять практичні рекомендації по заходах захисту інформації і протидії несанкціонованому доступу. Під ***організаційними заходами*** захисту розуміють заходи загального характеру, які обмежують доступ до цінної інформації стороннім особам, незалежно від особливостей методів передачі і каналів витоку інформації. Будь-яка робота по забезпеченню безпеки зв'язку в каналах телекомунікацій повинна починатися з таких організаційних заходів захисту:

1. Встановлення персональної відповідальності за забезпеченням захисту інформації.
2. Обмеження доступу в приміщення, де проходить підготовка і обробка інформації.
3. Доступ до обробки, збереження і передачі конфіденційної інформації тільки перевіреним посадовим особам.
4. Призначення конкретних зразків технічних засобів для обробки цінної інформації і подальша робота тільки на них.
5. Збереження магнітних носіїв, жорстких копій і реєстраційних матеріалів в закритих міцних шафах (бажано в сейфах).
6. Виключення перегляду сторонніми особами змісту оброблюваної інформації за рахунок відповідного встановлення дисплея, клавіатури, принтера і т.п.
7. Постійний контроль пристроїв виводу цінної інформації на фізичні носії.
8. Збереження цінної інформації на зовнішніх носіях тільки в засекреченому вигляді.
9. Використання криптографічного закриття при передачі по каналах зв'язку цінної інформації.
10. Знищення фізичних носіїв або матеріалів, що можуть містити фрагменти цінної інформації.
11. Заборона ведення переговорів про безпосередній зміст цінної інформації особам, які зайняті її обробкою.
12. Чітка організація робіт і контроль виконання.

1.1 ТЕХНІЧНІ ЗАХОДИ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ДЕРЖАВНИХ СТРУКТУРАХ.

Інженерно-технічні методи і засоби захисту АС реалізуються в рамках інженерно-технічного захисту об'єктів інформатизації. Основними завданнями цього захисту є:

• створення фізичних перешкод на шляху зловмисників з метою запобігання несанкціонованого доступу на об'єкт і до АС;

• запобігання спробам отримання інформації зловмисниками різними засобами технічної розвідки (за рахунок ПЕМВН, акустики та ін.);

• оповіщення служб захисту про спроби проникнення до комп'ютерних систем, що захищаються.

Відповідно до цих завдань існують три основні групи засобів технічного захисту інформації.

Першу групу технічних засобів частіше називають фізичними. Фізичні засоби (заходи) засновані на застосуванні різного роду механічних, електро-механічних або електронно-механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи і інформації, що захищається. В якості фізичних засобів слід розглядати різного роду електронні замки, спеціальні посилені двері, спеціальні перегородки і кабіни, ґрати на вікнах, різного роду екрани, огорожі та ін.

До ***технічних засобів другої групи*** слід віднести всі ті кошти, які призначені для обмеження доступу до АС в цілому і захисту інформації від технічних розвідок, тобто що входять до складу АС і виконують (самостійно або в комплексі з іншими засобами) функції захисту. Це також засоби створення перешкод технічних засобів розвідки (генератори шумів та ін.) Тобто засоби, які знижують або виключають побічні електромагнітні випромінювання (ПЕМВН).

Методи і засоби технічного захисту конфіденційної інформації включають:

• методи і засоби захисту об'єктів від спостереження в оптичному діапазоні електромагнітних хвиль, від радіолокаційного і радіотеплолокаціонного спостереження;

• методи захисту ліній зв'язку установ і підприємств від витоку конфіденційної інформації;

• методи і засоби усунення (зниження) витоку інформації за рахунок паразитних електромагнітних випромінювань і наведень (ПЕМВН),

• кошти радіоелектронної протидії засобам радіо і радіотехнічної розвідки;

• методи і засоби захисту акустичної інформації, заходи по приховуванню об'єктів від акустичної, гідроакустичної і сейсмічної розвідки;

• методи захисту об'єктів від хімічної, радіаційної і магнітометричної розвідки.

Третю групу представляють технічні засоби охорони. Це різного роду електронні засоби відеоспостереження та сигналізації, лазерні, оптичні, інфрачервоні засоби сигналізації про проникнення в приміщення де розташовані АС, тобто технічні засоби візуального спостереження, зв'язку та охоронної сигналізації, які застосовуються службами безпеки підприємств, офісів та ін . До технічних засобів охорони відносяться:

• датчики;

• прилади візуального спостереження;

• системи збору та обробки інформації;

• засоби зв'язку;

• засоби живлення і сигналізації.

Недоліком інженерно-технічних методів і засобів захисту є те, що вони не можуть захистити інформацію від персоналу допущеного до роботи в АС. Для вирішення цього

завдання призначені програмно-апаратні методи та засоби захисту. Однак, вони є занадто дорогими.

5.3 ОРГАНІЗАЦІЙНІ І ТЕХНІЧНІ ЗАХОДИ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В КОМЕРЦІЙНИХ СТРУКТУРАХ.

Блокування несанкціонованого отримання інформації за допомогою технічних засобів є досить складним завданням, а його вирішення вимагає суттєвих матеріальних затрат. Тому перед тим, як прийняти конкретні заходи, необхідно проаналізувати стан справ і врахувати наступні рекомендації:

1. Найнадійнішим методом обмеження електромагнітного випромінювання є повне екранування приміщення, в якому знаходяться засоби обробки і передачі цінної інформації. Екранування здійснюється сталевими або алюмінієвими листами або листами із спеціальної пластмаси товщиною не менше 2 мм з надійним заземленням.

2. При обробці цінної інформації основним джерелом високочастотного електромагнітного випромінювання є дисплей персонального комп'ютера. Необхідно пам'ятати, що зображення з його екрану можна приймати на віддалі кількох сотень метрів. Повністю нейтралізувати відхід інформації з екрану можна, лише використовуючи генератор шуму. Для обробки особливо важливої інформації рекомендується використання плазмових або рідкокристалічних дисплеїв, в сучасних умовах, коли такі дисплеї стали поширеними слід приділяти особливу увагу випадкам, коли застосовується застаріле обладнання.

3. Джерелом потужного низькочастотного випромінювання є друкуючий пристрій. Для блокування відходу інформації в цьому випадку рекомендується використати зашумлення або термодрук чи струменевий принтер.

4. В багатьох випадках існують небезпечні наводки на провідники, що виходять за межі приміщення, яке підлягає охороні. Необхідно слідкувати, щоб всі з'єднання обладнання із "зовнішнім світом" здійснювалися через електричну розв'язку.

5. Дуже небезпечні спеціально внесені в схему обладнання обробки і зв'язку мікропередавачі або радіомаяки (закладки). Тому, після повернення обладнання з ремонту необхідно переконатися, що в ньому немає подібних закладок. Не рекомендується обробляти цінну інформацію на випадкових персональних комп'ютерах.

6. Якщо у вас з'явилися сумніви відносно безпеки інформації, запросіть спеціалістів – вони визначать можливий канал витоку і запропонують ефективні заходи для захисту.

При виборі технічних засобів захисту інформації потрібно враховувати наступні фактори:

1. Режим шифрування-дешифрування повинен бути простим і зручним для санкціонованого користувача.

2. Ефективність і надійність алгоритму шифрування не повинна залежати від змісту інформації, що передається.

3. Не варто віддавати перевагу тим системам, в яких криптографічні алгоритми є комерційною таємницею організації-розробника. Набагато краще, коли алгоритм відомий до деталей і відповідає деякому стандарту, а необхідний рівень стійкості визначається, наприклад, довжиною ключа.

4. Аналогові скремблери не забезпечують гарантований захист переговорів, оскільки в каналі зв’язку присутні частини вихідного аналогового сигналу. Використання їх має сенс лише в тих випадках, коли використання цифрових засобів захисту мови неможливе або економічно невигідне.

Оптимальне вирішення складної проблеми забезпечення безпеки зв’язку можливе лише при комплексному підході з використанням, як організаційних, так і технічних заходів. Досягнення сучасної мікроелектроніки, обчислювальної техніки і методів криптографічного перетворення дозволяють оптимістично дивитись на перспективи забезпечення безпеки зв’язку. Цьому сприяє і основна тенденція розвитку сучасних систем зв’язку — перехід до цифрових методів обробки інформації, які забезпечують безпеку зв’язку за рахунок високої стійкості криптографічного перетворення.

Закони й нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, створюваних у державі, у відомствах, установах і організаціях. При розгляді питання безпеки інформації така діяльність ставиться до організаційних методів захисту інформації.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації.

Відповідно до законів і нормативних актів у міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації створюються спеціальні служби безпеки (на практиці вони можуть називатися й інакше). Ці служби підпорядковуються, як правило, керівництву установи. Керівники служб організують створення й функціонування систем захисту інформації. Повну відповідальність за стан інформаційної безпеки несуть керівники організації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системі:

- організація робіт з розробки системи захисту інформації;
- обмеження доступу на об'єкт і до ресурсів системи;
- розмежування доступу до ресурсів системи;
- планування заходів;
- розробка документації;
- виховання й навчання обслуговуючого персоналу й користувачів;
- сертифікація засобів захисту інформації;
- ліцензування діяльності по захисту інформації;
- атестація об'єктів захисту;
- удосконалювання системи захисту інформації;
- оцінка ефективності функціонування системи захисту інформації;
- контроль виконання встановлених правил роботи в системі.

Організаційні методи є базисом комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації

системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких будуть розміщуватися системи; проектуванні системи, монтажі й налагодженні її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Основні властивості методів і засобів організаційного захисту:

- обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;
- обмеження можливості перехоплення ПЕМВН;
- розмежування доступу до інформаційних ресурсів і процесів (встановлення правил розмежування доступу, шифрування інформації при її зберіганні і передачі, виявлення та знищення апаратних і програмних закладок);
- резервне копіювання найбільш важливих з точки зору втрати масивів документів;
- перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв;
- кількість осіб, що бере участь у конфіденційних переговорах має бути обмежена до мінімуму;
- вхід сторонніх осіб під час проведення наради має бути заборонений;
- повинна бути чітко розроблена охорона виділеного приміщення під час наради , а також спостереження за обстановкою на поверсі ;
- будь-які роботи в кімнаті, що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання, ремонт побутової техніки, невеликий косметичний ремонт, повинен проводитися в обов'язковій присутності працівника служби безпеки;
- після проведення наради кімната повинна ретельно оглядатися, закриватися і опечатуватися;
- між нарадами кімната повинна бути закрита і опечатана відповідальною особою;
- профілактика зараження комп'ютерними вірусами.

Основою проведення організаційних заходів є використання й підготовка законодавчих і нормативних документів в області інформаційної безпеки, які на правовому рівні повинні регулювати доступ до інформації з боку користувачів.

Процеси обміну інформацією.

Необхідно встановіти систему обмежень на використання відкритих каналів зв'язку для передачі конфіденційної інформації. Такими каналами є переговори з реальними і потенційними партнерами, ділове листування, надання документації компаньйонам і контрольним органам, реклама, спілкування з представниками преси, державних органів, громадських організацій. Відповідальність покладається на персонал якій готує документи та безпосередньо приймає участь у цих діях. Зрозуміло, що персонал повинен пройти перевірку на лояльність організації та користуватись певною довірою з боку організації. Персонал, що не пройшов перевірку або втратив довіру, до відомостей з обмеженим доступом не допускається.

Потрібно охороняти від можливого підслуховування або сканування свої телефони, факси, комп'ютери, офіси, автомобілі, квартири. Використовувати апаратуру зв'язку, що засекречує генератори перешкод, прилади для виявлення "жучків" і сканувальних пристроїв, застосовувати умовні кодові позначення.

Вироби та документи.

Потрібно організувати надійний облік усіх товарів, промислових і експериментальних зразків, відомості про які не повинні стати надбанням конкурентів. Охороняти перелічені вироби слід на всіх етапах їх "руху" усередині фірми (придбання, виготовлення, випробування чи перевірка якості, транспортування, зберігання, експлуатація, ремонт). Вироби та зразки небхідно надійно зберігати, обмежити час, коли вони знаходяться на руках виконавців. Виконавці несуть персональну відповідальність за носії інформації з обмеженим доступом під час роботи з ними. Сдача та прийом таких виробів та документів проходить під особистий розпис.

Основні методи захисту інформації технічними засобами.

Загалом технічними засобами захист інформації забезпечують, коли:

- джерело і носій інформації локалізовані в межах об'єкта захисту і містять механічні перешкоди від контакту з ними зловмисника чи дистанційного впливу на них полів його технічних засобів добування інформації;

- співвідношення енергії носія і перешкод на виході приймача каналу витоку таке, що зловмисникові не вдасться зняти з носія інформацію належної якості;

- зловмисник не може знайти джерело чи носій інформації;

- замість справжньої зловмисник приймає несправжню інформацію, котру він оцінює як справжню.

Ці варіанти реалізують такими методами захисту:

- запобігання безпосередньому проникненню зловмисника до джерел інформації за допомогою інженерних конструкцій і технічних засобів охорони;

- приховування достовірної інформації;

- дезінформація - "підсунення" зловмисникові неправдивої інформації. Застосування інженерних конструкцій і охорона - найбільш давній метод захисту людей і матеріальних цінностей. Способи захисту на основі інженерних конструкцій у поєднанні з технічними засобами охорони також поширені. Разом вони утворюють так званий фізичний захист. Але цей термін не можна вважати вдалим, оскільки інші методи захисту інформації за допомогою технічних засобів також ґрунтуються на законах фізики. З огляду на те, що основу розглянутого методу становлять інженерні конструкції і технічні засоби охорони, доцільно визначити його як інженерний захист і технічна охорона об'єктів (ІЗТОО).

Основним завданням є запобігання безпосередньому контакту зловмисника чи сил природи з об'єктами захисту – люди і матеріальні цінності, носії інформації, локалізовані в просторі. До носіїв інформації належать папір, машинні носії, фото- й кіноплівка, продукція, матеріали, тобто все, що має розміри й вагу. Носії інформації у вигляді електромагнітних та акустичних полів, електричного струму не мають чітких меж, і для захисту інформації на них методи інженерного захисту неприйнятні (поле з інформацією, наприклад, не можна зберігати в сейфі). Для захисту інформації на таких носіях застосовують методи приховування інформації.

Приховування інформації передбачає такі зміни структури й енергії носіїв, за яких зловмисник не може безпосередньо чи за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах.

Розрізняють інформаційне й енергетичне приховування. Інформаційного приховування досягають зміною чи створенням несправжнього інформаційного портрета семантичного повідомлення, фізичного об'єкта чи сигналу. Інформаційним портретом можна

назвати сукупність елементів і зв'язків між ними, що відображують зміст повідомлення (мовного чи цифрового), ознаки об'єкта чи сигналу. Елементами дискретного семантичного повідомлення, наприклад, є літери, цифри чи інші знаки, а зв'язок між ними визначається їх послідовністю. Інформаційними портретами об'єктів спостереження, сигналів і речовин є еталонні ознаки їх структури.

Можливі такі способи зміни інформаційного портрета:

- видалення частини елементів і зв'язків, що утворюють інформаційний вузол (найбільш інформативну частину) портрета;
- зміна частини елементів інформаційного портрета при збереженні незмінності зв'язків між елементами, що залишилися;
- усунення зміни зв'язків між елементами інформаційного портрета при збереженні їх кількості.

Зміну інформаційного портрета об'єкта зумовлює зміна зображення його зовнішнього вигляду (видових демаскувальних ознак), характеристик випромінюваних ним полів чи електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення структур об'єкта і навколишнього його фону.

В умовах ринку, коли виробник змушений рекламувати свій товар, найбільш доцільним способом інформаційного приховування є вилучення з реклами чи відкритих публікацій найбільш інформаційних зведень чи ознак - інформаційних вузлів, що містять таємницю, яка охороняється. До інформаційних вузлів належать принципово нові технічні, технологічні рішення й інші досягнення, що становлять ноу-хау. Вилучення з технічної документації інформаційних вузлів не дасть змоги конкуренту скористатися інформацією, що міститься в рекламі чи публікаціях. Цей спосіб дає змогу:

- зменшити обсяг інформації, що захищається, і тим самим спростити проблему захисту даних;
- використовувати в рекламі нової продукції відомості про неї, не боячись розголошення.

Інший метод інформаційного приховування полягає в трансформації вихідного інформаційного портрета в новий, який відповіли несправжній інформації чи несправжній ознаковій структурі, і "нав'язуванні" нового портрета органу розвідки. Такий метод ще називається дезінформуванням.

Він є одним із найефективніших способів захисту інформації, оскільки:

- створює у власника інформації, яка має бути захищена, запас часу, зумовлений перевіркою з боку розвідки вірогідності отриманої інформації;
- наслідки прийнятих конкурентом на основі удаваної інформації рішень можуть бути для нього гіршими порівняно з рішеннями, прийнятими за відсутності інформації, яку добувають.

Розрізняють такі способи дезінформування:

- заміна реквізитів інформаційних портретів, які мають бути захищені, у випадку, коли інформаційний портрет об'єкта захисту схожий на інформаційні портрети інших "відкритих" об'єктів і не має специфічних інформативних ознак. При цьому обмежуються розробленням і підтримкою версії про інший об'єкт, видаючи за його ознаки дані об'єкта, який потрібно захищати. Наприклад, нині велика увага приділяється продукції подвійного застосування: військового і цивільного. Поширення інформації про виробництво продукції цивільного використання є надійним прикриттям для продукції військового призначення;

- підтримка версії з ознаками, запозиченими з різних інформаційних портретів реальних об'єктів. Застосовують, коли організація одночасно виконує кілька закритих тем. Використовуючи різні ознаки, що стосуються певних тем, можна нав'язати протилежній стороні неправильне уявлення про роботи, що ведуться, без імітації додаткових ознак;
- поєднання справжніх і несправжніх ознак, причому останніми заміняють незначну, але найбільш цінну інформацію, що стосується об'єкта, який підлягає захисту;
- зміна тільки інформаційних вузлів зі збереженням незмінною іншої частини інформаційного портрета.

Використовують переважно різні комбінації цих варіантів.

Іншим ефективним методом є енергетичне приховування інформації. Воно полягає в застосуванні способів і засобів захисту інформації, що запобігають виконанню енергетичної умови розвідувального контакту або утруднюють його.

Енергетичного приховування досягають зменшенням потужності сигналів, тобто носіїв (електромагнітного або акустичного полів і електричного струму) інформації і створенням перешкод. Зменшити відношення сигнал/перешкода (слово "потужність", як правило, опускається) можна двома методами: зниженням потужності або збільшенням потужності перешкоди на вході приймача.

Для конкретних видів інформації і модуляції сигналу існують граничні значення відношення перешкода, нижче яких забезпечується енергетичне приховування інформації.

Необхідність і ефективність інженерного захисту і технічної охорони підтверджується статистикою, за якою понад 50% вторгнень відбувається на комерційні об'єкти з вільним доступом персоналу і клієнтів і тільки 5% - на об'єкти з посиленим режимом охорони із застосуванням спеціально навченого персоналу і складних технічних систем охорони.

І. ЗАХИСТ ОБ’ЄКТІВ.

1.1 ЗАХИСТ ОБ’ЄКТІВ ВІД СПОСТЕРЕЖЕННЯ В ОПТИЧНОМУ ДІАПАЗОНІ ЕЛЕКТРОМАГНИТНИХ ХВИЛЬ.

Захист інформації від спостереження в оптичному діапазоні заснований на загальних методах з урахуванням особливостей оптичного каналу витоку інформації. Для захисту об'єктів спостереження зменшують контраст/фон, знижують яскравість об'єкта і не допускають наближення зловмисників до об'єкта.

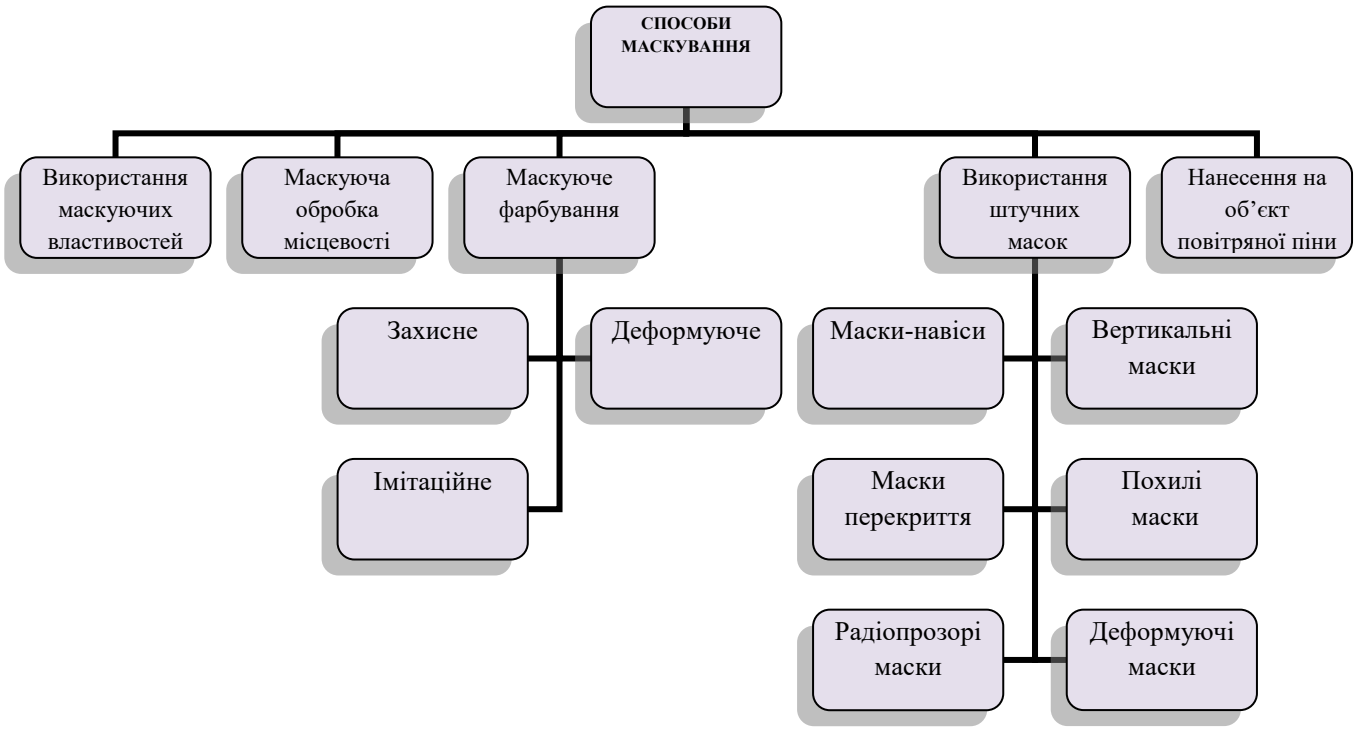
Маскування

Основний напрямок захисту об'єктів від спостереження – це їх маскування, який представляє собою метод інформаційного приховування ознак об'єкта спостереження шляхом руйнування його інформаційного портрету.

Спостереження передбачає отримання і аналіз зображення об'єкта спостереження, а також добування семантичної інформації і сигнальних ознак. В результаті спостережень видобуваються в основному видові ознаки об'єктів. Але може бути отримана і семантична інформація, якщо об'єкт спостереження представляє зображення на мові спілкування. Так, текст або схема конструкції приладу на столі керівника або фахівця можуть бути підглянуті в ході їх відвідування.

Об'єкти можуть спостерігатися безпосередньо – очима або за допомогою технічних приладів та засобів. Розрізняють такі способи спостереження з використанням технічних засобів:

- візуально-оптичний;
- за допомогою приладів спостереження в ІЧ-діапазоні;
- спостереження з консервацією зображення (фото і кінозйомка);
- телевізійне спостереження;
- лазерне спостереження;
- радіолокаційне спостереження;
- радіотеплове спостереження.



Мал. 1.1.1 Класифікація способів маскування

Використання маскуючих властивостей місцевості (нерівностей ландшафту, гір, пагорбів і т.п.) є найбільш дешевим способом, однак для реалізації даного способу необхідна наявність в місці знаходження об'єкта таких масок. Крім того, що маскуючі можливості рослинності залежать від пори року (мал. 1.1.1).

Якщо недостатні для маскування природні умови, то в цьому випадку застосовується додаткова обробка місцевості, що підвищує її маскувальні здатності. Вона полягає в нарізуванні дерну, посіві трави, створенні огорож з живою рослинністю, в хімічній обробці ділянок місцевості.

Маскувальне фарбування досягається шляхом нанесення на поверхню об'єкта фарб, підібраних за кольором і яскравістю, близькими до фона. Існують наступні види маскувального фарбування:

- захисне,
- деформуюче,
- імітаційне.

Захисне фарбування виробляється одноколірною фарбою під колір і середню яскравість фону навколишньої місцевості і предметів, що знаходяться поруч.

Деформуюче фарбування передбачає нанесення на поверхні об'єкту плям неправильної геометричної форми, що імітують світлові плями навколишнього середовища.

При імітаційному фарбуванні колір і характер плям на поверхні підбирається під забарвлення навколишньої місцевості. У цьому випадку забезпечується найбільш краще приховування.

Для маскування без фарбування створюються спеціальні конструкції – штучні маски. Існують наступні види штучних масок:

- маски-навіси,
- вертикальні маски,
- маски перекриття,
- похилі маски,
- радіопрозорі маски,
- деформуючі маски.

Маски-навіси призначені для приховування об'єктів, розташованих на відкритих майданчиках, на верхніх поверхах будівель, височинах і захищають їх від спостереження.

Вертикальні маски захищають об'єкти від спостереження з землі.

Маски перекриття складаються з каркаса і маскувального покриття, які повністю закривають об'єкт.

Похилі маски використовуються для приховування тіней об'ємних предметів, по довжині яких з урахуванням висоти Сонця визначають висоту об'єктів при спостереженні зверху.

Радіопрозорі маски виконуються з радіопрозорих матеріалів (склопластику, пінопласту і т.п.) у формі кулі для приховування демаскуючих ознак і захисту антен).

Деформуючі маски приховують не тільки зовнішній вигляд об'єкта, але і створюють хибне уявлення у спостерігача про його форми. Штучні маски виготовляються у вигляді різних збірних пересувних конструкцій, які можуть багаторазово використовуватися, не впливають на природу, сумісні з іншими видами конструкцій.

Світлонепроникні одно- і багато кольорові повітряні піни, швидко наносяться за допомогою піногенераторів на об'єкти, забезпечують їх ефективне маскування в широкому діапазоні довжин хвиль протягом декількох годин.

Енергетичне приховування об'єктів досягається шляхом зменшення яскравості об'єкта і фону нижче чутливості очей або оптичного приймача, а також їх осліплення.

Енергетичне приховування об'єктів, які спостерігаються у відбитому світлі, забезпечують розглянуті штучні маски і аерозолі (речовини у вигляді дисперсії твердих частинок і крапель рідини, що знаходяться в підвішеному стані в повітрі). До аерозолів відносять дим, пил, тумани.

Небажані випромінювання різних пристроїв можуть містити небезпечні сигнали. В процесі функціонування технічних засобів обробки інформації елементи генераторів, підсилювачів і інших випромінювачів електромагнітних полів пристроїв можуть виявитися в зоні дії електромагнітних полів небезпечних сигналів. Вплив електромагнітного поля небезпечного сигналу на пристрої може призвести до зміни параметрів окремих елементів генератора або підсилювача (наприклад, крутизни характеристики активного елемента, контурної ємності або індуктивності, ємностей p-n переходів транзисторів, опору навантаження каскаду і т.п .). Результатом такої зміни є паразитна модуляція небезпечним сигналом небажаних випромінювань технічних засобів. Вид і кількісні параметри, що характеризують цю модуляцію, визначаються конкретною ситуацією. Таким чином, зовнішній вплив електромагнітних полів небезпечних сигналів на елементи високочастотних генераторів, підсилювачів і інших технічних засобів може привести до амплітудної та кутової модуляції високочастотних коливань в цих пристроях. Наслідком цього є поява в навколишньому середовищі небажаних випромінювань, модульованих небезпечними сигналами, тобто створюються передумови для витоку інформації, що обробляється технічними засобами.

Між двома електричними ланцюгами (елементами, вузлами, засобами), що знаходяться на деякій відстані один від одного, можуть виникати небажані електромагнітні зв'язки. Наявність таких зв'язків призводить до того, що сигнали, які циркулюють в одного ланцюга (в ланцюзі джерела наведення), з'являються в іншому електричному колі (в ланцюзі рецептора наведення). Основними шляхами виникнення небажаних зв'язків є:

- ближнє електричне поле;
- ближнє магнітне поле;
- електромагнітне поле випромінювання;
- з'єднувальні дроти, кабелі і хвилеводи, ланцюги живлення, заземлення та інші струмопровідні елементи та конструкції.

На малих відстанях можуть існувати всі зазначені види небажаних зв'язків. Зі збільшенням відстані послаблюються і зникають зв'язки через близьке електричне та магнітне поля, а на великих відстанях – і через електромагнітне поле випромінювання.

Зв'язок через близьке електричне та магнітне поля.

Теоретично повна незалежність ближнього електричного і магнітного полів може спостерігатися тільки в статичних умовах. Електростатичним називається поле нерухомих зарядів. При будь-якому переміщенні цих зарядів з’являється магнітне поле. Так само магнітостатичне поле постійного магніту або електромагніту, що живиться постійним струмом. При будь-якій зміні цього поля з'являється електричне

поле. Вичерпний аналіз зв'язку ланцюгів з урахуванням взаємозалежності електричного і магнітного полів може бути виконаний за допомогою рівнянь Максвелла.

Електромагнітні випромінювання, супутні роботі технічних засобів систем інформатизації та зв'язку, поширюються в навколишньому середовищі. У зону дії цих випромінювань потрапляє велика кількість токопровідних елементів і конструкцій, що володіють властивостями антен. У таких випадкових антенах електромагнітне поле наводить ЕРС або ток небезпечного сигналу. Роль випадкових антен можуть грати провідники монтажних схем технічних засобів, струмопровідні елементи систем заземлення, металеві корпуси апаратури, металоконструкції систем водопостачання та каналізації, сторонні протяжні провідники (наприклад, проводи відкритого телефонного або гучномовного зв'язку, сигналізації, часифікации, електроживлення і т.п.). Токи небезпечних сигналів, що наводяться електромагнітними полями, супутніми роботі технічних засобів, поширюючись по електропровідних комунікаціях, створюють реальні передумови витоку інформації.

1.2 СПОСОБИ ЗАХИСТУ ЛІНІЙ ЗВ'ЯЗКУ УСТАНОВ І ПІДПРИЄМСТВ ДЕРЖАВНИХ І КОМЕРЦІЙНИХ СТРУКТУР ВІД ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ.

Об'єкт посягань інженерно-технічної розвідки противника – це інформація, витік якої здатний завдати шкоди безпеці об'єкту. Для раціонального забезпечення захисту інформації та скорочення витрат на реалізацію конкретних заходів, необхідно враховувати наступні принципи, що характеризують професійний підхід до цих питань:

• відповідність рівня захисту ступеня цінності інформації;

• гнучкість захисту;

• багатозональність засобів захисту (тобто розміщення джерел інформації в зонах з контрольованим рівнем її безпеки);

• багаторубіжність засобів захисту інформації на шляху руху ворожого агента (або технічного засобу розвідки).

Відповідність рівня захисту цінності інформації. Цей принцип визначає економічну доцільність тих чи інших заходів захисту. Він полягає в тому, що витрати на захист не повинні перевищувати ціну, що захищається. В іншому випадку захист нерентабельний.

Гнучкість захисту проявляється в можливості зміни ступеня захищеності відповідно до зміненими вимогами до безпеки об'єкту захисту в цілому та інформації зокрема. Захист повинна бути гнучкою тому, що ціна інформації - величина змінна, що залежить як від джерела інформації, так і від часу.

Ступінь захищеності інформації визначає рівень її безпеки. Необхідний рівень безпеки інформації досягається багатозональна і многорубежностью захисту.

Багатозональна забезпечує диференційований санкціонований доступ різних категорій співробітників і відвідувачів НХС до джерел інформації.

Даний принцип реалізується шляхом поділу простору, займаного об'єктом захисту.

Типовими зонами є:

• територія, яку займає організацією і обмежена огорожею або умовної зовнішнім кордоном;

• будівлі та інші споруди на цій території;

• коридори, сходові марші, шахти ліфтів;

• приміщення (кабінети, кімнати, зали, технічні приміщення, склади і т.д.);

• шафи, сейфи, сховища.

Зони можуть бути незалежними (будівлі, приміщення в будинках), що перетинаються і вкладеними (кімнати всередині будівлі, сейфи всередині кімнат).

Для перешкоджання проникненню агента противника в зону на її кордоні створюються один чи кілька рубежів захисту. Особливістю захисту кордону зони є вимога рівної міцності рубежів на кордоні, а також наявність контрольно-пропускних пунктів (постів), що забезпечують керований доступ людей і автотранспорту в зону.

Додамо, що своєрідними рубежами захисту є також негласні помічники СБ України. Вони знаходяться в контрольованих зонах у зв'язку зі своїми основними службовими обов'язками і одночасно відстежують ситуацію. При необхідності вони негайно повідомляють в підрозділ служби безпеки про виявлені порушення або інших значущих фактах.

Рубежі захисту створюються і всередині зон на можливі шляхи руху агентів або поширення носіїв інформації (перш за все, електромагнітних і акустичних полів). Так, для захисту від підслуховування може бути встановлений кордон захисту у вигляді акустичного екрану.

Кожна зона характеризується рівнем безпеки знаходиться в ній інформації. Безпека інформації в зоні залежить від чинників:

• відстані від джерела інформації (сигналу) до шпигуна або його кошти добування інформації;

• числа і рівня захисту рубежів (агентурних і технічних) на шляху руху шпигуна або носія інформації (наприклад, поля);

• ефективності способів і засобів управління допуском людей і автотранспорту в зону;

• заходів щодо захисту інформації всередині зони.

Чим далі віддаленість джерела інформації від місця знаходження суб'єкта розвідки противника (або його технічного засобу добування інформації) і чим більше рубежів захисту, тим більше час займає просування шпигуна до цього джерела (тим сильніше слабшає енергія носія у вигляді поля або сили електричного струму).

Число зон і рубежів захисту, їх просторове розташування слід вибирати таким чином, щоб забезпечити необхідний рівень безпеки інформації, що захищається як від зовнішніх загроз (що знаходяться поза територією), так і внутрішніх (проникли на територію агентів, встановлених там технічних засобів знімання інформації). Чим більш цінною є інформація, що захищається, тим більшим числом рубежів і зон доцільно оточувати її джерело.

При створенні інженерно-технічної системи захисту доцільно, крім того, враховувати принципи:

• надійність агентурних і технічних засобів системи, що виключають як пропуск загроз, так і помилкові дії;

• обмежений і контрольований доступ до інженерно-технічних елементів системи забезпечення безпеки інформації;

• безперервність роботи системи в будь-яких умовах функціонування об'єкта захисту (наприклад, при короткочасній відсутності електроенергії);

• адаптованість (пристосовність) системи до змін навколишнього середовища.

Сенс зазначених принципів очевидний.

1.3 СПОСОБИ УСУНЕННЯ (ЗНИЖЕННЯ) ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК ПАРАЗИТНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ І НАВЕДЕНЬ.

Всі системи захисту телефонних ліній діляться на пасивні і активні.

До засобів ***пасивного захисту*** відносяться фільтри (мал. 1.3.1) і інші засоби, призначені для зриву деяких видів прослуховування приміщень за допомогою телефонних ліній, що знаходяться в режимі відбою. Ці засоби можуть встановлюватися в розрив телефонної лінії або вбудовуватися безпосередньо в ланцюзі телефонного апарату.

Позитивні властивості засобів пасивного захисту:

• запобігання перехопленню мовної інформації методом ВЧ-нав’язування;

• запобігання перехопленню мовної інформації через витік мікроЕДС-ланцюга дзвінка;

• запобігання перехопленню за допомогою мікрофонів, що передають мовну інформацію по телефонній лінії в довгохвильовому діапазоні, за умови правильного розміщення фільтра телефонної лінії.

Недоліком засобів пасивного захисту є те, що вони не захищають від інших систем перехоплення.

Крім зазначених пристроїв широко застосовуються різні індикаторні прилади (мал.1.3.2)

Мал. 1.3.1 Захисні фільтри

Мал. 1.3.2 Індикатор стану телефоних ліній

Принцип дії індикаторних пристроїв заснований на вимірюванні та аналізі параметрів телефонних ліній. Основними параметрами, які найбільш легко піддаються контролю, є значення постійної складової напруги в лінії і величина постійного струму, що виникає в лінії під час розмови. Крім того, аналізу можуть бути піддані виміри активної і реактивної складової комплексного опору лінії, зміни напруги в момент зняття трубки. У більш складних приладах проводиться аналіз не тільки постійної, а й змінної складової сигналу.

На основі проведених вимірювань прилад приймає рішення про наявність несанкціонованих підключень або просто сигналізує про зміну параметрів лінії. Саме використання досить складного алгоритму прийняття рішення і відрізняє аналізатор від простого індикатора.

Звичайно, апаратура контролю ліній зв'язку не забезпечує повного захисту від зловмисників, але життя їм істотно ускладнює. Для того щоб включитися в захищену лінію і не бути при цьому виявленим, зловмисникові доведеться використовувати системи перехоплення, які практично не змінюють параметрів лінії або максимально компенсують зміни.

Однак слід зазначити, що аналізатори та індикатори мають і ряд істотних недоліків.

По-перше, відсутні чіткі критерії для встановлення факту наявності несанкціонованого підключення. Телефонні лінії (особливо вітчизняні) далеко не ідеальні. Навіть в специфікації на стандартні параметри сигналів міських АТС передбачений великий розкид. Крім того, параметри міняються в залежності від часу доби, завантаженості АТС, коливань напруги в електромережі, вологості і температури. Сильно впливають і різного виду наводки.

По-друге, висока ймовірність помилкових спрацьовувань. Більш надійними є ті прилади, які просто фіксують зміни того чи іншого параметра, надаючи приймати рішення самому користувачеві.

По-третє, найбільшим недоліком аналізаторів є те, що вони можуть зафіксувати лише невелику частину пристроїв перехоплення з багатого арсеналу зловмисників.

По-четверте, майже всі аналізатори влаштовані так, що при їх установці потрібно балансування під параметри лінії. Якщо при цій операції на лінії вже була встановлена закладка, то вона виявлена не буде.

1.4 АКТИВНА РАДІОЕЛЕКТРОННА ПРОТИДІЯ ЗАСОБАМ РАДІО І РАДІОТЕХНІЧНОЇ РОЗВІДКИ.

Методи контролю провідних ліній, як слабкострумових (телефонних ліній, систем охоронної та пожежної сигналізації тощо), так і силових, засновані на виявленні в них інформаційних сигналів (низькочастотних і високочастотних) і вимірі параметрів ліній.

Використання того чи іншого методу контролю визначається типом лінії і характеристиками апаратури контролю.

Методи контролю телефонних ліній, як правило, засновані на тому, що будь-яке підключення до них викликає зміна електричних параметрів ліній: амплітуд напруги і струму в лінії, а також значень ємності, індуктивності, активного і реактивного опорів лінії. Залежно від способу підключення закладного пристрою до телефонної лінії (послідовного, в розрив одного з проводів телефонного кабелю або паралельного), ступінь його впливу на зміну параметрів лінії буде різною.

За винятком особливо важливих об'єктів, лінії зв'язку побудовані за стандартним зразком. Введення лінії в будівлю здійснюється магістральним багатопарним (багатожильним) телефонним кабелем до внутрішнього розподільного щита. Далі від щита до кожного абонента проводиться розводка двопровідним телефонним дротом марки ТРП або ТРВ. Дана схема характерна для житлових і адміністративних будівель невеликих розмірів. При великих розмірах адміністративних будівель внутрішня розводка робиться набором магістральних кабелів до спеціальних розподільних колодок, від яких на невеликі відстані (до 20-30 м) розводка також проводиться проводом ТРП або ТРВ.

У статичному режимі будь-яка двухпроводна лінія характеризується хвильовим опором, яке визначається погонними ємністю (пФ/м) і індуктивністю (Гн/м) лінії. Хвильовий опір магістрального кабелю лежить в межах 130-160 Ом для кожної пари, а для проводів марки ТРП і ТРВ має розкид 220 - 320 Ом.

Підключення засобів знімання інформації до магістрального кабелю (як зовнішнього, так і внутрішнього) малоймовірно. Найбільш уразливими місцями підключення є: вхідний розподільний щит, внутрішні розподільні колодки і відкриті ділянки з дроту ТРП, а також телефонні розетки і апарати. Наявність сучасних внутрішніх міні-АТС не впливає на зазначену ситуацію.

Основними параметрами радіозакладок, що підключаються до телефонної лінії, є наступні. Для закладок з паралельним включенням важливою є величина вхідної ємності, діапазон якої може змінюватися в межах від 20 до 1000 пФ і більше, і вхідний опір, величина якого становить сотні кілоОм. Для закладок з послідовним включенням основним є її опір, яке може становити від сотень Ом в робочому до декількох мегаОм в черговому режимах.

Телефонні адаптери з зовнішнім джерелом живлення, гальванічно підключаються до лінії, мають великий вхідний опір до декількох мегаОм (в деяких випадках і більше 100 МОм) і досить малу вхідну ємність.

Важливе значення мають енергетичні характеристики засобів знімання інформації, а саме споживаний струм і падіння напруги в лінії.

Найбільш інформативним, легко вимірюваним параметром телефонної лінії є напруга в ній при покладеній і піднятій слухавці. Це обумовлено тим, що в стані, коли телефонна трубка покладена, в лінію подається постійна напруга 60-64 В (для вітчизняних АТС) або 25-36 В (для імпортних міні-АТС), в залежності від моделі. При піднятті трубки напруга в лінії зменшується до 10-12 В.

Якщо до лінії буде підключено закладний пристрій, ці параметри зміняться (напруга буде відрізнятися від типової для даного телефонного апарату).

Однак одне лише падіння напруги в лінії (при покладеній і піднятій трубці) не дозволяє однозначно судити про те, чи встановлена в лінії закладка чи ні. Справа в тому, що коливання напруги в телефонній лінії можуть відбуватися через її погану якість (як результат

зміни стану атмосфери, пори року чи випадання опадів і т.п.). Тому для визначення факту підключення до лінії закладного пристрою необхідний постійний контроль її параметрів.

При підключенні до телефонної лінії закладного пристрою змінюється і величина споживаного струму (при піднятті трубки телефонного апарату). Величина відбору потужності з лінії залежить від потужності передавача закладки і його коефіцієнта корисної дії.

При паралельному підключенні радіозакладки споживаний струм (при піднятій телефонній трубці), як правило, не перевищує 2,5-3,0 мА.

При підключенні до лінії телефонного адаптера, що має зовнішнє джерело живлення і великий вхідний опір, споживаний з лінії струм незначний (20-40 мкА).

Комбіновані радіозакладки з автономними джерелами живлення і паралельним підключенням до лінії, як правило, мають високий вхідний опір (кілька мегаОм і більше) і практично не споживають енергію з телефонної лінії.

Вимірюючи струм в лінії під час розмови і порівнюючи його з типовим, можна виявити факт підключення закладних пристроїв із струмом споживання більше 500-800 мкА.

Для вимірювання напруги і струму витоку в лінії може використовуватися, наприклад, прилад ТСМ-03.

Визначення технічними засобами контролю закладних пристроїв з малим струмом споживання з лінії обмежена власними шумами лінії, викликаними нестабільністю як статичних, так і динамічних параметрів лінії. До нестабільності динамічних параметрів насамперед належать флуктуації струму витоку в лінії, величина якого досягає 150 мкА.

Для контролю ліній зв'язку необхідно мати її схему і "паспорт". На схемі (виконанії в масштабі) графічно або у вигляді таблиці вказуються всі санкціоновані з'єднання: розподільні коробки, щити, паралельні відводи, блокатори і т.п. із зазначенням дальності від розетки до з'єднань. Під "паспортом" зазвичай розуміються виміряні параметри лінії.

Лише при наявності схеми і "паспорта" проводиться контроль лінії технічними засобами.

Якщо лінія попередньо була очищена і паспортизована, то одним із способів виявлення підключення до лінії засобів знімання інформації є вимір електрофізичних параметрів лінії, до яких відносяться ємність, індуктивність і опір лінії.

За цим методом вимірюється загальна ємність лінії від телефонного апарату до розподільного щита і опір лінії при її відключенні (розмиканні) і замиканні на розподільчому щитку.

Надалі контроль лінії полягає в періодичній перевірці її електрофізичних параметрів.

При включенні в лінію будь-якого несанкціонованого засобу відбувається зміна її параметрів, які можуть бути виявлені, в тому числі виміром зміни ємності або опору. Так, при відключенні (розмиканні) лінії на розподільному щиті її опір або буде прагнути до нескінченності при відсутності в лінії паралельно підключеного закладного пристрою, або буде дорівнювати вхідному опору даного пристрою при його підключенні. Вимірюючи опір лінії при її замиканні на розподільному щиті, легко виявити послідовно підключені закладні пристрої.

Ефективність даного методу досить висока, однак вона обмежена флуктуаціями статичних параметрів лінії.

До типових пристроїв контролю параметрів телефонної лінії відноситься телефонний перевірочний пристрій ТПП-5.

Найбільш ефективним способом виявлення підключення до телефонної лінії засобів знімання інформації є використання локаторів провідних ліній.

1.5 ЗАСОБИ ПО УТАЄННЮ ОБ'ЄКТІВ ВІД АКУСТИЧНОЇ, ГІДРОАКУСТИЧНОЇ І СЕЙСМІЧНОЇ РОЗВІДКИ.

Акустична розвідка (АР) – це отримання інформації шляхом прийому та аналізу акустичних сигналів інфразвукового, звукового, ультразвукового діапазонів, що розповсюджуються у повітряному середовищі від об'єктів розвідки.

АР забезпечує отримання інформації, яка знаходиться безпосередньо у мові, що вимовляється або відтворюється (акустична мовна розвідка), а також у параметрах акустичних сигналів, що супроводжують роботу озброєння та воєнної техніки, механічних пристроїв оргтехніки та інших технічних систем (акустична сигнальна розвідка).

АР вирішує наступні задачі:

- дистанційний перехват змістовної мовної інформації;
- визначення технічних та тактичних характеристик озброєння і військової техніки (оцінка потужності вибухів боєприпасів та вибухових речовин при їх випробуваннях, визначення параметрів авіаційних та ракетних двигунів при стендових випробуваннях та т.п.);
- визначення характера та направленності робіт на військово-промислових об'єктах;
- визначення шумових сигнатур озброєння та військової техніки.

Для вирішення данних задач АР використовує портативну апаратуру приймання та реєстрації акустичних сигналів та стаціонарну апаратуру їх обробки і аналізу.

Гидроакустична розвідка (ГАР) – це отримання інформації шляхом приймання та аналізу акустичних сигналів інфразвукового, звукового, ультразвукового діапазонів, що розповсюджуються у водному середовищі від надводних та підводних об'єктів.

ГАР містить в собі:

- розвідку гідроакустичних шумових полів, що створюються працюючими гребними гвинтами, різними двигунами та механізмами надводних кораблів і підводних човнів;
- гідролокаційну видову розвідку, що забезпечує добування інформації, яка знаходиться у зображеннях дна та об'єктів і отримується з реєструємих відбитих сигналів;

- гідролокаційну параметричну розвідку, яка забезпечує отримання інформації, що знаходиться в просторових, швидкісних та інших характеристиках об'єкта та отримується з реєструємих відбитих сигналів;

- розвідку гідроакустичних сигналів, що створюються різними працюючими засобами гідроакустичного озброєння надводних кораблів та підводних човнів;

- розвідку звукопідводного зв'язку з метою перехоплення повідомлень (інформаційних потоків) , що передаються по каналам цього звязку, а також визначення тактичних та технічних характеристик систем звукопідводного зв'язку.

За принципом використання енергії акустичного випромінювання засоби ГАР поділяються на активні (гідролокатори) та пасивні. Гідролокатор працює за принципом випромінювання у водному середовищі зондуючих акустичних сигналів з наступним прийманням та аналізом відбитих від об'єктів та морського дна ехо-сигналів.

При веденні пасивної ГАР використовують шумопеленгатори, які приймають та аналізують шумові акустичні випромінювання у водному середовищі, які виникають при роботі двигунів, гребних валів, машин та механізмів різноманітних агрегатів надводних кораблів (НК), підводних човнів (ПЧ) та інших плавзасобів, а також засобів розвідки, що призначені для прийому та аналізу акустичних сигналів, створюваних гідролокаторами, ехолотами, системами гідроакустичного зв'язку та іншим гідроакустичним озброєнням НК, ПЧ та інших плавзасобів.

Сейсмічна розвідка (СР) – це добування інформації шляхом виявлення та аналізу деформаційних та здвигових полів в земній поверхні, що виникають під впливом різноманітних вибухів.

Основне направлення СР – розвідка підземних ядерних вибухів та визначення іх параметрів.

СР вирішує наступні завдання:

- визначення координат епіцентру вибуху;
- визначення потужності вибуху;
- визначення часу вибуху;
- визначення кількості вибухів у груповому вибухі.

Для отримання сейсмограм, які характеризують з необхідними подробицями хвильове поле, що досліджується, застосовують технічні засоби та методичні прийоми, які сворюють у сукупності узагальнений сейсмореєструючий канал. У вузькому сенсі під сейсмореєструючим каналом розуміють тільки прийом, посилення та реєстрацію коливань точок випромінюючого середовища. В цьому випадку метою реєстрації є отримання запису коливань на деякому носії. В сейсмореєструючому каналі коливання можуть бути трохи викривленні, для кращого знаходження корисних коливань.

Сейсмореєструючий канал є сукупністю послідовно з'єднаних апаратів, які виконують прийом механічних коливань ґрунту, їх перетворення в електричні коливання, підсилення, перетворення та запис на носій.

В залежності від носія, що використовується, розрізняють сейсмореєструючі канали з відтворюваною (проміжною) та з невідтворюваною реєстрацією. Застосування відтворюваного запису дозволяє відновлювати записані коливання та піддавати їх послідуючій обробці в спеціальних пристроях або ЕОМ.

У якості носія інформації використовують світлочутливу бумагу та плівки, магнітну стрічку, електрохімічну бумагу і т.п.

Прикладом відтворюваної реєстрації є запис на магнітку стрічку.

Невідтворювана реєстрація виключає можливість застосування апаратурних засобів виділення корисних сигналів при обробці. Тому сейсмореєструючий канал повинен містити пристрої, які дозволяють виділити корисні коливання при реєстрації. Канал складається із сейсмоприймача, підсилювача, фільтрів та реєструючого пристрою. Сейсмоприймач встановлюють на поверхні ґрунту або всередині середовища і виникаючі в ньому електричні коливання передають по кабелю на сейсморозвідувальну станцію, де встановлена реєструючи апаратура.

В якості реєструючого пристрою використовують дзеркальний гальванометр; в цьому випадку носій запису – світлочутлива бумага або плівка. Іноді у якості реєстратора застосовують «електричне перо», яке записує коливання на електротермічну або електрохімічну бумагу. В деяких випадках в якості реєструючого пристрою використовують ЕПТ.

1.5.1 ЗАХИСТ ОБ’ЄКТІВ ВІД АКУСТИЧНОЇ РОЗВІДКИ.

За змістом захист від акустичних засобів розвідки поділяється на організаційні та технічні.

Організаційні заходи включають:

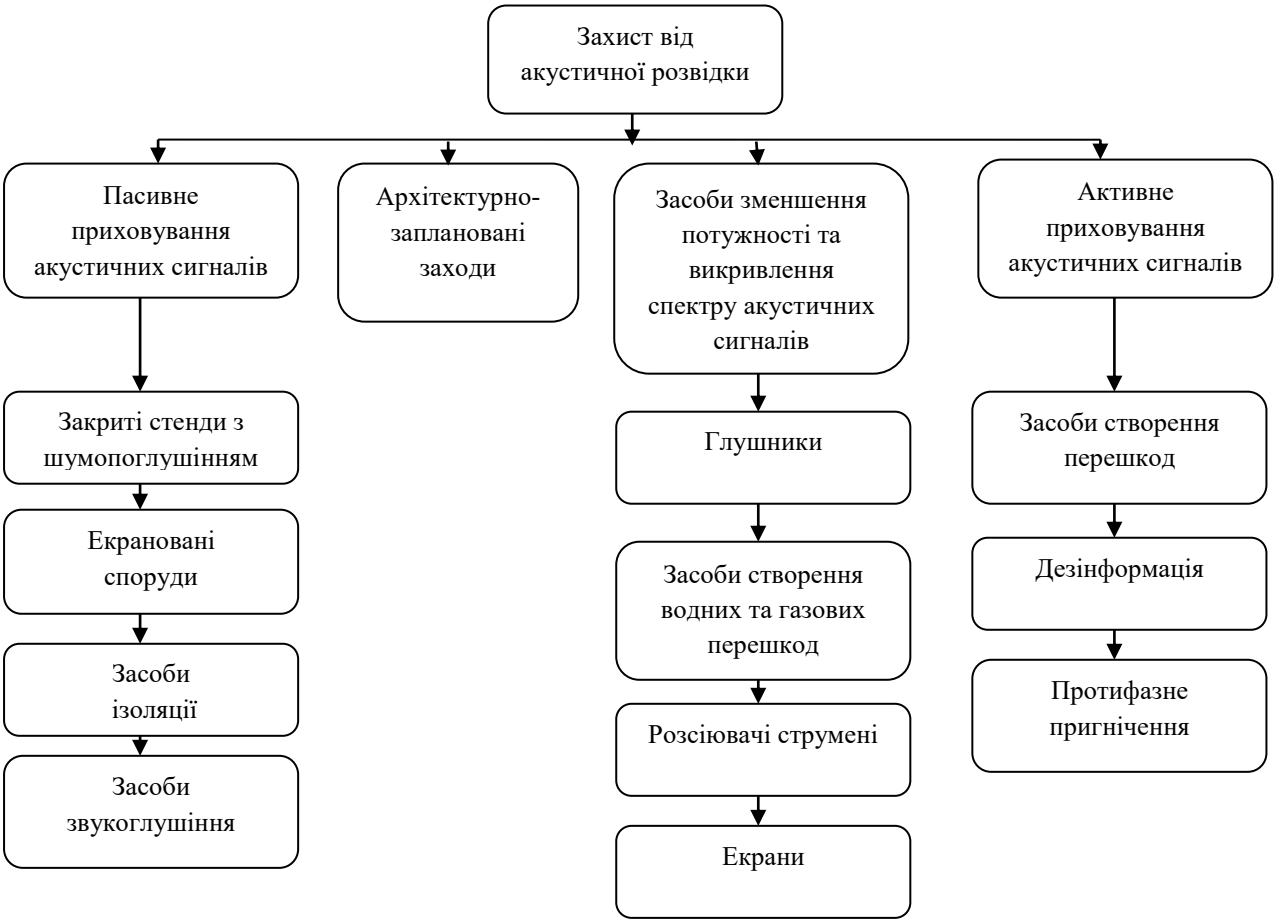
- часові, просторові та територіальні обмеження;
- посилення охорони об’єктів, що приховуються, з метою виключення можливості наближення до них технічними засобами розвідки на дальність можливого виявлення акустичних сигналів;
- вибір часу вибуху спецбоєприпасів, який співпадає з початком найближчого землетрусу;
- проведення групового вибуху спецбоєприпасів різного складу з їх просторовим розподіленням та здвигом у часі їх підриву, що забезпечує спотворення спектрального складу сейсмічних хвиль.

Технічні заходи полягають в розробці спеціальних рішень, які виключають або ускладнюють добування інформації, що міститься в акустичному полі.

Із основних технічних заходів по приховуванню акустичних сигналів (АС) від технічних засобів розвідки можна виділити:

- пасивне приховування АС;
- архітектурно-заплановані заходи;
- засоби зменшення потужності та викривлення спектру АС;
- активне приховування АС.

Класифікаційна схема засобів захисту від апаратури акустичної розвідки представлена на мал. 1.5.1.



Мал. 1.5.1 Класифікація засобів захисту від акустичної розвідки.

Пасивні засоби приховування акустичних сигналів призначені для зниження їх інтенсивності до рівня навколишнього шумового акустичного фону.

До пасивних засобів приховування АС відносяться:

- використання закритих випробувальних стендів з шумоглушінням, які забезпечують зниження шумів до рівня навколишнього акустичного фону;
- проведення випробувань об’єктів з підвищеним акустичним випромінюванням в екранованих спорудах (підземні виробки або спеціальні споруди з надійною звуковою ізоляцією та закритою системою комунікацій);
- засоби звукоізоляції елементів техніки та об’єктів, які шумлять. До них відносяться: звукоізолюючі кожухи, екрани двигунів та робочих місць, звукопоглинаючі конструкції, вібропоглиначі покриття, амортизуючі кріплення механізмів та ін.
- засоби звукопоглинання.

Пристрої ***шумопоглинання*** використовуються при випробуваннях ракетних двигунів та двигунів для літаків на закритих стендах. Конструктивно вони виконуються у вигляді: газодинамічної труби, яка забезпечує необхідну висотність та розрахункову течію газу у

сверхзвуковому соплові; газорідинного ежектора, у центральну частину якого потрапляє потік гарячих газів, а в периферійну частину через форсунки потрапляє потік води; змішувального каналу, в якому відбувається охолодження газів та створюється газорідинна суміш; закритого приймального басейну з вузлом вводу газорідинної суміші під рівнем води та вертикальної вихлопної труби для виводу в атмосферу і розсіювання продуктів згоряння із двигуна. Ефективність пристроїв по зниженню рівня акустичних шумів може досягати 70-80 дБ.

Подібні пристрої забезпечують захист і від інших засобів розвідки, тому що усуваються світові випромінювання та видимі викиди компонентів палива. Недоліком пристрою є труднощі, які пов'язані з великим використанням води при випробуваннях потужних двигунів.

Екрановані споруди – це звукоізольовані будівлі (приміщення), басейни, підземні полігони, виробітки та інші конструкції, форма та розмір яких визначається типом випробувального засобу. Основною характеристикою подібних засобів приховування АС є ефективність екранування (звукове послаблення). Ефективність екранування залежить від товщини стін, перекриття стелі або насипу, облицювального та поглинаючого матеріалу. Як правило, вони використовуються при випробуваннях двигунів бронетанкової та авіаційної техніки, а також стрілецької зброї.

Звукоізоляція є найбільш ефективним методом зниження енергії акустичного випромінювання. Вона заключається у використанні спеціальних звукоізолюючих та огороджуючих конструкцій на шляху розповсюдження АС.

До звукоізолюючих конструкцій відносяться спеціальні кожухи, екрани, вигородки. Застосування звукопоглинаючих кожухів сприяє послабленню енергії звукового випромінювання. Кожухи можуть бути з'ємними або роз'ємними. Вони виконуються із сталі, дюраля та інших негорючих матеріалів. Внутрішні поверхні стінок кожуха покриваються звукопглинаючим матеріалом. Звукоізолюючий екран – це пристрій, який створює у звуковому полі акустичну тінь. Екран може бути встановлений як поблизу джерела шуму, так і поблизу захищаємого об'єкта.

Сутність звукоізоляції при використанні огороджуючих конструкцій заключається в тому, що більша частина падаючої на огорожу звукової хвилі відбивається і лише невелика частина проникає через огорожу.

Огороджувальні конструкції бувають одношарові та багатошарові. *Одношарові огороджувальні конструкції* – це конструкції, які складаються із одного або декількох шарів, щільно пов'язаних один з одним. До них відносяться стіни, перегородки, перекриття.

Багатошарові огороджувальні конструкції – це конструкції, які складаються із декількох шарів, які не мають між собою щільного зв'язку. Між шарами можуть бути повітряні проміжки або м'які ізоляційні шари. До них відносяться стіни з гнучкими плитами, роздільні (подвійні) конструкції, міжповерхові перекриття.

З метою підвищення ефективності звукоізоляції внутрішня поверхня огорожі приміщень облицьовується звукопоглинаючим матеріалом або спеціальними звукопоглинаючими панелями. Крім того, всередині приміщення можуть біти розміщенні штучні звукопоглиначі, які представляють собою вільно підвішені об'ємні звукопоглинаючі тіла різної форми.

При падінні акустичного сигналу на звукопоглинаючий матеріал або звукопоглинаючу конструкцію значна частина звукової хвилі поглинається, а менша частина – відбивається.

За принципом поглинання звуковиз хвиль усі матеріали поділяються на три групи: пористі, резонансні та штічні.

До пористих матеріалів відносяться:

- пористі структури з твердим каркасом (плитки на пемзолиті, штукатурні плити з наповнювачем, гіпсовий та цементний фібролит);

- пористі структури з напівтвердим каркасом (деревноволокнисті, мінераловатні плити на різних зв'язках з фарбованою та профільованою поверхнею);

- пористі структури з пружним каркасом (поліуретановий поропласт, пористий полівінілхлорид, прошиті та обернуті у тканину мати з капронового волокна і т.п.).

Резонансні конструкції представляють собою перфоровані екрани, які обклеєні зі зворотнього боку тканиною та розташовані на певній відстані від жорсткої поверхні. В якості екранів використовують листи металу, деревоволокнисті та азбоцементні плити, фанера та ін. До резонансних конструкцій відносяться також мембранні (щитові) поглиначі у вигляді рамок з натягнутими на них еластичними плівками; листів фанери, пластику, древесностружних плит, які розташовані на деякій відстані від твердих стінок.

Штучні звукопоглиначі представляють собою об'ємні звукопоглинаючі тіла у формі щитів, конусів, призм, паралелепіпедів, кульок та ін., які вільно підвішуються до стелі, будівельної конструкції або до підвісної системи (наприклад, натянутої проволоки). Їх виконують із перфорованих листів твердого картону, пластмаси, металу або рулонної алюмінієвої фольги, яка обклеєна всередині войлочною тканиною або заповнена звукопоглинаючим матеріалом.

Приблизна ефективність конструктивних засобів зниження шуму в децибелах наведена у таблиці 1.5.1.

Заходи по зниженню шуму та позначення їх акустичної ефективності	**Середні частоти октавних полос, Гц**							
	63	125	250	500	1000	2000	4000	8000
Застосування щитового металічного кожуху (*δ=2 мм)* вібропоглинаючою мастикою (*δ=6 мм)* та звукопоглинаючим матеріалом	1	3	10	14	16	18	20	20
Встановлення металічного екрану (*δ=1,5 мм)* із звукооглинаючим матеріалом з боку двигуна, площа екрану не більше 40% поверхні двигуна	0	0	1	2	3	3	4	4
Розміщення малошумних агрегатів в ізольованих приміщеннях: одного з трьох агрегатів	0	0	1	1	1	2	2	2
двух із трьох агрегатів (також при встановленні ГРЩ в ЦПУ)	1	1	2	2	3	4	4	4
одного з двух агрегатів	1	1	2	2	3	5	5	5

всіх агрегатів	1	1	2	3	4	6	6	6
Встановлення звукопоглинаючих конструкцій площею не менше 50% площини огороджень при товщині матеріалу близько 50 мм, в приміщеннях, де $V/S_п$: менше 0,6	2	2	3	5	7	7	7	6
від 0,6 до 0,7	0	1	2	4	6	6	5	5
більше 0,7	0	0	1	3	5	5	4	4

Засоби звукоглушення застосовуються для зниження шуму всмоктування та газовихлопу двигунів внутрішнього згоряння, систем вентиляції та кондиціонування повітря, різних гідроприводів та ін.

Глушники по принципу дії поділяються на активні (звукопоглинаючі патрубки та пластинчаті); реактивні (камерні та резонансні) і комбіновані. До комбінованих можуть бути також віднесені екранні глушники.

Глушники активного типу ефективні на середніх та високих частотах, а реактивні та комбіновані – в широкому діапазоні частот.

Активний глушник створюється каналом або системою каналів, облицьованих звукопоглинаючим матеріалом з мінімальним аеродинамічним опором. Найпростішим глушником активного типу є звукопоглинаючий патрубок. Особливістю цього глушника є наявність спаду ефективності, починаючи з октави, у межах якої попадає значення частоти f_m:

$$f_m = 11200/\sqrt{D \cdot \delta},$$

де D – діаметр глушника, см; δ – товщина звукопоглинача, см.

При великих перехідних перетинах доцільно використовувати пластичні глушники активного типу.

Реактивні глушники виконуються у вигляді камер розширення та звужування, в яких можуть бути перегородки з резонансними відростками. На судах, як правило, використовують однокамерні та двухкамерні глушники. Двухкамерні глушники забезпечують більш широку полосу заглушення, ніж однокамерні і при різній довжині камер практично не мають провалів частотної характеристики.

У тих випадках, коли необхідно отримати широку полосу заглушення, використовують глушники, які складаються із розширюючих камер, які облицьовуються звукопоглинаючим матеріалом. Окрім того, можуть використовуватися складові глушники, які складаються з комбінації активних та реактивних глушників. Зниження шуму складовими глушниками визначається підсумовуванням ефективності усіх вхідних в нього елементів.

Архітектурно-плановані заходи повинні проводитися на стадії проектування нових військово-промислових об’єктів та враховувати характер місцевості, споруд та зелених насаджень, які суттєво впливають на розповсюдження звуку від об’єктів. Величини зниження рівня акустичного сигналу земними насадженнями та спорудами наведені у таблиці 1.5.2.

Таблиця 1.5.2

Вид забудови або озеленення	Зниження рівня сигналу, дБ
Використання природного рельєфу та споруд-екранів	7-25
Багаторядні посадки дерев	4-5
Розташування джерел сигналів у виїмках	10-20
Споруди-екрани спеціальної конструкції	10-30

Засоби зменшення потужності та викривлення спектру акустичних сигналів призначені для часткового зниження або посилення рівня звуку, викривлення окремих дільниць спектру випромінювання або зміні напрямку випромінювання.

До цих засобів відносяться глушники звуку, пристрої створення водних та газових завіс, розсіювачі струменю, екрани.

Глушники звуку призначені для часткового зниження рівня акустичного сигналу. Зазвичай вони можуть використовуватися при випробуваннях двигунів авіаційної та бронетанкової техніки у якості стовбурних шумогасячих насадок для знарядь. Ефективність цих пристроїв складає 10-20 дБ.

Засоби створення газових та водяних завіс використовується при випробуваннях ракетних та авіаційних двигунів. Ці засоби призначені для зниження рівнів дискретних складових у спектрі або загального зниження рівня сигналу за рахунок охолодженя газової струї. Зниження рівня дискретних складових у спектрі акустичного шуму ракетного двигуна забезпечується шляхом встановлення з одного боку газового струменя двигуна завіси з газу, швидкість звуку якої відрізняється від швидкості звуку в навколишньому середовищі.

Водяні завіси використовуються шляхом вприскування води в газовий струмень двигуна спеціальними патрубками, які розташовані поза струменем або в струмені газу. Істотне зниження рівня шуму відбувається на високих частотах. Зниження шуму за допомогою розсікачів відбувається через дроблення газового струменю на дрібні струмені, що еквівалентно гальмуванню струменю. Розсікачі встановлюються у сверхзвуковому струмені перпендикулярно потоку газу. Найкращі результати дають розсікачі із співвідношенням діаметру розсікача ло діаметру струменя 0,1-0,2. Послаблення звуку при восьми розсікачах та числі М= 3,5-4 складає 6-8 дБ. При цьому переважно знижуються низькочастотні складові спектру.

Екрани використовуються для часткового зниження рівня акустичного сигналу, який випромінюється струменем газового потоку двигуна або окремими елементами. При екрануванні сверхзвукових струменів використовують циліндричні труби, які встановлюються симетрично вісі струменя на початковій ділянці. При співвідношенні довжини труби до довжини струменю більше 5 інтенсивність звуку зменшується на 10-15 дБ. При цьому значно знижується рівень високочастотних складових акустичного спектру.

При частковому екрануванні окремих ділянок двигуна внутрішнього згоряння або двигуна в цілому рівень шуму знижується на 3-5 дБ. Як правило, на практиці застосовують спільно засоби вприскування води, розсічення струменя та екранування. Це дає змогу знизити спектральні складові акустичного поля на 45-50 дБ.

Активне приховування використовується у тому випадку, коли заходи пасивного приховування не забезпечують необхідну ефективність захисту від акустичних засобів розвідки. Воно включає: засоби створення перешкод акустичній розвідці, дезінформацію та протифазне подавлення АС.

При створенні перешкод можуть використовуватися застарілі зразки озброєння та військової техніки, а також допоміжне обладнання. Ефективність захисту при створенні перешкод вважається достатнім, якщо відношення акустичного тиску захищаємого сигналу до акустичного тиску природніх або навмисних перешкод у полосі спектру частот сигналу не перевищує встановлених норм і вимог. Значні труднощі у використанні застарілих зразків озброєння виникають при захисті об'єктів з рівнями акустичних сигналів більше 120-130 дБ. Тому вказані засоби перешкод можут використовуватися при захисті об'єктів з відносно низьким рівнем сигналів.

До допоміжних засобів активного захисту відносяться засоби перешкод типу сирен, резонаторів, гучномовних пристроїв.

Для створення маскуючих акустичних сигналів у повітряному середовищі можна використовувати гучномовці рупорного типу (25ГРД-2,5 – 8РВ, -7ВЗГ; 50ГРД-8, 100ГРД-1). У якості джерел електричного сигналу для збудження вказаних гучномовців рекомендуються підсилювачі типу Г2-1, генератори сигналів Г3-34, ИГ-52, ГСМ.

Характеристики вказаних пристроїв представлені в табл. 1.5.3.

Таблиця 1.5.3

Тип прибору	**Номінальна потужність, Вт**	**Полоса відтворення частот, Гц**	**Середній звуковий тиск, Н/м^2**
ГУЧНОМОВЦІ:			
25 ГРД-2	25	100-6000	0,8
25 ГРД-5	25	500-3500	1,5
25 ГРД-8РВ	25	500-4000	1,2
25 ГРД-7В3Г	25	500-4000	1,2
50ГРД-8	50	120-6000	0,7
100РГД-1	100	120-5500	1,5
ПІДСИЛЮВАЧІ:			
ТУ-50М	50	600-8000	
ТУ-100М	100	60-8000	
ТУ-600	600	60-8000	
ГЕНЕРАТОРИ ШУМУ НИЗЬКОЇ ЧАСТОТИ:			
Г2-1 (ГШН-1)		50-6*10^6	

Г2-37		50-6,5*10^6	
ГЕНЕРАТОР СИГНАЛІВ НИЗЬКОЇ ЧАСТОТИ			
Г3-34	0,5	20-20*10^6	
ІМПУЛЬС-ГЕНЕРАТОРИ			
ИГ-52		(1-100) 10^3	
ГСМ	100, 300, 1000	300-100*10^3	

До особливих засобів активного захисту відноситься дезінформація, яка об'єднує як організаційні, так і технічні заходи. Сутністю дезінформації є навмисне випромінювання штучних акустичних сигналів, в яких містяться хибні технічні параметри або будь-яка змістовна інформація з метою ввести в оману розвідку ймовірного противника.

До засобів захисту можна віднести також методи протифазного подавлення акустичного сигналу, який забезпечується електроакустичної системою, яка складається із мікрофонів, які сприймають акустичні сигнали, посилювача та динаміка. Ця система має регулюєму фазову характеристику посилювача та створює гасячу звукову хвилю в протифазі з акустичною хвилею, яка несе закриту інформацію.

З метою зниження витрат на активні засоби захисту рекомендується розположити виробничі корпуси з високим рівнем шумів поблизу межі охороняємої території.

1.5.2 ЗАХИСТ ОБ'ЄКТІВ ВІД ГІДРОАКУСТИЧНОЇ РОЗВІДКИ.

Заходи по захисту від гідроакустичних засобів розвідки направлені на введення противника в оману відносно призначення, типу та місця знаходження надводних суден (НС), підводних човнів (ПЧ) та інших обєктів, що знаходяться у водному середовищі або на його поверхні; спектральних і енергетичних характеристик власних шумів НС та ПЧ, мінно-торпедного озброєння; призначення, тактико-технічних характеристик активних гідроакустичних засобів (ГАЗ) виявлення, зв'язку, перешкод та навігаційного гідроакустичного обладнання морських полігонів.

1.5.2.1 Гідроакустичне маскування НС та ПЧ.

При захисті від гідроакустичної розвідки здійснюється цілий ряд специфічних заходів, які використовують особливості фізичних явищ, що властиві гідроакустичним полям.

Специфічні організаційні заходи по приховуванню об'єктів від гідроакустичної розвідки спрямовані: на зниження власних шумів цих об'єктів та інтенсивності відбитих від них сигналів активних засобів гідроакустичної розвідки; підвищення прихованості роботи встановленних на об'єктах гідролокаторів, засобів звукопідводного зв'язку та гідроакустичних перешкод. Вони включають:

- вибір маршрутів руху НС та ПЧ подалі від можливих місць розміщення засобів гідроакустичної розвідки та з урахуванням гідрографічних і гідроакустичних характеристик акваторії;

- встановлення конкретного порядку використання активних гідроакустичних засобів;

- введення обмежень на параметри гідроакустичних сигналів, які випромінюються;

- суворе виконання встановлених правил використання засобів звукопідводного зв'язку;

- дотримання вимог, які пред'являються до «охороняємих від гідроакустичної розвідки акваторії», тобто гарантоване виключення можливості знаходження у межах охороняємої акваторії будь-яких засобів розвідки;

- легендування (спосіб захисту інформації від технічних розвідок, який передбачає навмисне розповсюдження та підтримку неправдивої інформації про функціональне призначення об'єкта захисту) суднобудівельних та судоремонтних заводів, випробувальних баз та випробувань, які проводяться;

- раціональний вибір акваторії для проведення випробувань об'єктів.

При раціональному виборі акваторії для проведення випробувань необхідно прагнути, щоб акваторія:

- знаходилась у закритій зоні або була максимально віддалена від дозволених маршрутів проходу іноземних судів;

- була закритого або полузакритого типу, тобто представляла собою озеро чи залив з якомога більш вузькою горловиною (вхідними воротами);

- мала достатньо складну конфігурацію берегової лінії та природні звукоізолюючі перешкоди (острови, отмелі, миси і т.п.) на найбільш небезпечних напрямах розповсюдження демаскуючих випромінювань;

- характеризувалася в основному м'яким грунтом (іл, пісок і т.п.);

- мала добрі природні звукопоглинаючі пастки у вигляді вузьких берегових клинів у напрямах можливої орієнтації демаскуючого випромінювання.

У місцях постійного проведення випробувань і на акваторіях, межі яких мають невелику протяжність, рекомендується установка стаціонарних берегових огорож, бонових загорож уздовж водної межі, сигналізації.

У місцях епізодичного проведення випробувань і на акваторіях значної протяжності рекомендується проводити патрулювання.

До числа основних технічних заходів, які дозволяють здійснити гідроакустичне маскування НС, ПЧ та мінно-торпедного озброєння можна віднести:

1. заходи по зниженню шумності НС і ПЧ;
2. заходи противогідролокаційного маскування, які полягають у зменшенні сили цілі та використанні гідрологічних особливостей районів плавання;
3. дезінформаційні заходи з застосуванням хибних гідроакустичних цілей та імітаторів;
4. створення активних перешкод гідроакустичним засобам розвідки.

Зниження шумності НС та ПЧ.

Задача зниження шумності НС та ПЧ є однією з найбільш актуальних та складних задач сучасного військового суднобудування. Випробування в області зниження власних шумів НС та ПЧ ведуться за багатьма нарямками і носять комплексний характер.

Як показують результати випробувань, зниження рівня власних шумів може бути досягнутий наступними основними способами:

- підвищенням критичної швидкості НС та ПЧ шляхом використання співвісних гвинтів, низькообертних гребних гвинтів великого діаметру;

- підвищенням точності виготовлення гребних гвинтів та монтажу валу;

- застосуванням малошумових гребних гвинтів спеціальної конструкції та ліквідацією так званого «співання» гвинта;

- раціональним розміщенням механізмів;

- зменшенням безпосереднього шумовипромінювання працюючих механізмів за рахунок врівноваження рухомих мас, покращення обробки зубчатих передач, зниження ваги рухомих складових та установки звукопоглинаючих кожухів на двигуни;

- використанням жорстких масивних фундаментів для установки машин та механізмів;

- зниженням рівня структурних шумів шляхом установки механізмів на амортизатори та звукоізольовані фундаменти і шляхом усунення жорстких зв'язків механізмів з корпусом;

- зниженням рівня відбитих шумів за допомогою пористих або волокнистих облицьовок для внутрішніх поверхонь машинних відділень;

- глушінням шумів вихлопних та всмоктуючих систем.

Застосування перерахованих заходів може забезпечити зниження шумності головних та допоміжних механізмів у діапазоні частот 500-2000 Гц на 20-25 дБ.

У якості одного із основних шляхів зниження шумності торпедних атомних підводних човнів можна відмітити переход до елетроруху. На цих човнах турбоелектричний агрегат повинен виробляти електроенергію для двигуна, який обертає гребні гвинти. При цьому виключається необхідність у зубчатому редукторі, який є основним джерелом шумів атомних підводних човнів. Відмова від кріплення механізмів та іншого обладнання безпосередньо до корпусу може забезпечити човну малу шумність на швидкості ходу до 25 вузлів.

На більшій частині атомних підводних човнів американського флоту встановлюються одновальні енергетичні установки. Ведуться пошуки вигідної форми гвинтів. Великі сподівання на співвісні гвинти, які конструктивно представлють собою два гвинти з протилежним кроком, які обертаються на загальній осі.

Однією із особливостей сучасних підводних човнів є їх дуже мала шумність. Серед заходів та технічних рішень, які забезпечують зниження шумності, вказується також на вибір більш сучасної форми корпусу, застосування подвійного корпусу, який створює додатковий повітряний звукопоглинаючий прошарок, широке застосування у елементах конструкції звукопоглинаючих матеріалів. Ядерна енергетична установка нових човнів має водяне охолодження при природній циркуляції води.

Тактичні заходи по зниженню шумності ПЧ передбачають рух у районах патрулювання малими ходами та на глибині, на якій кавітаційні шуми є мінімальними, припинення роботи сильно шумлячих допоміжних механізмів, надійне кріплення предметів на палубі і у надбудовах, підтримання у справності ліній гребних валів, обмеження використання гідроакустичних засобів в активному режимі та ін. Так, наприклад, підводні човни американського флоту на глибині 120 м мають здатність бути малошумними на швидкості ходу до 15 вузлів.

ЗМЕНШЕННЯ СИЛИ ЦІЛІ.

Приховування надводних суден та підводних човнів від гідролокаційних засобів розвідки досягається прийняттям заходів протигідролокаційного маскування, які полягають у зменшенні *сили цілі* (це результат, який можна отримати одразу, якщо прийняти рівними нулю суму робіт усих сил) та використанні гідрологічних особливостей районів плавання.

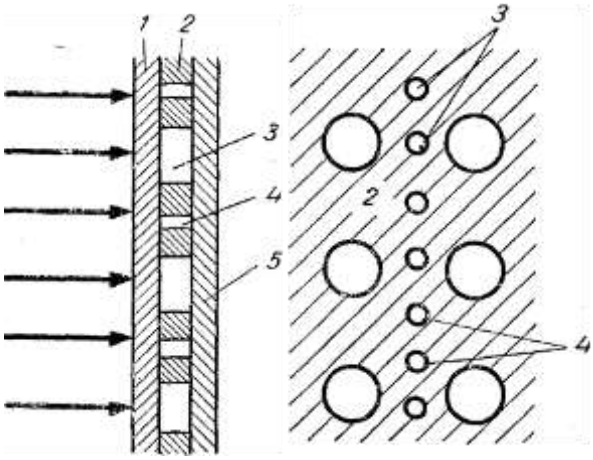
Зменшення сили мети надводних та підводних об'єктів може бути досягнуте різними методами.

Відомо, що сила мети малої сфери або будь-якого рівного об'єкта на низькій частоті залежить тільки від об'єму об'єкта. Тому на низьких частотах, коли довжина хвилі акустичного випромінювання велика у порівнянні з розмірами об'єкта, єдиним можливим методом зниження сили мети є зменшення об'єму цілі. Звідси виходить, що для тіла, розміри якого малі у порівнянні з довжиною хвилі, ніякі зміни форми тіла, так само як і ніякі покриття, не є ефективним засобом зниження сили мети.

Однак, у випадку малих довжин хвиль, це можливо здійснити наприклад, зміною форми тіла (якщо це можливо). Тобто необхідно виключити із конструкції елементи, у яких радіус кривизни прямує до нескінченності – пласкі пластини та циліндри. Форма тіла повинна бути рівною, без виступів, отворів та полостей, які діють як розсіювачі звуку.

Наступний спосіб зменшення сили мети об'єкта полягає у використанні поглинаючих покриттів різних типів.

Звукопоглинаючі покриття представлють собою слої матеріалів, які приклеюються або кріпляться до об'єкта з метою зниження інтенсивності ехо-сигналів від нього. Найбільш важливим є в'язкопоглинаюче покриття, яке послаблює звук, що досягає мети та відбивається від неї, у процесі в'язкого перетворення його енергії в тепло. Прикладом такого типу покриття може слугувати резина з металічними присадками, у якій найдрібніші повітряні полості у поєднанні з металічними часточками викликають здвигову деформацію резини та призводять до втрати енергії акустичного поля у результаті перетворення його в тепло.



На малюнку зліва показано *протигідролокаційне покріття*, де 1 – зовнішній суцільний шар резини; 2 – внутрішній перфорований шар резини; 3 – великі отвори; 4 – малі отвори; 5 – корпус підводного човна).

Зовнішній шар суцільний, внутрішній має отвори різного діаметру. Комбінація отворів створює коливальні контури, які поглинають енергію ультразвукових коливань. Недоліком резонансних поглинаючих покриттів є залежність їх коефіцієнта поглинання від температури та тиску навколишнього середовища.

Покриття із змінними параметрами складається з клинів та конусів з великими втратами; вершини цих елементів направлені у бік приходу падаючої звукової хвилі. Прикладом такого покриття є конструкція із древесно-опилочного матеріалу «інсулькрета»,

яка використовується для облицювання заглушеного басейну. Для гідроакустичних цілей цей матеріал дуже масивний та крихкий.

Компенсаційне покриття складається із шарів акустично твердих та акустично м'яких матеріалів, які чергуються, відбиваючих звук із протилежними фазовими здвигами; при цьому звук не повертається від цілі до джерела. Нажаль, повна компенсація має місце лише при нормальному падінні, у інших напрямках це явище виражене слабо або взагалі не спостерігається.

«Чвертьхвильовим шаром» називається покриття товщиною $\lambda/4$, яке має акустичний імпеданс, що дорівнює середньому геометричному імпедансів матеріалів по обидві боки шару, наприклад імпедансів води та сталі. Однак таке покриття ефективне тільки на одній частоті (на її непарних гармоніках) при нормальному падінні, що робить його некорисним для практичного застосування у гідроакустиці.

У сучасних умовах в якості матеріалу для виготовлення покриття можуть використовуватися нейлон, поліетилен, поліпропілен та різні пластмаси, які містять каучук. Із останніх найкращою вважають поліхлоропренову пластмасу із вмістом чорної сажі, якій властиві необхідні акустичні властивості, порівняно недорогу та маслостійку.

Тактичними заходами по протигідролокаційному маскуванню є використання гідрологічних особливостей районів плавання.

Враховуючі розподілення температури води на різних рівнях можна вибрати вигідну глибину, на якій підводний човен важко виявити. Літом, коли нижчі шари води холодніші за верхні та звукові промені відхиляються униз, найбільша прихованість досягається на малих глибинах. Зимою навпаки, нижчі шари води тепліші верхніх та звукові промені відхиляються до поверхні моря. Тому підводний човен узимку важче виявити на великій глибині.

Вважається, що підводному човну, який має більшу глибину занурення, легше знайти різні температурні шари води, на межах яких створюється звуковий бар'єр, який перешкоджає розповсюдженню імпульсів гідролокаторів противника та викривляє їх напрямок. Із збільшенням глибини занурення підвищуються безшумні швидкості ходу підводного човна та збільшуються перешкоди роботі гідролокаторів.

ДЕЗІНФОРМАЦІЙНІ ТЕХНІЧНІ ЗАХОДИ.

Заходи по технічній дезінформації спрямовані на введення гідроакустичної розвідки противника в оману відносно дійсного призначення та характеристик приховуємих надводних і підводних об'єктів. Дезінформаційні заходи забезпечуються за допомогою хибних гідроакустичних цілей та імітаторів.

Велику увагу приділяють створенню імітаторів підводних човнів. Такі імітатори в умовах мирного часу є ефективним засобом забезпечення бойової підготовки протичовнових сил, а у військовий час можуть використовуватися у якості одного із засобів гідроакустичної протидії, відволікаючи сили противника на хибні напрямки.

Сучасні самоходні імітатори підводних човнів – складні та довершені технічні пристрої. Вони можуть відворювати як первинні - шумові, так і вторинні – відбите акустичні поля підводного човна, імітувати кільватерний струмінь, який відбиває акустичні хвилі, а деякі зразки імітаторів можуть відтворювати і інші фізичні поля підводного човна, наприклад магнітне. Імітатори можуть здійснювати довготривале маневрування по заданій програмі. Все це робить їх вельми ефективними засобами гідролокаційної протидії.

Прикладом подібного пристрою може слугувати імітатор типу 21В12 ВМС США. Цей імітатор може використовуватися з надводних суден, вертольотів та підводних човнів і має форму малогабаритної торпеди. Його основні тактико-технічні дані: довжина 3,3 м, діаметр корпусу 0,25 м, максимальний діаметр 0,35 м, маса 155, ,6 кг, швидкість ходу 8 вузлів,

максимальний час роботи 2 год, глибина ходу (регулюємо) в межах від 15 до 122 м, діапазон робочих частот при імітації шумів від 0,1 до 10 кГц, при ретрансляції посилок гідролокаторів та вибухів від 8 до 30 чи від 3 до 7 кГц. Шуми, які створюються приладом, можуть виявлятися кораблями на дистанції до 4-5 км. Дальність дії приладу при ретрансляції посилок гідролокаторів залежить головним чином від випромінюваної ними потужності.

У США розроблений та прийнятий на озброєння більш удосконалений імітатор типу Мк 30. Цей імітатор має корпус із алюмінієвих сплавів, розділених на п'ять основних відсіків. Акустичні антени, що розташовані по дві з кожного борту, забезпечують прийом та ретрансляцію посилок гідролокаторів у широкому діапазоні частот. Швидкість ходу і характер маневрування імітатора у напрямку та глибині визначається попередньо розробленою програмою, яка може бути складена та нанесена на перфострічку безпосередньо у корабельних умовах перед кожним використанням приладу.

Джерелом живлення імітатора слугують срібно-цинкові акумулятори. Оскільки в імітаторі використовується двигун з постійним числом обертів, то регулювання швидкості у широках межах досягається подаванням на нього напруги у вигляді імпульсів, тривалість та інтервали між якими задаються програмними пристроями.

На данному етапи у світі розглядаються питання створення імітації великої підводної цілі шляхом насиченя бульбашками повітря кільватерного струменю самоходного носія. Для збільшення часу, у період якого бульбашки залишаються нерозчиненими у воді, передбачається створювати для них полімерні оболонки та заповнювати їх спеціальною речовиною, яка зменшить швидкість спливання на поверхню.

Вважається, що з появою атомних підводних човнів виникла необхідність створення більш досконалого імітатора з підвищенною швидкістю ходу, глибиною занурення, рухливістю, здатного імітувати відбиті сигнали та фізичні характеристики сучасних підводних човнів. При цьому однією із проблем є проблема імітації реальних шумів підводного човна, які пеленгуються всіма типами пасивних гідроакустичних станцій.

За існуючими поглядами передбачається, що при використанні самоходних імітаторів їх виставленню повинне передувати подавлення приймального тракту гідролокатора противника активними перешкодами. Тоді момент і сам факт виставлення імітатора може залишитися непоміченим противником, і імітатор, який виходить за межі сектору перешкод, з більшою ймовірністю зможе привернути до себе увагу протичовникових сил противника та відволікти їх на хибний напрямок, полегшуючи тим самим відрив підводного човна від переслідування.

СТВОРЕННЯ АКТИВНИХ ПЕРЕШКОД ГІДРОАКУТИСЧНИМ ЗАСОБАМ.

Застосування активних перешкод є достатньо ефективним способом гідролокаційної протидії.

Засоби створення перешкод апаратурі гідроакустичної розвідки поділяються на наступні:

- передавачі активних загороджувальних перешкод;
- допоміжні засоби флоту;
- збудники вібрацій корпусу судна.

Передавачі активних загороджувальних перешкод виконуються у мобільному та стаціонарному варіантах. Мобільний варіант використовується для створення перешкод у швидкоплинному середовищі, наприклад, при переходах кораблів. Для цього передавачі

вистрілюються із торпедних апаратів. Вони забезпечують створення загороджувальних перешкод в діапазоні від 0,5 до 85 кГц.

Стаціонарний варіант застосовується для закриття випробувальних акваторій суднобудівних заводів. Для цього передавачі перешкод встановлюються на вході у випробувальні акваторії та забезпечують створення загороджувальних перешкод в діапазоні частот від 1 до 40 кГц. Потужність випромінювання таких передавачів перешкод складає 50-100 кВт.

Під час переходів морем або при проведенні неакустичних випробувань ПЧ та НС широко застосовуються допоміжні засоби флоту: кораблі, які не мають приховуючи характеристик, гідроакустичні буксуючі трали. В цьому випадку допоміжні засоби флоту розташовуються поміж випробувальним судном та можливим місцеположенням засобів гідроакустичної розвідки, власним гідроакустичним шумом приховують гідроакустичне поле захищаємого судна.

Збудники вібрацій корпусу судна забезпечують штучне викривлення характеристик гідроакустичного поля НС і ПЧ. Збудники вібрацій корпусу судна можуть бути електродинамічними (електромолоток), механічними, гідравлічними, пневматичними. Потужність випромінювання збудників може бути у межах 2-1000Вт, діапазон генеруємих частот 4-1000 Гц у зеалежності від типу збудника.

При проведені акустичних випробувань суден і ГАЗ, коли основною метою випробувань є отримання невикривлених характеристик гідроакустичного поля, випробувальні полігони закриваються суднами-постачальниками перешкод. Для цього передавачі перешкод розміщуються по дузі кола, центром якої є випробувальний об’єкт. Радіус дуги, на якій виставляються судна з передавачами перешкод, вибирається таким чином, щоб рівень перешкоджальних сигналів у місці ймовірного розташування апаратури розвідки був вищий за рівень захищаємих випромінювань. Відстань між суднами із засобами перешкод по дузі кола вибирається таким чином, щоб була виключена можливість кутової селекції випробувального засобу та суден-постачальників перешкод. Для виключення просторово-часового розділення інформаційних сигналів та перешкод, робота ГАЗ та засобів перешкод синхронізується системою програмного забезпечення.

1.5.2.2 Маскування сигналів гідроакустичних засобів.

Охороняємі параметри ГАЗ, інформацію про які можна отримати, використовуючи гідроакустичне поле, модна розділити на дві групи:

- параметри, пов’язані із зміною рівня сигналу (акустична потужність, характеристики спрямованості випромінювача, звуковий тиск);

- параметри, пов’язані із зміною частотно-часових характеристик (несуча частота, тривалість імпульсу, спектральний склад, сквапність і т.п.).

Одним із основних способів захисту ГАЗ на всіх етапах їх створення повинно бути приховування гідроакустичного сигналу.

Приховування повинно виключати або значно ускладнювати виявлення та вимірювання переховуємих характеристик ГАЗ, визначення характерних особливостей підприємств та виконуємих ними робіт шляхом усунення або послаблення їх демаскуючих ознак. З цією метою у першу чергу необхідно максимально використовувати маскуючи властивості районів випробувань та акустичні властивості споруд, будівель та конструкцій.

Заходи по приховуванню гідроакустичних сигналів проводяться на етапах проектування, випробувань, виготовлення та експлуатації ГАЗ. Наприклад, у процесі проектування та розробки приймаються технічні заходи для звужування діаграми спрямованості гідроакустичної антени та усуненню або зменшенню рівня бокового

випромінювання; введеню декількох режимів роботи по випромінюваній потужності, кодуванню випромінюваних сигналів.

У процесі натурних випробувань та при експлуатації ГАЗ повинні проводитися наступні захисні заходи:

- застосування природніх пасивних заходів приховування;
- використання штучних пасивних засобів приховування;
- вибір місця та часу проведення робіт, випробувальних акваторій, а також конструкцій випробувальних споруд;
- зменшення енергії випромінюваних гідроакустичних сигналів та зниження їх інформативності;
- використання природних, індустріальних та цілеспрямованих гідроакустичних перешкод;
- застосування технічної дезінформації та активних перешкод.

До природних пасивних засобів приховування відносяться гідрографічні та гідрологічні особливості водного басейна, випробувальних та сдаточних баз.

Застосування для маскування гідрологічних та гідрографічних властивостей навколишнього середовища базується на використанні особливостей розповсюдження звуку у конкретних гідрологічних обставинах випробувальної акваторії. Відомо, що дальність розповсюдження звуку залежить від багатьох факторів: товщини водного шару (глибини акваторії), градієнту температури в акваторії під час проведення випробувань, солоності води, характеру берегової лінії, профілю дна, наявності островів, поглинаючих та відбиваючих властивостей донних ґрунтів, закону розширення фронту акустичної хвилі та втрат енергії хвилі внаслідок затухання звуку, рефракції звукових променів, розсіюванні звуку, реверберації і т.п. Тому місця випробування ГАЗ краще розташовувати у глибині заливів і бухт. Бажана наявність у них островів, мілин та перепадів глибини. Характер донних ґрунтів суттєво впливає на розповсюдження акустичних сигналів. Замулені або мулисто-пісчані ґрунти мають найменші відбиваючі властивості і тому більше підходять, ніж каменисті.

Значення коефіцієнтів відбиття для різних ґрунтів наведені у таблиці 1.5.2.2.1

Таблиця 1.5.2.2.1

Вид ґрунту	**Середній розмір елементарних часток ґрунту, мм**	**Коефіцієнт відбиття**
Мул	0,012	0,17
Мул – пісок	0,015	0,33
Пісок – мул	0,28	0,5
Пісок	0,26	0,51
Пісок	0,3	0,7
Пісок	0,46	0,85
Пісок	0,58	0,61

Пісок	0,59	0,41
Каменистий ґрунт	1,0	0,56
Кам’яний ґрунт	1,4	0,82

При штучних способах приховування у випадках проведення випробувань у дослідних басейнах і в баках високого тиску широке застосування знаходять звукопоглинаючі покриття. В цьому випадку усі їх внутрішні поверхні повинні бути облицьовані нерезонансними резиновими покриттями типу НППРК, що випускаються промисловістю у вигляді пластин з розмірами 500х400 мм. Ці покриття ефективно працюють в діапазоні частот 3-100 кГц.

Частотні характеристики коефіцієнтів відбиття покриттів НППРК наведені у таблиці 1.5.2.2.2.

Таблиця 1.5.2.2.2

Тип покриття	**Коефіцієнти відбиття на частотах, кГц**						
	4	**5**	**6**	**10**	**20**	**50**	**100**
НППРК-7	0,25	0,18	0,15	0,14	0,14	0,14	0,14
НППРК-4 товщина 72 мм	0,25	0,1	0,8	0,1	0,1	0,1	0,1
НППРК-4д товщина 51 мм	0,38	0,44	0,33	0,1	0,08	0,09	0,09

При проведенні випробувань ГАЗ на акваторіях для ізоляції їх від «відкритої» води може бути рекомендоване використання молів, дамб та створення бульбашкових завіс. У якості джерел бульбашкових завіс можут використовуватися трубки з отврами не більше 0,25 мм, які прокладаються по дну водойми у найбільш вузькому місці акваторії. В трубках необхідно підтримувати значний тиск біля 1кг/см^2. Така завіса може знизити рівень акустичного сигналу на 20-30 дБ у діапазоні частот 1-20 кГЦ.

Якщо приховування гідроакустичних сигналів не забезпечує потрібного зниження рівня їх потужності, слід застосувати активне гідроакустичне маскування.

Активне маскування гідроакустичних сигналів може бути досягнуто шляхом створення загороджувальних шумових перешкод (ЗШП). У якості джерел ЗШП можуть бути використані вимірюючі гідроакустичні випромінювачі та спеціальні засоби гідроакустичних перешкод. При проведенні активного маскування можуть застосовуватися також засоби перешкод, що використовуються для гідроакустичного маскування НС та ПЧ.

Організаційні та технічні заходи по захисту від гідроакустичної розвідки вважаються ефективними, якщо відношення акустичного тиску інформативного сигналу до акустичного тиску природних або навмисних перешкод у полосі частот сигналу на межі охороняємої території (акваторії) не перевищує допустимої величини. Ця величина визначається спеціальними нормами.

1.5.3 ЗАХИСТ ОБ'ЄКТІВ ВІД СЕЙСМІЧНОЇ РОЗВІДКИ.

Сейсмічна розвідка - отримання інформації шляхом виявлення і аналізу деформаційних і зсувних полів, що виникають в грунті при різних впливах на неї. Також під цим терміном розуміють отримання інформації, яка міститься в характеристиках сейсмічних коливань, джерелом яких є об'єкт розвідки с застосуванням сейсмічної апаратури.

Сейсморозвідка зародилась у 20-ті роки XX сторіччя та використовувалась для потреб геологічної розвідки при вивченні глибинної структури земної кори. За допомогою сейсморозвідки вивчається глибинна будова Землі, виділяються родовища корисних копалин (в основному нафти і газу), вирішуються завдання гідрогеології та інженерної геології, проводиться сейсмічне мікрорайонування. Сейсморозвідка відрізняється високою роздільною здатністю, технологічністю і великим об'ємом одержуваної інформації. Якщо ми говоримо про використання сейсмічної розвідки для одержання інформації про дії супротивника обо конкурента, то насамперед сейсморозвідка використовується для фіксації ядерних випробувать, звичайних вибухів, земляних робіт при спорудженні інженерних споруд та комунікацій, розміщення технологічного устаткування, пересування транспорту та техніки, тощо.

В основі сейсмічних методів лежить збудження пружних хвиль за допомогою технічного пристрою або комплексу пристроїв - джерела. Джерело створює в товщі гірських порід надлишковий тиск, що компенсується середовищем протягом деякого часу. В процесі компенсації пов'язані частинки порід здійснюють періодичні коливання, що передаються в глиб землі пружними хвилями. Найважливішим властивістю хвилі є її швидкість, залежить від літологічного складу, стану гірських порід (тріщинуватості, виветрелості і т. Д.), віку, глибини залягання.

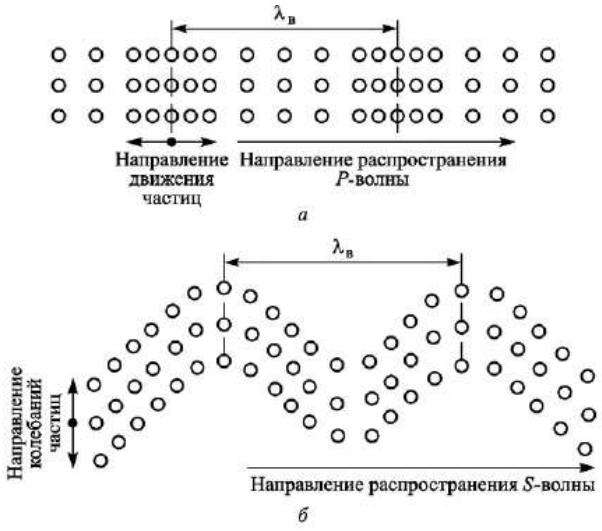
Поширюючись в обсязі гірських порід, пружні хвилі потрапляють на межі шарів з різними пружними властивостями, змінюють напрямок, кути променів і амплітуду, утворюються нові хвилі. На шляху проходження хвиль розміщуються пункти прийому, де за допомогою сейсмоприемников приймаються коливання частинок і перетворюються в електричний сигнал.

Пункти прийому, вживані для реєстрації хвиль від одного пункту збудження (джерела) утворюють «розстановку». Залежно від розмірності сейсморозвідки розстановка має форму прямої лінії (2d сейсморозвідка) або блоку паралельних приймальних ліній (3d сейсморозвідка)[2]. Графіки записаних коливань (траси) групуються в сейсмограми і аналізуються для знаходження властивостей хвиль. З отриманих сейсмограм витягається геолого-геофизическая інформація про сейсмогеологических межі. Найбільш ефективна сейсморозвідка при вивченні осадового чохла древніх платформ, оскільки його горизонтально-шарувата будова найпростіше знаходиться за сейсмічними даними. Зі збільшенням нахилу цільових геологічних меж надійність отримуваною сейсморозвідкою інформації падає.

Для збудження коливань застосовуються вибухи зарядів тротилу в неглибоких свердловинах (10-20 м) а також тривала (вібраційне) або коротка (імпульсне) ударна дія на гірські породи. Вибухові джерела характеризуються найбільшою потужністю і компактністю, при цьому вимагають дорогих підготовчих і ліквідаційних робіт, а також наносять великий ущерб довкіллю. У 1956-88 році в СРСР, Індії, та інших странах «членах ядерного клубу» використовувалися так звані "мирні" підземні ядерні вибухи для цілей глибинного сейсмічного зондування земної кори і верхньої мантії, найчастіше ці вибухи попутно вирішували питання випробування ядерної зброї. Недоліки таких вибухів – екологічна небезпека.

Невибухові джерела набагато слабкіші, але можуть використовуватися багаторазово в одній і тій же точці, більше керовані, а також безпечніше для людини і екології (таким прикладом можуть служити автомобілі-вібратори).

Джерело збуджує два типи незалежних сейсмічних хвиль - подовжні і поперечні. З подовжніми хвилями пов'язані коливання, спрямовані уздовж променя хвилі, а з поперечними - упоперек. Прямою хвилею називається подовжня або поперечна хвиля, що поширюється безпосередньо від джерела до точки спостереження. Подовжні хвилі характеризуються великими швидкостями, приходять у будь-яку точку середовища раніше поперечних, поширюються практично у будь-яких речовинах і менше.



Мал.1.5.3.1 Продольні (а), та поперечні (б) сейсмічні хвиі

Мал.1.5.3.2 Структура сейсморозвідувального каналу

Зрозуміло, що загальні заходи з захисту об’єктів від сейсмічної розвідки є тотожними до аналогічних заходів захисту від інших розвідок, які вивчалися раніше, але є деякі особливості, притаманні саме сейсмічної розвідки. Найбільш близькими за фізичною природою є акустична розвідка та гідроакустична розвідка, але в випадку сейсмічних коливань ми маемо справу з потужними джерелами коливань, зазвичай розподіленими у просторі. З урахуванням того, що коливання поширюються у горних породах на великі відстані, завдання енергетичного та інформаційного приховування являє собою дуже складну задачу. Якщо досить невеликі об’єкти – джерела коливань можна розмістити на віброізолюючому фундаменті і таким чином зменшити потужність демаскуючих сигналів, то в випадках великих об’єктів, пересуванні транспорту, роботи важкої техніки, земляних роботах це практично неможливо. Технологічні та інші вибухи, які є короткочасними та потужними сигналами взагалі неможливо послабити до необхідного рівня. Розвиток засобів захисту від сейсмічної розвідки, вочевидь, полягає в напрямках дезінформації противника та маскування ложними цілями та об’єктами.

Контрольні питання.

1. Поняття акустичної розвідки. Для вирішення яких задач застосовуються. Якими приладами.
2. Поняття гідроакустичної розвідки. Основні завдання та способи роботи.
3. Поняття сейсморозвідки. Основні завдання та способи реєстрації.
4. Які основні організаційні та технічні заходи захисту інформації від акустичної розвідки.
5. Пасивні засоби приховування акустичних сигналів. Принцип дії.
6. Архітектурно-заплановані заходи.
7. Призначення та принцип дії засобів зменшення потужності та викривлення спектру акустичних сигналів.
8. Коли використовується активне приховування. Допоміжні засоби активного захисту.
9. Призначення гідроакустичної розвідки. Організаційні заходи гідроакустичного маскування.
10. Основні технічні заходи гідроакустичного маскування. Зниження шумності НК та ПЧ.
11. Зменшення сили цілі.
12. Дезінформаційні технічні заходи.
13. Створення активних перешкод гідроакустичним засобам.
14. Маскування сигналів гідроакустичних засобів.

1.6 ОРГАНІЗАЦІЯ РОБІТ ПО ІНЖЕНЕРНО-ТЕХНІЧНОМУ ЗАХИСТУ НА ПІДПРИЄМСТВАХ І УСТАНОВАХ ДЕРЖАВНИХ І КОМЕРЦІЙНИХ СТРУКТУР.

Інтегральний підхід до забезпечення інформаційної безпеки передбачає, в першу чергу, виявлення можливих загроз, включаючи канали витоку інформації. Реалізація такого підходу вимагає об'єднання різних підсистем безпеки в єдиний комплекс, оснащений загальними технічними засобами, каналами зв'язку, програмним забезпеченням і базами даних. Тому при виявленні технічних каналів витоку інформації розглядається основне обладнання технічних засобів обробки інформації (ТЗОІ), кінцеві пристрої, з'єднувальні лінії, розподільні і комутаційні системи, обладнання електроживлення, схеми заземлення і т. п. Поряд з основними необхідно враховувати і допоміжні технічні засоби і системи (ДТЗС), наприклад пристрої відкритого телефонного, факсимільного, гучномовного зв'язку, радіофікації, годинникові механізми, електропобутові прилади і т. п.

Залежно від способів перехоплення інформації, фізичної природи збудження сигналів, а також середовища їх поширення можна виділити технічні канали витоку, канали перехоплення при передачі інформації системами зв'язку, канали витоку акустичної та видової інформації, комп'ютерні способи знімання інформації.

На мал.1.6.1. зображені наступні канали витоку інформації:

1 – витік за рахунок структурного звуку в стінах і перекриттях,

2 – знімання інформації з стрічки принтера, погано стертих дискет і т. п.,

3 – знімання інформації з використанням відеозакладок,

4 – програмно-апаратні закладки і ПК,

5 – радіозакладки в стінах і меблях,

6 – знімання інформації за системою вентиляції,

7 – лазерне знімання акустичної інформації з вікон,

8 – виробничі та технологічні відходи,

9 – комп'ютерні віруси, логічні бомби і т. п.,

10 – знімання інформації за рахунок наведень і "нав'язування",

11 – дистанційне знімання відеоінформації (оптика),

12 – знімання акустичної інформації з використанням диктофонів,

13 – розкрадання носіїв інформації,

14 – високочастотний канал витоку в побутовій техніці,

15 – знімання інформації спрямованим мікрофоном,

16 – внутрішні канали витоку інформації (через персонал),

17 – несанкціоноване копіювання,

18 – витік за рахунок побічного випромінювання терміналу,

19 – знімання інформації за рахунок використання "телефоного вуха",

20 – знімання інформації з клавіатури принтера по акустичному каналу,

21 – знімання інформації з дисплея або електромагнітного каналу,

22 – візуальне знімання інформації з дисплея і принтера,

23 – наведення на лінії комунікацій і сторонні провідники,

24 – витік через лінії зв'язку,

25 – витік колами заземлення,

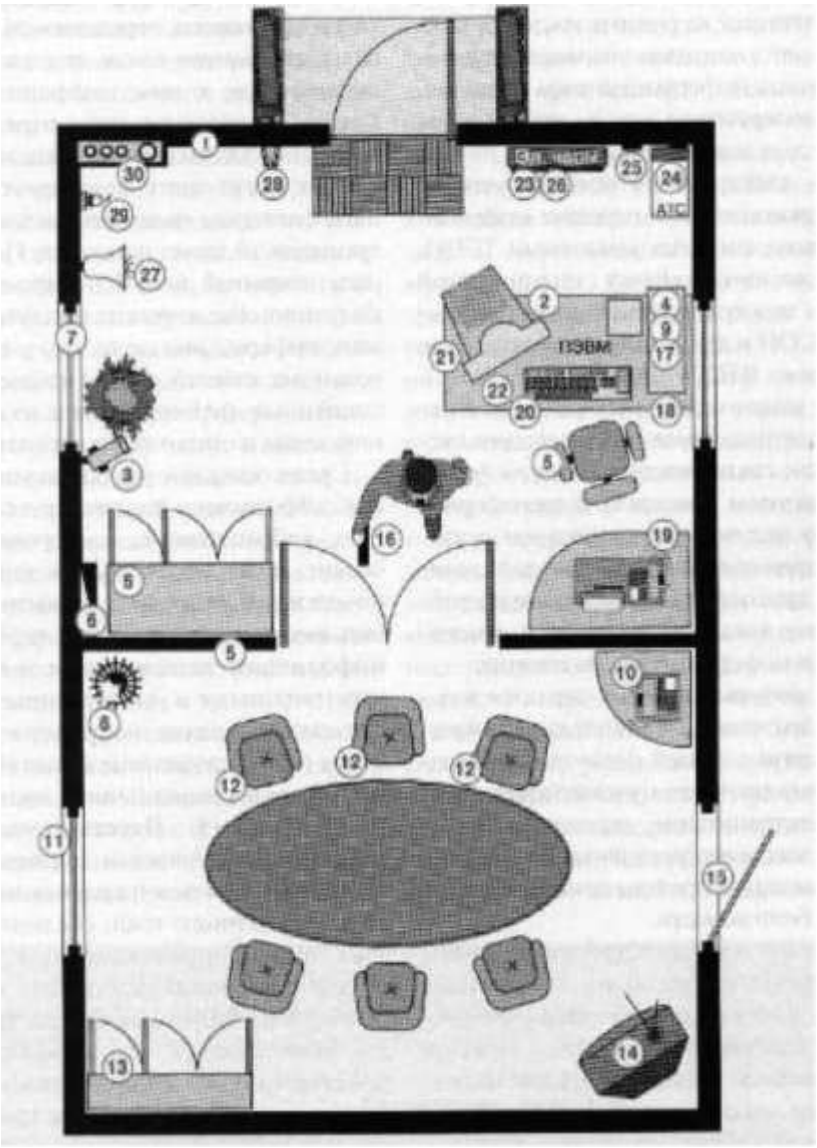
26 – витік через мережу «електронний годинник»,

27 – витік через трансляційну мережу і гучномовний зв'язок,

28 – витік через охоронно-пожежну сигналізацію,

29 – витік через мережі,

30 – витік через мережі опалення, газо-і водопостачання, електроживлення.



Мал. 1.6.1 Канали витоку інформації

Для контролю приміщень на відсутність заставних пристроїв необхідний постійний контроль відсутності в приміщеннях закладних пристроїв - свого роду «чистка». Доцільні такі види «чистки»:

• систематичний візуальний огляд приміщень;

• періодичний пошук закладних пристроїв з використанням технічних засобів;

• ретельне обстеження приміщення перед проведенням в ньому наради з обговоренням закритих тем;

• обов'язкове обстеження приміщення після капітального ремонту, переїзду в нову будівлю і т.п.;

• перевірка всіх нових предметів, що з'являються в приміщенні (представницькі подарунки, предмети інтер'єру, радіоелектронні засоби та ін.);

• періодичний радіомоніторинг приміщень протягом робочого дня.

Частота і способи перевірки приміщень з метою виявлення в них закладних пристроїв залежать від їх категорії та порядку допуску в них сторонніх осіб. Найбільшої уваги контррозвідки вимагають кабінети керівника і його найближчих заступників. З одного боку,

там часто відбуваються розмови по конфіденційним питанням, з іншого, - ці приміщення відвідують не тільки співробітники СБ, а й сторонні особи.

Пошук закладок шляхом візуального огляду полягає в ретельному огляді приміщення, меблів, електроарматури, побутових приладів, комп'ютерів, радіоприймачів, телефонів, пристроїв внутрішнього зв'язку, картин, портьєр, жалюзі, інших предметів, куди можна заховати малогабаритну закладку.

Огляд проводиться без розбирання розглядаємих предметів. Доцільно виробляти його за певною схемою, аналогічно схемі огляду місця події криміналістами: від дверей або проти годинникової стрілки, від периферії до центру приміщення. Під час огляду необхідно звертати увагу на свіжі подряпини на шпалерах, на стінах, біля мережевих і телефонних розеток, вимикачів освітлення, гвинтах корпусу телефонного апарату, на пилові сліди зміщення предметів, на відрізки проводів, на інші сліди, на предмети (і особливо їх деталі) незрозумілого призначення.

Для візуального огляду під час пошуку закладних пристроїв необхідно застосовувати недороге допоміжне обладнання, що значно підвищує ймовірність виявлення закладки. До такого обладнання відносяться драбини, ліхтарі, оглядові дзеркала, волоконно-оптичні технічні ендоскопи. Ефективність візуального огляду підвищується завдяки контролю важкодоступних місць за допомогою індикаторів поля. Для забезпечення функціонування закладки під час перевірки необхідно включити радіоприймач (телевізор) або голосно розмовляти.

Візуальний огляд кабінету керівника перед початком (або після завершення) робочого дня доцільно доручати його секретарю (який повинен бути внутрішнім агентом контррозвідки), так як він (вона) швидше будь-кого іншого помітить нові предмети, що з'явилися в кабінеті, аж до авторучки на столі. Якщо перевірка проводиться ввечері, то кабінет необхідно закривати на ніч на ключ.

Періодично (наприклад, один раз в квартал) необхідно здійснювати поглиблену перевірку приміщень для виявлення в них усіх видів закладок, особливо таких, які неможливо виявити шляхом візуального контролю. До їх числа відносяться камуфльовані і малогабаритні некамуфлірованние закладки (в тому числі провідні закладки).

Одним з важливих завдань підрозділу контррозвідки служби безпеки при підготовці до відповідальної наради є перевірка того приміщення, де вона повинна відбуватися. Глибина його «чистки» залежить від загального характеру використання даного приміщення. Якщо це спеціальне приміщення для нарад, яке закривається на ключ, опечатується печаткою, здається щодоби під охорону з відповідним записом у журналі, то контроль перед нарадою можна зробити шляхом візуального огляду з використанням засобів аналізу випромінювань. Якщо ж нарада проходить в звичайному службовому приміщенні, то обсяг перевірки повинен відповідати обсягу поглибленої перевірки.

Крім того, не можна виключити можливість наявності закладок у одного або декількох учасників наради. Тому має сенс розмістити всередині приміщення датчики відповідних приладів, а самі ці прилади можуть перебувати в сусідній кімнаті.

Капітальний ремонт приміщень завжди пов'язаний із загрозою встановлення закладок в конструктивних (або спеціально створених) пустотах в стінах, стелях, підлогах, в електроарматуру, освітлювальних і нагрівальних приладах і т.п. Постійно контролювати

робітників, які виконують ремонтні роботи, практично неможливо. Тому після капітального ремонту необхідно ретельно обстежити порожні приміщення (ще до розміщення в ньому меблів і приладів) за допомогою технічних засобів.

Меблі і всі прилади, що знаходилися в кабінеті, на час ремонту необхідно винести в інше приміщення, закрити його на ключ і опечатати. Якщо ж меблі і прилади залишалися у відремонтованому приміщенні або їх виносили в незакрите приміщення (в коридор), то необхідно перевірити кожен предмет.

Виявлені закладні пристрої найчастіше вилучають, а іноді залишають на місці для проведення дезінформаційних заходів з порушниками інформаційної безпеки.

Контрольні питання:

1. Скільки типових завдань захисту об’єктів від ТСР (ТЗРозв.). Перерахуйте.
2. Приховування, що включає. Охарактерізуйте кожну складову.
3. Дезінформація. Види, опис кожного виду.
4. Що таке маскуючий єфект, від чого залежить його ефективність, кількісні та якісні параметри.
5. Умови отримання маскуючого ефекту. Методи маскування. Класифікація.
6. Наведіть приклади методів маскування. Охаректеризуйте кожний приклад.
7. Методи енергетичного приховування.
8.

Змістовий Модуль ІІ. КОНТРОЛЬ ЕФЕКТИВНОСТІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

1.1 ОРГАНІЗАЦІЙНІ ЗАХОДИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ.

Врахувати специфіку каналу обліку і методу передачі або обробки інформації дозволяють організаційно-технічні заходи, які при цьому не вимагають для своєї реалізації нестандартних прийомів і обладнання.

1. Організація електроживлення обладнання, що обробляє цінну інформацію, від окремого джерела живлення і від загальної електромережі через стабілізатор напруги (мережний фільтр) або мотор-генератор (бажаніше).

2. Обмеження доступу сторонніх осіб всередину приміщення, в якому знаходиться обладнання, шляхом встановлення механічних запорів або замків.

3. При обробці і вводі-виводі інформації використовувати для відображення дисплеї, а для реєстрації — принтери.

4. При відправці в ремонт технічних засобів обов'язкове знищення всієї інформації, що містяться на них.

5. Розміщення обладнання для обробки цінної інформації на відстані не менше 2,5 м від пристроїв освітлення, кондиціонування, зв'язку, металевих труб, теле - і радіоапаратури, а також іншого обладнання, що використовується для обробки цінної інформації.

6. Встановлення клавіатури і друкарських пристроїв на мягкі прокладки з метою зниження відходу інформації по акустичному каналу.

7. При обробці цінної інформації на персональному комп'ютері, крім випадку передачі цієї інформації по мережі, відключення комп'ютера від локальної мережі або мережі віддаленого доступу.

8.Знищення інформації після її використання або передачі.

1.2 ОСНОВНІ НОРМАТИВНО-ПРАВОВІ ДОКУМЕНТИ З ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЇ.

Закони і підзаконні акти складають верхній ешелон документів, що регламентують правовідносини у галузі технічного захисту інформації. Вони можуть тільки концептуально визначати деякі підходи та особливості технології технічного захисту. Основний же зміст робіт з ТЗІ та оцінювання їх ефективності міститься в спеціальній нормативній документації.

Наявність комплексної, функціонально повної системи документації, що регламентує всі етапи проведення заходів ТЗІ, а також весь життєвий цикл засобів ТЗІ (розробка, виготовлення, випробування, експлуатація, ремонт, зберігання і утилізація) є досить важливим системоутворюючим фактором, що впливає на ефективність функціонування всієї системи ТЗІ в державі.

Тому створення науково обґрунтованої системи нормативних документів є досить актуальним завданням.

Хоча наразі є деяка кількість нормативних документів, які відповідають на окремі питання і дають можливість вирішувати деякі завдання за окремими напрямами ТЗІ.

Основне рішення цієї проблеми бачиться в створенні системи стандартів та нормативних документів у галузі ТЗІ. В основу класифікації цієї системи може бути покладений матричний принцип. У цьому випадку основний поділ системи стандартів і нормативних документів буде проводитися за функціональними групами: основоположні стандарти, стандарти та нормативні документи за напрямами і на продукцію, послуги, процеси і т. і. А всередині цих груп – по предметній області. За основу для предметного поділу слід взяти види технічних розвідок або, що більш обґрунтовано, види і типи носіїв інформації.

Система стандартів і нормативних документів одночасно є нормативною базою для системи сертифікації засобів ТЗІ.

Основними нормативно-правовими документами з питань захисту інформації наразі є наступні законодавчі акти, нормативно-правові акт (НПА) та нормативні акти (стосовно захисту інформації) в Україні, список не повний (до нього не входять НПА з обмеженим доступом та деякі НПА). Актуальні зміни на сайті Державної служби спеціального зв'язку та захисту інформаціїУкраїни: http://www.dstszi.gov.ua (Розділ нормативно-правова база).

1. **Закони України:**
   - Закон України «Про інформацію» від 02.10.1992 № 2657-XII
   - Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
   - Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
   - Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
2. **Постанови КМУ:**
   - Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
   - Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893
3. **Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ**:
   - НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
   - Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.
   - НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
   - НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
   - НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

- НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
- Автоматизированные системы. Требования к содержанию документов РД 50-34.698.
- Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89.
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

4. **Галузеві стандарти:**
   - ГСТУ СУІБ 1.0/ISO/IEC 27001: Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD).
   - ГСТУ СУІБ 2.0/ISO/IEC 27002: Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD).

1.3 ОСНОВНІ КЕРІВНІ ДОКУМЕНТИ ПО ЗАХИСТУ ПІДПРИЄМСТВ І УСТАНОВ ВІД ІНОЗЕМНОЇ ТЕХНІЧНОЇ РОЗВІДКИ.

Керівні документи по захисту підприємств і установ від іноземної технічної розвідки, в залежності від джерела походження розділяють на: закони, які приймає ВР України, укази президента України, постанови та розпорядження Кабінета міністров України, накази керівників відповідних державних установ, державні стандарти та норми, документи судової практики, кодекси. Слід пам'ятати, що нормативна база постійно змінюється, тому слід ретельно вивчати як основні засади вимог сучасного законодавства так і зміни у нормативно-правової площини захисту інформації, які необхідно відслідковувати у офіційних виданнях.

Всі закони та норматині акти розроблюються на основі Коституції України, яка відображає основні засади побудови держави.

Нижче наведен актуальний перелік законів України та указів президента, які мають безпосередне відношення до захисту інформації:

Закон України "Про Державну службу спеціального зв'язку та захисту інформації України"

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"

Закон України "Про Національну систему конфіденційного зв'язку"

Закон України "Про інформацію"

Закон України "Про телекомунікації"

Закон України "Про радіочастотний ресурс України"

Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки"

Закон України "Про державну таємницю"

Закон України "Про ліцензування певних видів господарської діяльності"

Закон України "Про електронні документи та електронний документообіг"

Закон України "Про наукову і науково-технічну експертизу"

Закон України "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання"

Закон України "Про ратифікацію Статуту і Конвенції міжнародного союзу електрозв'язку"

Закон України «Про електронний цифровий підпис», від 22.05.2003 № 852-IV

Закон України «Про електроні документи та електронний документообіг», від 22.05.2003 № 851-IV

Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», від 05.04.2007 № 877-V

Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI

Закон України «Про доступ до публічної інформації», від 13.01.2011 № 2939-VI

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 80/94-ВР

Закон України «Про засади державної мовної політики», від 03.07.2012 № 5029-VI

Закон України «Про основні засади забезпечення кібербезпеки України»

Указ Президента України від 30.06.2011 № 717/2011 "Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України"

Указ Президента України від 22.05.1998 № 505 "Про Положення про порядок здійснення криптографічного захисту інформації в Україні"

Указ Президента України від 27.09.1999 № 1229 "Про Положення про технічний захист інформації в Україні"

На підставі основних законів розроблюються подальші документи, з якіх складається нормативна-правова база з питань захисту інформації. На сайті Держспецзв'язку оприлюднено «Інформаційний перелік документів Фонду нормативних документів у сфері технічного та криптографічного захисту інформації», якій містить необхідні актуальні нормативні документи по напрямкам.

1. Загальні питання організації та функціонування системи технічного захисту інформації

Закони України

Закон України „Про Державну службу спеціального зв'язку та захисту інформації України".
Закон України „Про інформацію".
Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".
Закон України „Про державну таємницю".

Закон України „Про захист персональних даних”.
Закон України „Про доступ до публічної інформації”.
Закон України „Про основи національної безпеки України”.

Укази, постанови, розпорядження Верховної Ради України, Президента України, Кабінету Міністрів України, накази Адміністрації Держспецзв’язку

Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.

Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011.

Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.

Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.

Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. Наказ Адміністрації Держспецзв’язку від 22.03.2007 № 36, зареєстрований в Міністерстві юстиції України 04.04.2007 за № 312/13579.

Державні стандарти України, нормативні документи системи ТЗІ, стандарти та нормативні документи колишнього СРСР

ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.
ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

2. Вимоги до захисту інформації

Накази Адміністрації Держспецзв’язку, нормативні документи системи ТЗІ

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною №1).

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2".

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.

НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99

3. Нормування порядку захисту інформації

3.1 Протидія технічним розвідкам

НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення.

3.2 Захист інформації в інформаційно-телекомунікаційних системах

Закони України

Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".

Постанови Кабінету Міністрів України

Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.1998 № 121.

Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180.

Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772.

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інфор-маційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.

Накази Адміністрації Держспецзв'язку

Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.

Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 10.04.2008 № 94, зареєстрований в Міністерстві юстиції України 07.07.2008 за № 603/15294.

Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 04.07.2008 № 112, зареєстрований в Міністерстві юстиції України 25.07.2008 за № 690/15381.

Нормативні документи системи ТЗІ, стандарти та нормативні документи колишнього СРСР

НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною №1).

НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ГОСТ 28195-89 Оценка качества программных средств. Общие положения.

ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде.

3.3 Захист інформації на об’єктах інформаційної діяльності

НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215

Державні стандарти України, нормативні документи системи ТЗІ

ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки.

НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

4. Дозвільна діяльність у сфері технічного захисту інформації

4.1 Ліцензування видів господарської діяльності в галузі ТЗІ

Закони України

Закон України „Про ліцензування певних видів господарської діяльності”.

Закон України „Про основні засади державного нагляду (контролю) у сфері господарської діяльності”.

Постанови Кабінету Міністрів України.

Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню. Постанова КМ України від 18.05.2011 № 517.

Перелік документів, які додаються до заяви про видачу ліцензій для окремого виду господарської діяльності. Постанова КМ України від 04.07.2001 № 756.

Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу. Постанова КМ України від 29.11.2000 № 1755.

4.2 Порядок надання дозволів на проведення робіт з ТЗІ для власних потреб

Накази Адміністрації Держспецзв’язку

Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533.

4.3. Ліцензійні умови провадження господарської діяльності з надання послуг у галузі технічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України), та Порядок контролю за додержанням Ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації інформації (згідно з переліком, що визначається Кабінетом Міністрів України).

Накази Адміністрації Держспецзв’язку

Наказ Адміністрації Держспецзв’язку від 14.10.2014 № 532 «Про затвердження Ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України), та Порядку контролю за додержанням Ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту інформації інформації (згідно з переліком, що визначається Кабінетом Міністрів України)

5. Оцінка якості робіт та послуг у галузі технічного захисту інформації

5.1 Сертифікація

Закони України

Закон України „Про підтвердження відповідності".

Закон України „Про акредитацію органів з оцінки відповідності".

Закон України „Про стандарти, технічні регламенти та процедури оцінки відповідності".

Закон України „Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання".

Постанови Кабінету Міністрів України

Про стандартизацію і сертифікацію. Декрет КМ України від 10.05.1993 № 46-93.

Положення про порядок надання суб'єктам зовнішньоекономічної діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю. Постанова КМ України від 08.06.1998 № 838.

Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання. Постанова КМ України від 28.01.2004 № 86.

Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів військового призначення. Постанова КМ України від 20.11.2003 № 1807.

Про затвердження Порядку здійснення процедури призначення органів з оцінки відповідності продукції, процесів і послуг вимогам технічних регламентів. Постанова КМ України від 24.01.2007 № 59.

Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів. Постанова КМ України від 13.03.2002 № 288.

Накази Адміністрації Держспецзв'язку

Про затвердження порядку надання висновків і погодження експорту та тимчасового вивезення товарів військового призначення і подвійного використання, які належать до криптографічних систем, засобів криптографічного та технічного захисту інформації або містять у своєму складі такі засоби. Наказ Адміністрації Держспецзв'язку від 11.03.2011 № 53, зареєстрований в Міністерстві юстиції України 01.04.2011 за № 437/19175.

Правила проведення робіт із сертифікації засобів захисту інформації. Спільний наказ Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 № 75/91, зареєстрований в Міністерстві юстиції України 14.05.2007 за № 98/13765.

Державні стандарти України

ДСТУ 2462-94 Сертифікація. Основні поняття. Терміни та визначення.

ДСТУ 3410-96 Система сертифікації УкрСЕПРО. Основні положення.

ДСТУ 3411-96 Система сертифікації УкрСЕПРО. Вимоги до органів з сертифікації продукції.

ДСТУ 3412-96 Система сертифікації УкрСЕПРО. Вимоги до випробувальних лабораторій.

ДСТУ 3413-96 Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції.

ДСТУ 3414-96 Система сертифікації УкрСЕПРО. Атестація виробництва. Порядок проведення.

ДСТУ 3415-96 Система сертифікації УкрСЕПРО. Реєстр Системи.

ДСТУ 3416-96 Система сертифікації УкрСЕПРО. Порядок реєстрації об'єктів добровільної сертифікації.

ДСТУ 3417-96 Система сертифікації УкрСЕПРО. Процедура визнання результатів сертифікації продукції, що імпортується.

ДСТУ 3418-96 Система сертифікації УкрСЕПРО. Вимоги до аудиторів та порядок їх атестації.

ДСТУ 3419-96 Система сертифікації УкрСЕПРО. Сертифікація систем якості. Порядок проведення.

ДСТУ 3420-96 Система сертифікації УкрСЕПРО. Вимоги до органів з сертифікації систем якості.

ДСТУ 3498-96 Система сертифікації УкрСЕПРО. Бланки документів. Форма та опис.

ДСТУ 3957-2000 Система сертифікації УкрСЕПРО. Порядок обстеження виробництва під час проведення сертифікації продукції.

ДСТУ EN 45011-2001 Загальні вимоги до органів, які керують системами сертифікації продукції.

ДСТУ ISO/IEC 17025-2001 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій.

ДСТУ 3278-95 Система розроблення та поставлення продукції на виробництво. Основні терміни та визначення.

ДСТУ 1.6:2004. Правила реєстрації нормативних документів.

ДСТУ 1.3-2004 Правила побудови, викладення, оформлення, погодження, прийняття та позначення ТУ.

КНД 50-008-93 Інструкція. Порядок державної реєстрації основних технічних умов.

ДСТУ 3639-97 Фільтри протизавадні. Загальні технічні умови.

Нормативні документи системи ТЗІ

НД ТЗІ 1.4-002-08 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань.

НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні положення.
НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації.
НД ТЗІ 2.3-001-01 Радіовиявлювачі вимірювальні. Методи та засоби випробувань.
НД ТЗІ 2.3-004-01 Радіовиявлювачі індикаторні. Методи та засоби випробувань.
НД ТЗІ 2.3-005-01 Радіовиявлювачі панорамні. Методи та засоби випробувань.
НД ТЗІ 2.3-006-01 Радіовиявлювачи аналізувальні. Методи та засоби випробувань.

Стандарти та нормативні документи колишнього СРСР

ГОСТ 15.005-86 Система разработки и постановки продукции на производство. Создание изделий единичного и мелкосерийного производства, собираемых на месте эксплуатации.

5.2 Державна експертиза у сфері ТЗІ

Закони України

Закон України „Про наукову і науково-технічну експертизу".

Накази Адміністрації Держспецзв'язку

Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175.

Порядок формування Реєстру організаторів державної експертизи у сфері технічного захисту інформації та Реєстру експертів з питань технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.04.2008 № 64.

Положення про Експертну раду з питань державної експертизи в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 01.10.2010 № 291.

Нормативні документи системи ТЗІ

НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

5.3 Державний контроль у сфері ТЗІ

Накази Адміністрації Держспецзв'язку

Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 86, зареєстрований в Міністерстві юстиції України 04.06.2007 за № 577/13844.

Положення про державний контроль за станом технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.

Інструкція про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення. Наказ Адміністрації Держспецзв'язку від 29.05.2007 № 100, зареєстрований в Міністерстві юстиції України 12.06.2007 за № 618/13885.

Нормативні документи системи ТЗІ

НД ТЗІ 2.3-002-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.

НД ТЗІ 2.3-003-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.

НД ТЗІ 4.7-001-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань.

Стандарти та нормативні документи колишнього СРСР

ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения.

ГОСТ 24555-81Система государственных испытаний продукции. Порядок аттестации испытательного оборудования. Основные положения.

6. Забезпечення діяльності у сфері технічного захисту інформації

6.1 Метрологічне забезпечення захисту інформації

Закони України

Закон України „Про метрологію та метрологічну діяльність".

Державні стандарти України, нормативні документи системи ТЗІ, стандарти та нормативні документи колишнього СРСР

ДСТУ 2681-94 Метрологія. Терміни та визначення.

ДСТУ 2708-2006 Повірка засобів вимірювальної техніки. Організація та порядок проведення.

ДСТУ 3215-95 Метрологія. Метрологічна атестація засобів вимірювальної техніки. Організація та порядок проведення.

ДСТУ 3400:2006 Метрологія. Державні випробування засобів вимірювальної техніки. Основні положення, організація, порядок проведення і розгляду результатів.

ДСТУ 3412-96 Вимоги до випробувальних лабораторій та порядок їх акредитації.

ДСТУ 3651.0-97 Метрологія. Одиниці фізичних величин. Основні одиниці фізичних величин. Міжнародної системи одиниць. Основні положення, назви та позначення.

ДСТУ 4134-2002 Метрологія. Канали вимірювальні вимірювальних інформаційних систем та автоматизованих систем керування технологічними процесами. Вимоги до структури та змісту методик виконання вимірювань.

ДСТУ-Н РМГ 51-2006 Метрологія. Документи до методик повірки засобів вимірювання. Основні положення (РМГ 51-2002, IDT).

ДСТУ ISO/IEC 17025-2006 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій.

6.2 Фінансування захисту інформації

Постанови Кабінету Міністрів України

Про фінансування заходів щодо криптографічного та технічного захисту інформації, охорона якої забезпечується державою відповідно до законодавства. Розпорядження КМ України від 13.12.2001 № 572-р.

6.3 Підготовка фахівців у сфері захисту інформації

Постанови Кабінету Міністрів України

Про перелік напрямів, за якими здійснюється підготовка кадрів у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавр. Постанова КМ України від 13.12.2006 № 1719.

При розробки КСЗІ від іноземної технічної розвідки треба враховувати наступне:

Добування інформації іноземними розвідками здійснюється постійно легальними способами і при недостатності отриманої цими способами інформації – шляхом проведення таємних операцій. При проведенні останніх, необхідно враховувати правове регулювання і можливі наслідки.

Легальне добування інформації проводиться шляхом вивчення та опрацювання відкритих джерел, публікацій з питань, які цікавлять, в засобах масової інформації, періодичних наукових і популярних журналах, працях вузів і науково-виробничих акціонерних товариств, урядових виданнях, навчальних посібниках тощо. Цінну інформацію можна отримати з урядових джерел, звітів компаній за операціями з цінними паперами, в місцевих юридичних відомостях, з матеріалів судової практики, які висвітлюють хід судового розгляду за участю конкурента, з інших легальних джерел.

Необхідну інформацію можна знайти в матеріалах, що мають безпосереднє відношення до діяльності фірми: в угоді про ліцензії, статтях і доповідях, річних звітах фірм, звітах комівояжерів, оглядах ринків і доповідей інженерів-консультантів, внутрішніх електронних виданнях, довідниках, рекламній літературі і проспектах. Цей перелік не є вичерпним.

Однак найбільш цінна інформація видобувається нелегальним шляхом в результаті проведення таємних заходів спецслужбами і органами комерційної розвідки, або так званого промислового шпигунства – «комерційної розвідки».

Добування інформації в загальному випадку представляє процес, який починається з моменту постановки завдання її користувачами (військово-політичним керівництвом країни або окремих відомств, керівництвом фірми) до моменту надання користувачам інформації, відповідно поставленим завданням і вимогам.

Технологія добування інформації включає наступні етапи:

- організація добування;
- добування даних і відомостей;
- інформаційна робота.

Організація добування інформації передбачає:

- декомпозицію (структурування) завдань, поставлених користувачами;
- розробку задуму операції по добуванню інформації;
- планування;
- постановку завдань виконавцям;
- нормативне та оперативне управління діями виконавців і режимами роботи технічних засобів.

Первісна постановка задач, як правило здійснюється в досить загальному вигляді, тому необхідна конкретизація з урахуванням наявних даних про можливі джерела інформації, їх місцезнаходження, можливі способи доступу і перешкоди, можливості наявних технічних засобів добування і так далі. В результаті аналізу завдань і наявних попередніх даних і припущень розробляється задум операції, в якому намічаються шляхи вирішення поставлених завдань.

На результативність добування інформації впливають численні перешкоди і випадкові чинники – протидія контррозвідки і служби безпеки, недостатність інформації про джерела видобуваємих відомостей і даних, відмови апаратури, погодні умови, пильність громадян і співробітників організації та інші. Ці фактори необхідно враховувати при плануванні із зазначенням місця і часу дій всіх суб'єктів і технічних засобів, що беруть участь в операції.

Відомості та дані одержують з допомогою пошуку джерел інформації і її носіїв, їх виявлення, встановлення розвідувального контакту з ними, отримання даних і відомостей.

Відомості та дані представляють фрагменти інформації і відрізняються один від одного тим, що дані знімаються безпосередньо з носія (первинна інформація), а відомості - проаналізовані дані (вторинна інформація).

Виявлення об'єктів, які цікавлять розвідку, в процесі пошуку проводиться по їх демаскуючим ознакам шляхом виділення об'єкта на фоні інших об'єктів. Основою процесу виявлення є процедура ідентифікації – порівняння поточних ознакових структур з еталонною ознаковою структурою об'єкта.

Здобуті дані, як правило, розрізнені. Вони перетворюються в корисну інформацію, відповідно до поставлених завдань, в ході накопичення та обробки інформації.

В ході видової та комплексної обробки формуються первинні і вторинні відомості на основі методів синтезу інформації і процедур ідентифікації та інтерпретації даних і відомостей.

Формування первинних відомостей проводиться шляхом збору та накопичення даних і "прив'язки" їх до тематичного питання, по якому видобувається інформація. Для включення даних до первинних відомостей необхідно, щоб ці дані містили інформаційні ознаки про приналежність даних до інформації з конкретного питання.

Якщо отримані відомості відповідають на поставлені питання, то інформація, що міститься у відомостях, семантична і ознакова, у відповідній формі передається її споживачам.

Найчастіше виникає необхідність у формуванні вторинної, переробленої інформації, наприклад, якщо не збігаються дані підсумкової інформації та первинних відомостей, одержаних від органів добування. Якщо споживача інформації цікавлять зовнішні видові властивості продукції, створюваної конкурентом, то здобуті ознаки зовнішнього вигляду і зображення не потребують додаткової обробки. Але коли для споживача цікавий принцип роботи запропонованого технічного засобу або технології, то первинні ознаки не відповідають на ці питання. В цьому випадку формуються вторинні відомості у вигляді опису конструкції вузлів, деталей нової продукції та іншої інформації, які не вдається добути у вигляді оригіналів документації або копій.

1.4 КОНТРОЛЬ ЕФЕКТИВНОСТІ ЗАХОДІВ ПО ЗАХИСТУ ПІДПРИЄМСТВ І УСТАНОВ ВІД ІНОЗЕМНОЇ ТЕХНІЧНОЇ РОЗВІДКИ.

Комплексний технічний контроль - контроль за станом функціонування своїх радіоелектронних засобів та їх захисту від технічних засобів розвідки противника. Здійснюється в інтересах радіоелектронного захисту. Включає радіо-, радіотехнічний, фотографічний, візуально-оптичний контроль, а також контроль ефективності захисту інформації від її витоку технічними каналами при експлуатації засобів передачі та обробки інформації.

Завдання комплексного технічного контролю – недопущення чи припинення порушень безпеки функціонування своїх радіоелектронних засобів, зокрема, перевищення допустимих параметрів радіовипромінювань або передачі по відкритих каналах зв'язку секретних відомостей або інформації для службового користування.

Радіотехнічні методи контролю

Радіоконтроль – контроль можливості отримання інформації противником з використанням радіопошуку, перехоплення, аналізу інформації, що передається за допомогою своїх радіоелектронних засобів. Радіоконтроль використовує такі методи і засоби, як:

- виділення і аналіз сигналу з ліній і каналів зв'язку;
- аналіз трафіку, розпізнавання ключових слів, отримання тексту і аналіз тем;
- системи розпізнавання мови;
- безперервне розпізнавання мови;
- ідентифікація мовця і інші методи вибору голосових повідомлень.

В цілому радіоконтроль подібний до радіорозвідки, але спрямований на свої радіоелектронні засоби.

Радіотехнічний контроль – контроль можливості збору і обробки інформації противником про технічні параметри радіоелектронних засобів, таких, як положення джерела випромінювання, його швидкість, наявність даних в випромінюваних сигналах. Засоби радіотехнічного контролю дозволяють:

- встановити несучу частоту передавальних радіозасобів;
- визначити координати джерел випромінювання;
- виміряти параметри імпульсного сигналу (частоту повторення, тривалість і інші параметри);
- встановити вид модуляції сигналу;
- визначити структуру бічних пелюсток випромінювання радіохвиль;
- виміряти поляризацію радіохвиль;
- встановити швидкість сканування антен і метод огляду простору радіолокаційних станцій;
- проаналізувати і записати інформацію.

Радіолокаційний контроль – контроль за технічними параметрами радіовипромінювання від своїх радіолокаційних станцій.

Електронно-оптичні методи контролю

Телевізійний контроль – контроль можливості отримання інформації противником за допомогою телевізійних камер.

Інфрачервоний і радіотепловий контроль – контроль можливості отримання інформації противником при використанні в якості джерела інформації або власного теплового випромінювання об'єктів, або перевідбитого випромінювання Місяця, зоряного неба.

Контроль лазерних випромінювань – контроль за станом функціонування своїх радіоелектронних засобів, що використовують при роботі лазери.

Електронно-акустичні методи контролю

Акустичний контроль – контроль можливості отримання інформації противником шляхом прийому, реєстрації, обробки і аналізу акустичних сигналів, що поширюються в повітряному середовищі.

Гідроакустичний контроль – контроль можливості отримання інформації противником шляхом прийому, реєстрації, обробки і аналізу прийнятих гідроакустичних сигналів.

Суб'єкти і об'єкти при веденні комплексного технічного контролю

Суб'єктом комплексного технічного контролю можуть виступати як державні структури (наприклад, підрозділи комплексного технічного контролю в збройних силах), так і спеціальні підрозділи служб безпеки комерційних організацій. ***Об'єктом*** комплексного технічного контролю виступають свої структури, підрозділи або фізичні особи.

1.5 КОНТРОЛЬ ЕФЕКТИВНОСТІ ЗАХОДІВ ПО ЗАХИСТУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ ЗАСОБАМИ.

Коли намічені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це насправді так, то можна намічати дату найближчої переоцінки. В іншому випадку доведеться проаналізувати допущені помилки і провести повторний сеанс аналізу уразливості з урахуванням змін в системі захисту.

Незалежно від того, наскільки добре розроблені технічні та організаційні заходи безпеки і дотримання конфіденційності, вони, врешті-решт, ґрунтуються на людській діяльності, в якій можливі помилки і злий намір. Якщо окремий співробітник обдурить довіру, то ніяка система безпеки не зможе запобігти витоку інформації.

Для забезпечення впевненості в тому, що дана організація успішно підтримує функціонування системи безпеки, застосовуються різні методи перевірки. Це регулярні незалежні інспекції і ревізії, а також перевірочні комісії, що складаються з представників усіх осіб, що беруть участь в роботі з конфіденційною інформацією.

Так як ні одна з форм не є ідеальною, то загальний контроль за діяльністю системи захисту і її функціонуванням повинен здійснювати вищий орган керівництва організації, підприємства через спеціальні підрозділи забезпечення безпеки.

На конкретних об'єктах при контролі ефективності захисту, що забезпечується конкретними засобами захисту інформації, може мати місце значне розмаїття завдань перевірки. Так на одному об'єкті, може бути, досить здійснити перевірку ефективності екранування, на іншому – перевірити ефективність шумового захисту, а на третьому – необхідно переконатися, що випромінювання ПЕМВН можуть бути прийняті за межами території організації (підприємства), що охороняється. Аналогічно і при перевірці ефективності захисту інформації від несанкціонованого доступу: на одному об'єкті використовується, наприклад, монопольний режим обробки інформації, яка підлягає захисту, а на іншому – програмний захист. Все це означає, що робота по контролю ефективності захисту повинна починатися з визначення складу перевіряємих заходів і засобів.

Крім того, організаційно-режимні засоби і заходи повинні мати переважне значення по відношенню до інших заходів та засобів захисту, оскільки їх склад і ефективність надають визначальне значення для ефективность захисту від несанкціонованого доступу (НСД). Це пов'язано з тим, що при неправильному визначенні ступеня конфіденційності інформації, що захищається, може виявитися неефективним як заборона, так і захист від несанкціонованого доступу. Інакше кажучи, необхідно починати контроль ефективності захисту з контролю організаційно-режимних заходів і засобів захисту. Далі послідовність перевірки може бути довільною.

Організація і проведення перевірки організаційних заходів здійснюється з метою виявлення порушень вимог відповідної інструкції щодо забезпечення режиму, який діє на даному об'єкті, а також того, як за данною інструкцією виконавці запобігають виникненню порушень. При підготовці до перевірки доцільно на основі аналізу скласти перелік можливих порушень, що може надати істотну допомогу в організації перевірки.

Ефективність захисту на об'єкти забезпечується, як відомо, відповідно до категорії важливості цього об'єкту. У свою чергу, категорія важливості визначається відповідно до грифа секретності.

Контроль ефективності захисту інформації від витоку за рахунок ПЕМВН передбачає проведення робіт з використанням певної контрольно-вимірювальної апаратури відповідно до існуючих методик. Цей контроль має на меті визначити наявність каналів витоку інформації і їх рівень за межами території об'єкта, що охороняється.

Особливу увагу при оцінці ефективності системи захисту технічними засобами необхідно звернути на їх надійність і безвідмовність. При їх експлуатації мають місце поломки, збої, відмови, внаслідок чого вони не забезпечують виконання завдання захисту. Звідси завдання забезпечення належної надійності технічних засобів знаходить значну важливість, від якої в прямій залежності знаходиться якість і безпека захисту.

1.6 КОНТРОЛЬ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ЯКА Є ІНТЕЛЕКТУАЛЬНОЮ ВЛАСНІСТЮ.

Інтелектуальна власність є особливим інформаційним ресурсом, система охорони якого в сучасному вигляді почала формуватися в XIX сторіччі, а в цілому була сформована на при кінець XX сторіччя. На відміну від інших інформаційних ресурсів ключову роль відіграє саме юридичний аспект захисту.

Існує два протилежних метода захисту – декларативний, коли результати інтелектуальної діяльності публікуються і таким чином стають відомі широкому, практично необмеженому колу потенційних споживачів інтелектуальнго продукту, та метод заснований на утриманні результатів інтелектуальної діяльності як державної та комерційної таємниці. Другий метод зазвичай називають режимом «Ноу-Хау», що в буквальному перекладі означає «Знаю как». Переважна більшість об'єктів інтелектуальної власності захищається першим методом, шляхом отримання патентів, свідотств, або «по факту створення». Вся Інтелектуальна власність поділяється на два типа:

- промислова Інтелектуальна власність;
- об'єкти авторського права.

Юридичний захист першої групи регламентується наступними законами:

«Закон україни про захист прав

«Про охорону прав на винаходи і корисні моделі»

«Про охорону прав на промислові зразки»

«Про охорону прав на знаки для товарів і послуг»

«Про охорону прав на зазначення походження товарів»

«Про охорону прав на топографії інтегральних мікросхем»

Об'єкти авторського права захищаються законом «Про авторське право і суміжні права»

Для ефективного захисту інтелектуальної власності треба ретельно виконувати формальні юридичні процедури та постійно мониторити появу нових об'єктів інтелектуальної власності у конкурентів та на ринку в цілому. Сучасний стан розвитку глобальної економиці, над швидкий обмін інформацією, продукцією та ідеями між країнами вносить свої корективи в побудову дійсно ефективної системи захисту інтелектуальної власності, які треба постійно вивчати для підтримання високої конкурентоспроможності, як окремих підприємств, так і держави у цілому.

Оцінка ефективності варіантів побудови захисту.

Після прийняття того чи іншого варіанту політики безпеки необхідно оцінити рівень безпеки інформаційної системи. Природно, що оцінка захищеності проводиться за сукупністю показників, основними з яких є вартість, ефективність, реалізація.

Завдання оцінки варіантів побудови системи захисту інформації досить складна, що вимагає залучення сучасних математичних методів багатопараметричної оцінки

ефективності. До таких методів належать метод аналізу ієрархій, експертні методи, метод послідовних поступок і ряд подібних їм.

Тестування системи захисту

Така перевірка називається "тестування на проникнення". Метою тестування є надання гарантій того, що в системі не існує простих шляхів для порушення прав власника інтелектуальної власності.

Для цього виділяється група з двох чоловік, які мають вищу спеціальну освіту. Цій групі надається в розпорядження охоронні документи на об’єкти інтелектуальної власності, матеріальні зразки, технічна документація, тощо. Ця група протягом 1-3 місяців аналізує документи, формули винаходів та описи патентів на винвходи та промислові зразки, описи торгових марок та намагається знайти вразливі місця і розробити на їх основі тестові заходи для обходу механізмів захисту інтелектуальної власності для оцінки можливих дій з боку конкурентів та державних установ.

Для гарантії об'єктивності тестування перевіряючі повинні бути досить професійні і незалежні.

Один з можливих способів атестації безпеки системи – запрошення патентних повірених провести патентну експертизу. За результатами роботи представляють конфіденційну доповідь з оцінкою рівня доступності інформації і рекомендацій щодо поліпшення захисту.

Необхідно постійно стежити за змінами законодавства у сфері інтелектуальної власності, за публікаціями Держпатенту Уаїни та іноземних патентних установ, інших виданях для своєчасного реагування на появу можливих загроз.

Слід пам’ятати, що штрафні санкції за порушення у сфері інтелектуальної власноті досить жорстки, тому слід завчасно робити патентний пошук та перевірку «патентної чистоти» на всіх етапах життєвого циклу інноваційного продукту.

Найбільш поширеними загрозами є:

- Неправомірне використання запатентованих винаходів третими особами – конкурентами;
- Поява блокуючих патентів, які унеможливують випуст продукції, яка попадає під захист блокуючого патенту;
- Поява та реєстрація торгових марок, які можуть бути сплутані з торговими марками підприємства, та нанести моральну шкоду репутації;
- Аннулювання раніш виданих патентів за позовами третих осіб;
- Призупинення дії охороних документів у разі несвоєчасної сплати державного мита;
- Розголошення інформації, яка зберігалась як комерційна інформація у режимі «ноу-хау» без отримання охороних документів;
- Втрата технічної переваги через дії з боку конкурентів по технічному аналізу виробів, що реалізуються на ринку з метою їх копіювання;

Даний перелік постійно доповнюється.

З появою засобів тестування та технічного аналізу з'явилися і засоби перешкоджання самому тестуванню. В цьому проявляється діалектика розвитку всіх явищ природи. Але для

деякіх об’єктів досить складно розробити надійні засоби перешкоджання, а для деякіх – зовсім неможливо, наприклад для об’єктів авторського права, механічних систем, промислових зразків, архітектурних форм, наукових праць тощо. В сучасних умовах слід зазначити, що, як показує реальна практика, жоден із способів (засобів і заходів) забезпечення безпеки інтелектуальної власності не є надійним, а максимальний ефект досягається при об'єднанні всіх їх в цілісну підсистему контролю та захисту інформації.

Тільки оптимальне поєднання організаційних, технічних і юридичних заходів, а також постійна увага і контроль за підтриманням системи захисту в актуальному стані дозволить з найбільшою ефективністю забезпечити рішення постійно актуальної задачі. При цьому слід враховувати, що така підсистема повинна створюватися паралельно з усіма етапати життєвого циклу, починаючи з моменту вироблення загального задуму побудови, проектування, впровадження та продажу продукта.

Сформована в розвинених країнах практика забезпечення безпеки конфіденційної інформації фірм і компаній пройшла шлях від суто адміністративних обмежувальних режимних заходів, планомірного навчання персоналу прийомам і методам захисту закритої інформації, використання психологічних аспектів захисту комерційної таємниці до розуміння того, що тільки в поєднанні цих напрямків з науковим, системним підходом до розробки і реалізації програм фірм по захисту інформації можна домогтися успіху в забезпеченні надійного зберігання виробничих, комерційних і інтелектуальних секретів та запатентованих активів.

Для проведення повного аналізу та управління ризиками існують спеціально розроблені інструментальні засоби, побудовані з використанням структурних методів системного аналізу і проектування (SSADM - Structured Systems Analysis and Design), які забезпечують:

- побудову моделі інформаційної системи з точки зору інформаційної безпеки;
- методи для оцінки цінності ресурсів;
- інструментарій для складання списку загроз і оцінки їх ймовірностей;
- вибір контрзаходів і аналіз їх ефективності;
- аналіз варіантів побудови захисту;
- документування (генерацію звітів).

В даний час на ринку присутні кілька програмних продуктів цього класу. Найбільш популярний з них CRAMM.

У 1985 році Центральне Агентство по Комп'ютерам і телекомунікацій (ССТА) Великобританії почало дослідження існуючих методів аналізу ІБ для того, щоб рекомендувати методи, придатні для використання в урядових установах, зайнятих обробкою несекретной, але критичної інформації. Жоден з розглянутих методів не підійшов. Тому був розроблений новий метод, який відповідає вимогам ССТА. Він отримав назву CRAMM - Метод ССТА Аналізу та Контролю Ризиків. Потім з'явилося кілька версій методу, орієнтованих на вимоги міністерства оборони, цивільних державних установ, фінансових структур, приватних організацій. Одна з версій, "комерційний профіль", є комерційним продуктом.

Метою розробки методу було створення формалізованої процедури, що дозволяє:

- переконатися, що вимоги, пов'язані з безпекою, повністю проаналізовані і задокументовані;
- уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків;
- надавати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- забезпечити проведення робіт в стислі терміни;
- автоматизувати процес аналізу вимог безпеки;
- уявити обгрунтування для заходів протидії;
- оцінювати ефективність контрзаходів, порівнювати різні варіанти контрзаходів;
- генерувати звіти.

В даний час CRAMM є, судячи за кількістю посилань в Інтернет, найпоширенішим методом аналізу і контролю ризиків.

В одночас слід пам’ятати, що сучасна модель юридичного захисту інтелектуальної власності формувалась за умов XIX та XX сторіччь, до появи глобальних компьтерних мереж з майже миттевими швидкостями поширення, копіювання та пошуку інформації. Як визначаюь фахівці, «старіння» інформації прискорилось настільки, що в деякіх випадках процедура реєстрації та експертизи патентів на винаходи може бути занадто довгою на тлі швидкості старіння інформації, що є основою конкурентних переваг.

Зараз існує два великих класа інтелектуальної власності, які мають різні традиції правової охорони, і це також треба усвідомлювати.

Перший клас – промислова інтелектуальна власність, яка захищає права на винаходи, торгові марки, промислові зразки, топологію мікросхем, сорти рослин. Слід зазначити, що сюди не попадає захист програмного забезпечення та «ноу-хау», які взагалі не захищаються.

Другий клас – об’єкти авторського та суміжного права. Літературні та музичні твори, вироби мистетства, наукові відкриття, та тексти програмного забезпечення.

Також розрізняють майнові права на інтелектуальну власність та немайнові. Слід зазначити, що немайнові права неможна передавати, навіть за згодою автора, вони є невідємними та охороняються безстроково на відміну від майнових.

Наприклад – строк охорони майнового права на винахід – 20 років з дати пріоритету, художнього твору – 70 років з моменту смерті автора, або останього з соавторів. Строк дії свідотства на торгову марку – 10 років, але він може бути продовжено за наявності сплати мита. Таким чином, торгова марка фактично може охоронятися безстроково. Наприклад, дуже відома марка Кока-Кола охороняється вже більш сторіччя та оцінюється в астрономічні суми. В той же час існуютє безліч торгових марок, які так і не стали відомими, чи взагалі вийшли з ринку.

Строки та умови захисту об’єктів інтелектуальної власності вказані в відповідних законах. Слід пам’ятати, що в різних країнах можливі деякі розбіжності, які слід враховувати при отриманні патентів за кордоном. Також слід пам’ятати, що патенти, на відміну від аворських прав, діють лише на терріторії держави, де вони видані, тому, якщо є потреба захистити свою інтелектуальну промислову власність – необхідно находити кошти для зарубіжного патентування в інших країнах.

Особливу увагу слід поділяти точному виконанню вимог патентного законодавства країни, де проходить патентування. Наважливіше для отримання «стійкого патенту» на винахід – приділяти багато уваги оформленню опису винаходу та формулі винаходу.

Загальні вимоги на винаходи – це промислова придатність, новизна та винахідницькій рівень.

Існує безліч прикладів, коли недбале ставлення до юридичних процедур, правил оформлення патентів, строків подання, сплати держмита за підтримання чинності приводили до безкарного копіювання, опротестування патентів та інших конфліктних ситуацій, які тягли за собою величезні матеріальні та моральні збитки.