Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

Лекція 15
Організаційно-технічні засоби захисту інформації

План

1. Технічні канали витоку інформації
2. Методи та засоби захисту від витоку інформації
3. Класифікація спеціальних засобів ТЗІ

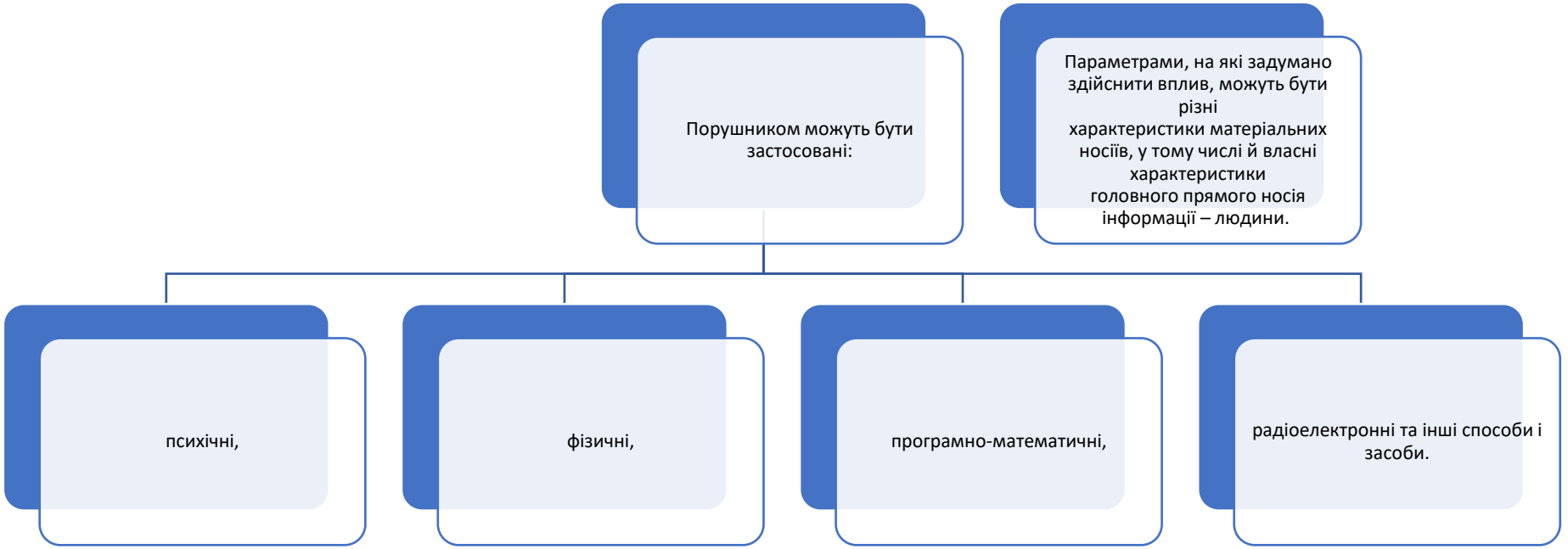
1. Технічні канали витоку інформації

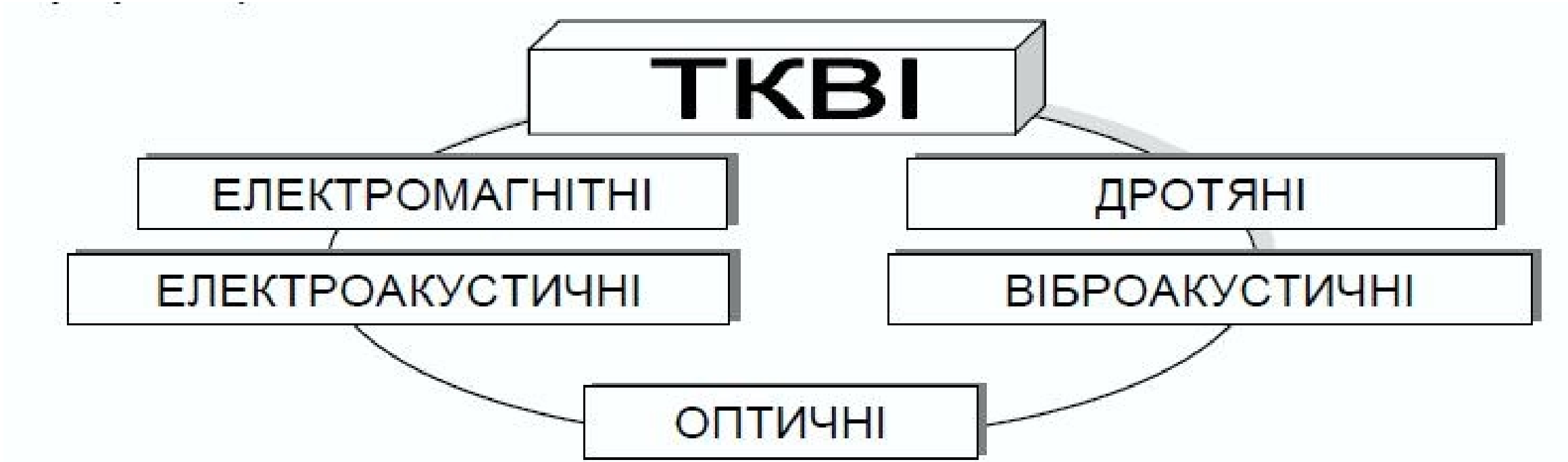
Для перехоплення, обробки та аналізу інформації за допомогою каналів витоку інформації (КВІ) можуть використовуватися різноманітні технічні засоби (ТЗс), а також люди (порушники).

КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів:

1. "людина – людина";
2. "людина – ТЗс ";
3. " ТЗс – ТЗс " ;
4. " ТЗс – людина".

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється *узагальнений канал витоку*, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за вищезгаданими чотирма типами каналів від порушника до носія інформації, то виникає так званий *узагальнений канал інформаційного впливу на носій інформації (канал спеціального впливу)*.





- **Рисунок 1. Структурна схема технічних каналів витоку інформації**

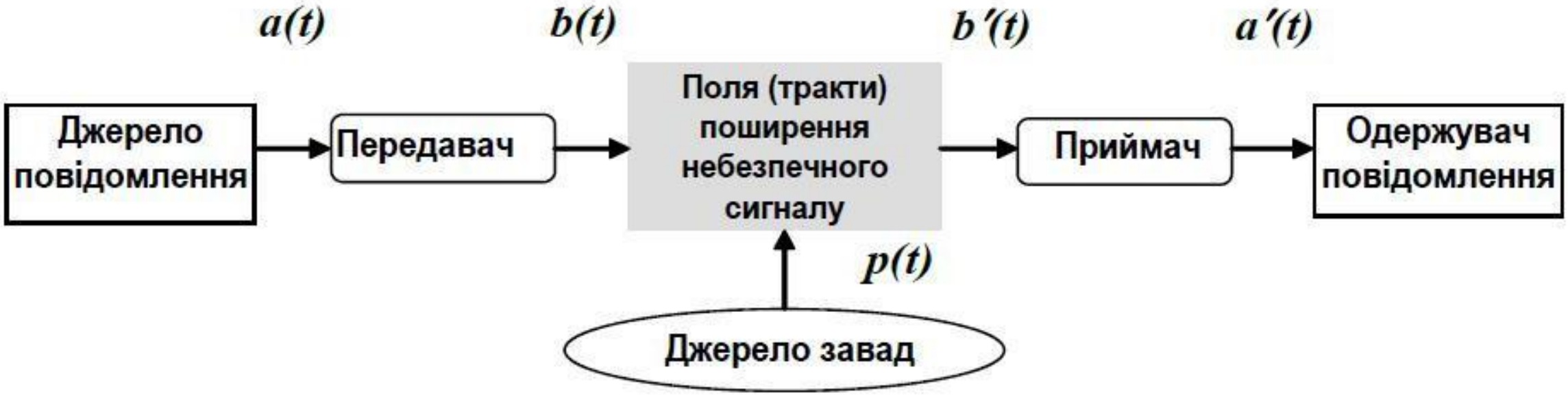


Рисунок 2 Процес передачі повідомлень

- На початку кожне повідомлення a(t) перетворюється передавачем у небезпечний (інформаційний) сигнал b(t). Небезпечний сигнал переміщується трактом його поширення, де на нього діє завада p(t), внаслідок чого він частково затухає. Далі одержаний на приймальній стороні небезпечний сигнал b'(t) перетворюється приймачем порушника в повідомлення a'(t). Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача b'(t) буде випадковим чином відрізнятися від b(t) і повідомлення a(t) може відрізнятися від a'(t).

- ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і за допомогою тільки приймачів, які приймають небезпечні сигнали,
утворені несанкціонованим перетворенням сигналів з ІПЗ у технічних засобах обробки інформації.

На рисунку використанні наступні умовні позначеня:
1 – витік за рахунок структурного звуку в стінах і перекриттях;
2 – зняття інформації із стрічки принтера, погано стертих дискет і т. п.;
3 – зняття інформації з використанням відеозакладок;
4 – програмно-апаратні закладки в ПЕВМ;
5 – радіозакладки у стінах і меблях;
6 – зняття інформації із системи вентиляції;
7 – лазерне зняття акустичної інформації з вікон;
8 – виробничі й технологічні відходи;
9 – комп'ютерні віруси, логічні бомби і т.п.;
10 – зняття інформації шляхом наведень і "нав'язування";
11 – дистанційне зняття відеоінформації (оптика);
12 – зняття акустичної інформації з використанням диктофонів;
13 – крадіжка носіїв інформації;
14 – високочастотний канал витоку в побутовій техніці;
15 – зняття інформації направленим мікрофоном;
16 – внутрішні канали витоку інформації (через обслуговуючий персонал);
17 –несанкціоноване копіювання;
18 – витік за рахунок побічного випромінювання терміналу;
19 – зняття інформації за рахунок використання "телефонного вуха";
20 – зняття з клавіатури і принтера за акустичним каналом;
21 – зняття з монітора з електромагнітного канала;
22 – візуальне зняття з монітора і принтера;
23 – наведення на лінії комунікацій і сторонні провідники;
24 – витік через лінії зв'язку;
25 – витік ланцюгами заземлення;
26 – витік мережею електрогодинника;
27 – витік трансляційною мережею та гучномовним зв'язком;
28 – витік охоронно-пожежною сигналізацією;
29 – витік мережею електроживлення;
30 – витік мережею опалювання, газо- і водопостачання.

2. Методи та засоби захисту від витоку інформації

Захист інформації від витоку технічними каналами досягається шляхом розробки та реалізації наступних заходів (у різних джерелах ці заходи виділяються і формулюються по-різному):

- організаційних;
- первинних технічних;
- основних технічних з використанням засобів забезпечення ТЗІ.

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом регламентації діяльності персоналу та порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Первинні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз без використання спеціальних засобів ТЗІ.

Основні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз із використанням спеціальних засобів ТЗІ.

Усі заходи розробляються одночасно і ув'язуються один з одним.

Організаційні заходи передбачають встановлення:

- окремих завдань захисту ІзОД та ІПЗ;
- структури й технології функціонування ТЗІ;
- вимог до забезпечення ТЗІ при організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) будівель, споруд і окремих приміщень;
- порядку реалізації організаційних, первинних і основних технічних заходів ТЗІ;
- прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІзОД та ІПЗ;
- порядку придбання засобів забезпечення ТЗІ і необхідних нормативних документів;
- контролю й обмежень доступу до виділених приміщень;
- територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів, що потребують захисту;

Організаційні заходи передбачають встановлення:

- порядку відключення на період проведення закритих заходів технічних засобів, які мають електроакустичні перетворювачі, від ліній зв'язку і т. д.;

- порядку залучення до проведення робіт із захисту інформації організацій, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами (Держспецзв’язок);

- порядку впровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

- порядку контролю функціонування СЗІ за її якісними характеристиками;

- порядку проведення атестації СЗІ з розробкою програми атестаційних випробувань;

- процедури керування СЗІ, яка полягає у:

- вивченні та аналізі технології проходження ІзОД та ІПЗ у процесі функціонування ІС;
- оцінці дії загроз на ІзОД та ІПЗ в конкретний момент часу;
- оцінці очікуваного ефекту від застосування засобів забезпечення ТЗІ;
- визначенні додаткової потреби в засобах забезпечення ТЗІ;

Первинні технічні заходи передбачають:

блокування каналів витоку інформації без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:	демонтажу технічних засобів, ліній зв'язку, сигналізації та управління, енергетичних мереж, використання яких не пов'язане з життєзабезпеченням підприємства і обробкою ІзОД;
	видалення окремих елементів технічних засобів, які є середовищем поширення полів і сигналів, з приміщень, де циркулює ІзОД;
	тимчасового відключення технічних засобів, що не беруть участь в обробці ІзОД, від ліній зв'язку, сигналізації, управління і енергетичних мереж;
	застосування способів і схемних рішень із захисту інформації, які не порушують основних технічних характеристик засобів забезпечення інформаційної діяльності;

блокування несанкціонованого доступу до інформації або її носіїв без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:	створення умов роботи в межах встановленого регламенту;
	виключення можливості використання (випробування) програмних, програмно-апаратних засобів, які не пройшли перевірку;
перевірку справності та працездатності технічних засобів і систем забезпечення інформаційної діяльності відповідно до експлуатаційних документів. Виявлені несправні блоки та елементи можуть сприяти витоку або порушенню цілісності інформації й підлягають негайній заміні (демонтажу).	

Основою первинних технічних заходів є використання захищених засобів (систем) забезпечення інформаційної діяльності, до яких включають:

- програмні засоби обробки інформації;

- технічні засоби (системи) обробки інформації;

- технічні засоби (системи) життєзабезпечення;

- оргтехніку;

- продукцію, процеси;

- інженерно-технічні споруди, будівлі, приміщення.

Основні технічні заходи

Принципи блокування ТКВІ

3. Класифікація спеціальних засобів ТЗІ

Заходи щодо блокування ТКВІ з використанням активних засобів

- просторове зашумлення:

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (у випадках виявлення та визначення частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТСПІ) з використанням засобів створення прицільних завад;

Просторове електромагнітне зашумлення комп'ютерного місця

Просторове електромагнітне зашумлення телефонної закладки

•створення акустичних і вібраційних завад з використанням генераторів акустичного шуму;

Створення віброакустичних завад лазерній системі розвідки

Створення віброакустичних завад радіосигналу

- *лінійне зашумлення:*
- лінійне зашумлення ліній електроживлення;

заглушення диктофонів у режимі запису з використанням відповідних пристроїв;

лінійне зашумлення сторонніх провідників і сполучних ліній ДТСЗ, що мають вихід за межі контрольованої зони;

- *знищення закладних пристроїв:*

•знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів "жучків").

Заходи щодо блокування ТКВІ з використанням активно-пасивних засобів

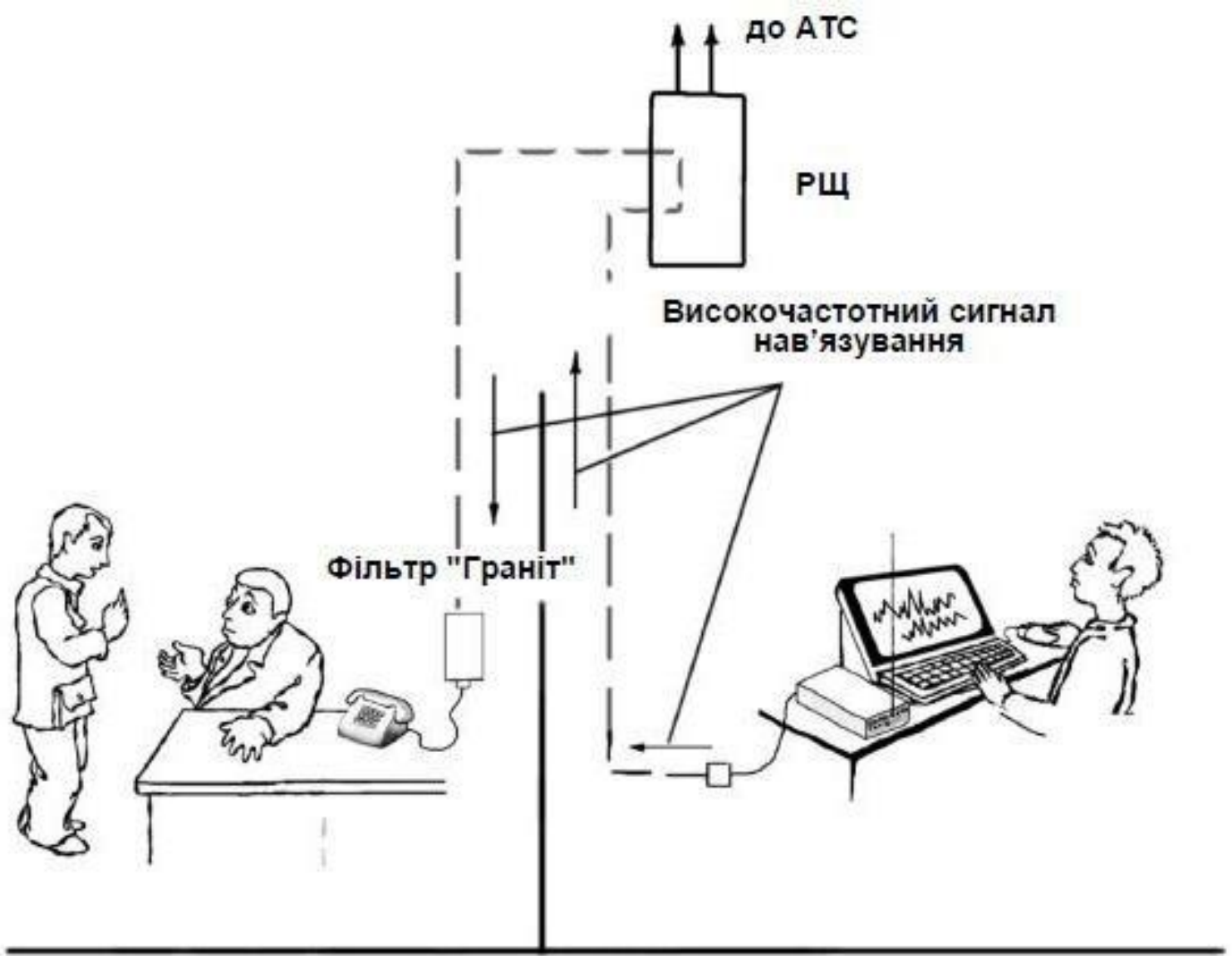
- розв'язування інформаційних сигналів з одночасним лінійним зашумленням:

установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень комбінованих пристроїв, що об'єднують в одному корпусі перешкодоглушильний фільтр і генератор шуму.

Заходи щодо блокування ТКВІ з використанням пасивних засобів

- *контроль і обмеження доступу* на об'єкти ТСПІ та у виділені приміщення: .
- - установка на об'єктах ТСПІ та у виділених приміщеннях технічних засобів і систем обмеження й контролю доступу;
- *локалізація випромінювань:*
- - екранування ТСПІ та їх сполучних ліній;
- - заземлення ТСПІ та екранів їх сполучних ліній;
- - звукоізоляція виділених приміщень;
- *розв'язування інформаційних сигналів:*
- - установка смугових фільтрів у допоміжних технічних засобах і системах, у яких спостерігається "мікрофонний ефект" і які мають вихід за межі контрольованої зони;

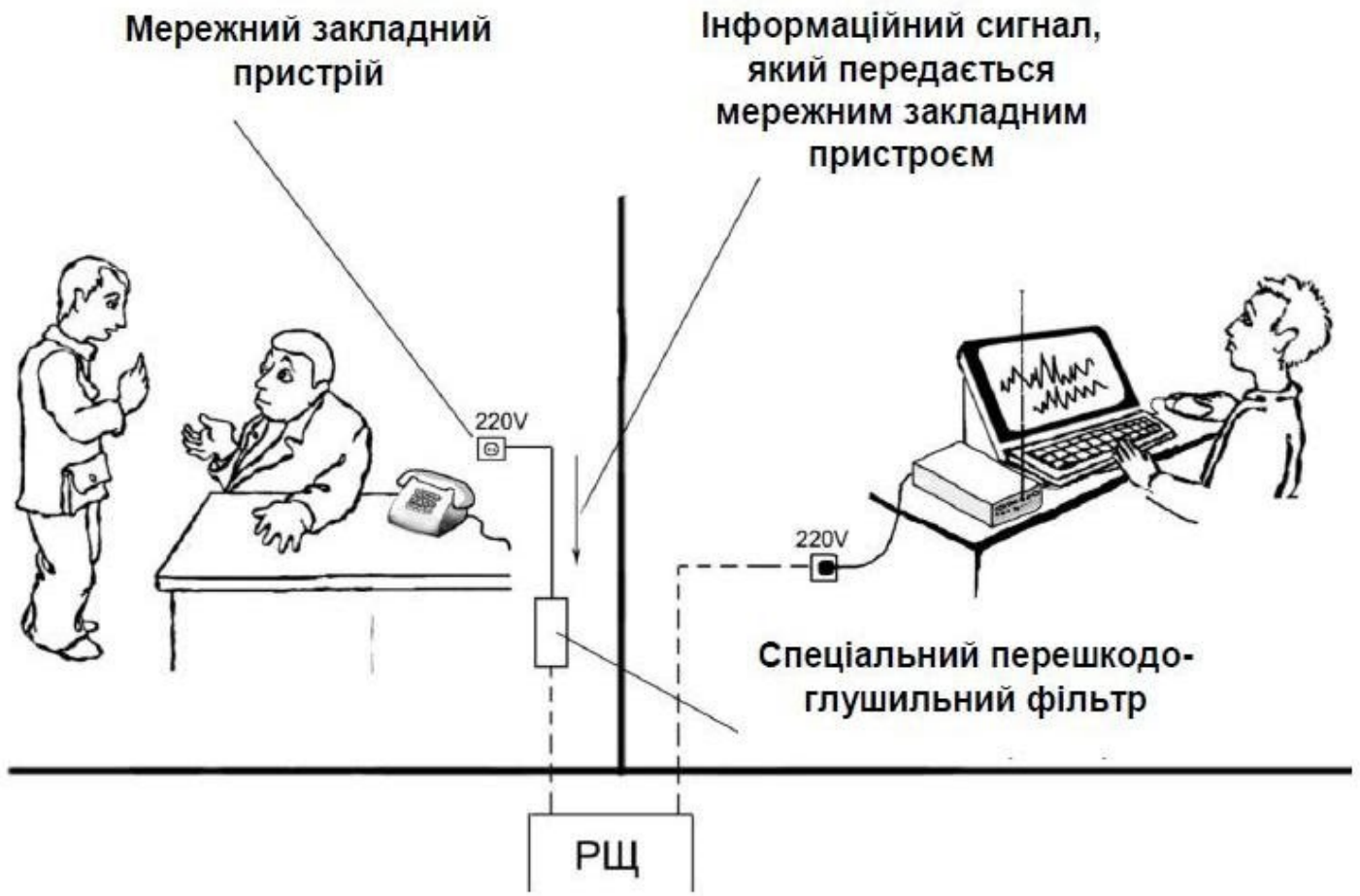
Установка смугових фільтрів



- установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання й каналізації, що мають вихід за межі контрольованої зони;

- установка автономних або стабілізованих джерел електроживлення ТСПІ;
- установка пристроїв гарантованого живлення ТСПІ (наприклад, генераторів мотора);
- установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень спеціальних глушильних фільтрів.

Установка заглушуючих фільтрів у мережі



Заходи щодо виявлення портативних електронних пристроїв перехоплення інформації

- виявлення закладних пристроїв з використанням пасивних засобів:

установка у виділених приміщеннях засобів і систем виявлення лазерного опромінювання (підсвічування) шибок;

установка у виділених приміщеннях стаціонарних виявлювачів диктофонів;

пошук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів і програмно-апаратних комплексів контролю;

організація радіоконтролю (постійно або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТСПІ;

Заходи щодо виявлення портативних електронних пристроїв перехоплення інформації

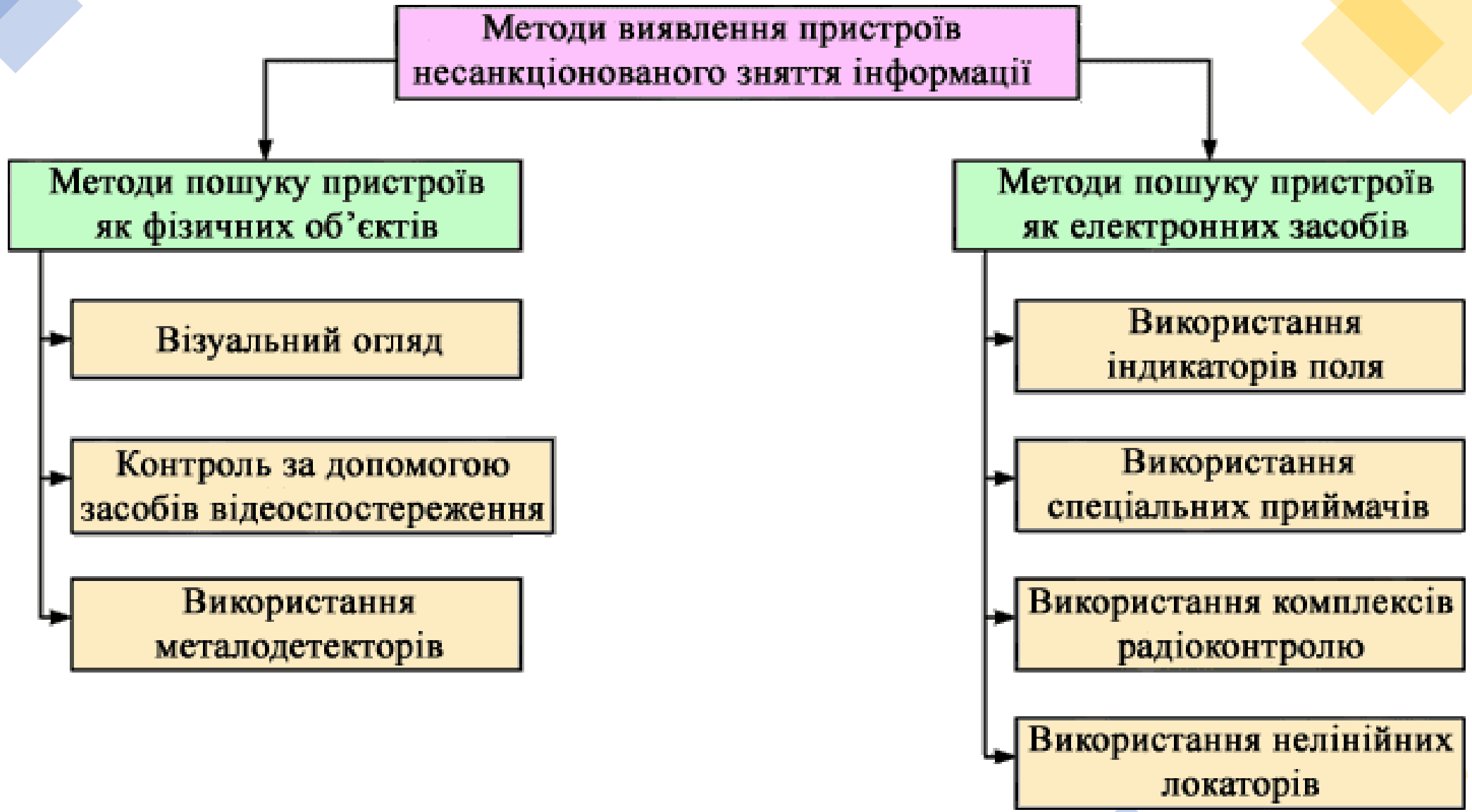
- виявлення закладних пристроїв з використанням активних засобів:

спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

спеціальна перевірка виділених приміщень, ТСПІ та допоміжних технічних засобів з використанням рентгенівських комплексів;

спеціальна перевірка виділених приміщень з використанням металошукачів;

спеціальна перевірка виділених приміщень з використанням ендоскопа та комплекту оглядових дзеркал;


Методи виявлення пристроїв несанкціонованого зняття інформації
Методи пошуку пристроїв як фізичних об'єктів
Візуальний огляд
Контроль за допомогою засобів відеоспостереження
Використання металодетекторів
Методи пошуку пристроїв як електронних засобів
Використання індикаторів поля
Використання спеціальних приймачів
Використання комплексів радіоконтролю
Використання нелінійних локаторів

Заходи щодо перетворення сигналів у каналах зв'язку

- *використання аналогових і цифрових скремблерів для перетворення мовних сигналів;*
- *використання програмного й апаратного шифрування даних.*