МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

ЕЛЕКТРОННИЙ НАВЧАЛЬНО-НАОЧНИЙ ПОСІБНИК

СХЕМОКОНСПЕКТ ЛЕКЦІЙ
з навчальної дисципліни
«МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»
для студентів всіх форм навчання освітнього ступеня «Бакалавр»
галузі знань 12 Інформаційні технології

Дрогобич, 2025

УДК 37:004:316.772.5

Схемоконспект лекцій з навчальної дисципліни «Методи та засоби технічного захисту інформації» для студентів всіх форм навчання освітнього ступеня «Бакалавр» галузі знань 12 Інформаційні технології : електронний навчально-наочний посібник / уклад. Я.Ю. Дорогий, Р.В. Корольов. – Дрогобич : ДонНТУ, 2025. – 787 с.

Навчальна дисципліна «Методи та засоби технічного захисту інформації» є актуальною і затребуваною в контексті підготовки сучасних фахівців у галузі інформаційних технологій та кібербезпеки та з огляду на формування когнітивних, афективних та моторних компетентностей в контексті вивчення та розуміння принципів організації та побудови систем технічного захисту інформації (СТЗІ).

Пропонований студентам для опанування схемоконспект лекцій з цієї дисципліни має за мету забезпечити їм певну допомогу під час вивчення ними ключових положень базових тем курсу. Схематична форма конспекту акцентує увагу студентів на закріпленні основних фахових знань, формуванні відповідних умінь і в цілому отриманні ними кваліфікаційних компетентностей.

Укладачі: _____ Я. Ю. Дорогий, професор, д. т. н., в.о. зав. кафедри ПМІ, Р.В. Корольов, доцент, к.т.н., доцент кафедри КБІТ ХНЕУ

Рецензент: _____ В. В. Цуркан, доцент, к. т. н., доцент спеціальної кафедри №5 ІСЗЗІ КПІ ім. Ігоря Сікорського,

Відповідальний за випуск: Я. Ю. Дорогий, професор, д. т. н., в.о. зав. каф. ПМІ

Затверджено навчально-методичним відділом ДонНТУ, протокол № 4 від 25.02.2025 р.

Розглянуто на засіданні кафедри прикладної математики і інформатики, протокол № 2 від 21.02.2025 р.

© Донецький національний технічний університет, 2025

ЗМІСТ

ВСТУП		**5**
Тема 1.	**Вступ до дисципліни. Нормативно-правові основи технічного захисту інформації.**	
	Лекція 1. Вступ до дисципліни. Загальні концептуальні положення інформаційної безпеки. Нормативно-правове забезпечення захисту інформації.	6
Тема 2.	**Побудова комплексу технічного захисту інформації.**	
	Лекція 2. Види інформації. Загрози інформації. Технічний захист інформації. Мета та етапи ТЗІ.	53
	Лекція 3. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. НД ТЗІ 1.1-005-07.	98
	Лекція 4. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.	133
	Лекція 5. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.	167
Тема 3.	**Технічні засоби захисту інформації.**	
	Лекція 6. Методи та засоби технічного захисту інформації.	197
	Лекція 7. Методи та засоби знищення інформації.	265

	Лекція 8. Програмні методи захисту інформації.	**304**
Тема 4.	**Технічні канали витоку інформації.**	
	Лекція 9. Технічні канали витоку інформації. Загальні поняття. Потенційні канали витоку інформації.	388
	Лекція 10. Просочування інформації технічними каналами.	418
	Лекція 11. Канали витоку інформації при експлуатації ЕОМ.	450
Тема 5.	**Розвідка та добування інформації.**	
	Лекція 12. Основи розвідувальної діяльності.	518
	Лекція 13. Оптична розвідка.	590
	Лекція 14. Акустична розвідка.	644
	Лекція 15. Радіоелектронна розвідка.	700
	Лекція 16. Кібернетична розвідка.	751
	СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ ДЛЯ САМОПІДГОТОВКИ	**785**

ВСТУП

У сучасних умовах розвитку інформаційних технологій, коли технологічний прогрес постійно набирає обертів, безпека інформації стає надзвичайно важливою сферою. Особливо в Україні, де прискорений цифровий розвиток та умови воєнної агресії вимагають відповідних заходів для забезпечення захисту інформації від різноманітних загроз. Курс «Методи та засоби технічного захисту інформації" спрямований на розуміння та впровадження систем технічного захисту інформації, спеціально адаптованих до реалій національного інформаційного простору та законодавства України.

Зосереджуючись на архітектурних аспектах захисту, цей курс дозволяє студентам здобути глибокі знання та практичні навички у сфері розробки та впровадження методі та заходів технічного захисту інформації. Він враховує технічні та стратегічні аспекти захисту інформації, адаптовані до динаміки сучасних загроз, що є особливо актуальним для української державної інформаційної інфраструктури.

Проходження курсу дозволить студентам освоїти сучасні методи та стратегії захисту інформаційних систем від широкого спектру загроз, інтегрувати їх в системи технічного захисту інформації, оцінити отримані результати.

Практичні заняття не лише сприятимуть розвитку навичок проектування, але й допоможуть у впровадженні таких систем, враховуючи особливості нормативно-правового регулювання даної сфери в Україні.

Донецький національний технічний університет



Тема 1. Вступ до дисципліни. Нормативно-правові основи технічного захисту інформації.
Лекція 1. Вступ до дисципліни. Загальні концептуальні положення інформаційної безпеки. Нормативно-правове забезпечення захисту інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Мета та структура курсу, РСО з дисципліни
- Системи захисту інформації
- Модель безпеки інформації, загрози
- Правовий захист інформації, основні НПА

Мета та структура курсу, РСО з дисципліни

Мета курсу

- Мета цієї навчальної дисципліни полягає в тому, щоб забезпечити студентів технічними та методичними засобами для забезпечення безпеки обробки інформації в різних інформаційних системах.
- Основна увага приділяється вивченню:
  - технічних механізмів та інструментів захисту інформації, що входять до складу сучасних систем безпеки;
  - удосконаленню професійної компетентності фахівців з технічного захисту інформації та забезпечення їхніх здатностей в контексті:
    - проведення обстеження об’єктів інформаційної діяльності,
    - виявленні технічних каналів витоку інформації,
    - розробці моделі загроз та технічного завдання щодо створення комплексних систем та комплексів технічного захисту інформації
- та передбачає оволодіння знаннями згідно з вимогами кваліфікаційного довідника професій працівників підрозділів технічного захисту інформації і забезпечує фахівцям теоретичні і практичні навички у справі організації технічного захисту інформації.

Структура курсу

- 16 лекцій, 12 семінар-тестів
- 13 практичних робіт
- Іспит

РСО з дисципліни

- **13 практичних робіт** оцінюються в 40 балів
- **12 семінар-тестів** оцінюються в 60 балів
- Якщо все здано вчасно, то виставляється оцінка за іспит автоматом
- Якщо не вчасно, студент здає іспит у вигляді екзаменаційного тесту на 100 питань.

Системи захисту інформації

Інформація

- Інформація – це відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх представлення.
  - Інформація може мати різну форму (дані, закладені в комп'ютерах, кресленнях, пам'ятних записках, досьє, формулах, діаграмах, моделях продукції, дисертаціях, судових документах тощо).
  - Інформація має споживачів, що потребують її, і тому має певні споживчі якості, а також має і своїх володарів або виробників.
- З точки зору споживача, якість використовуваної інформації дозволяє отримувати додатковий економічний або моральний ефект.
- З точки зору власника – збереження в таємниці комерційно-важливої інформації дозволяє успішно конкурувати на ринку виробництва, збуту товарів і послуг. Це природньо вимагає певних дій, спрямованих на захист конфіденційної інформації.

Інформаційна безпека

- **Інформаційна безпека** – це стан захищеності інформаційних ресурсів організації і підтримувальної інфраструктури від зовнішніх і внутрішніх загроз, які можуть завдати неприйнятного збитку суб’єктам інформаційних відношень.

Система захисту інформації (СЗІ)

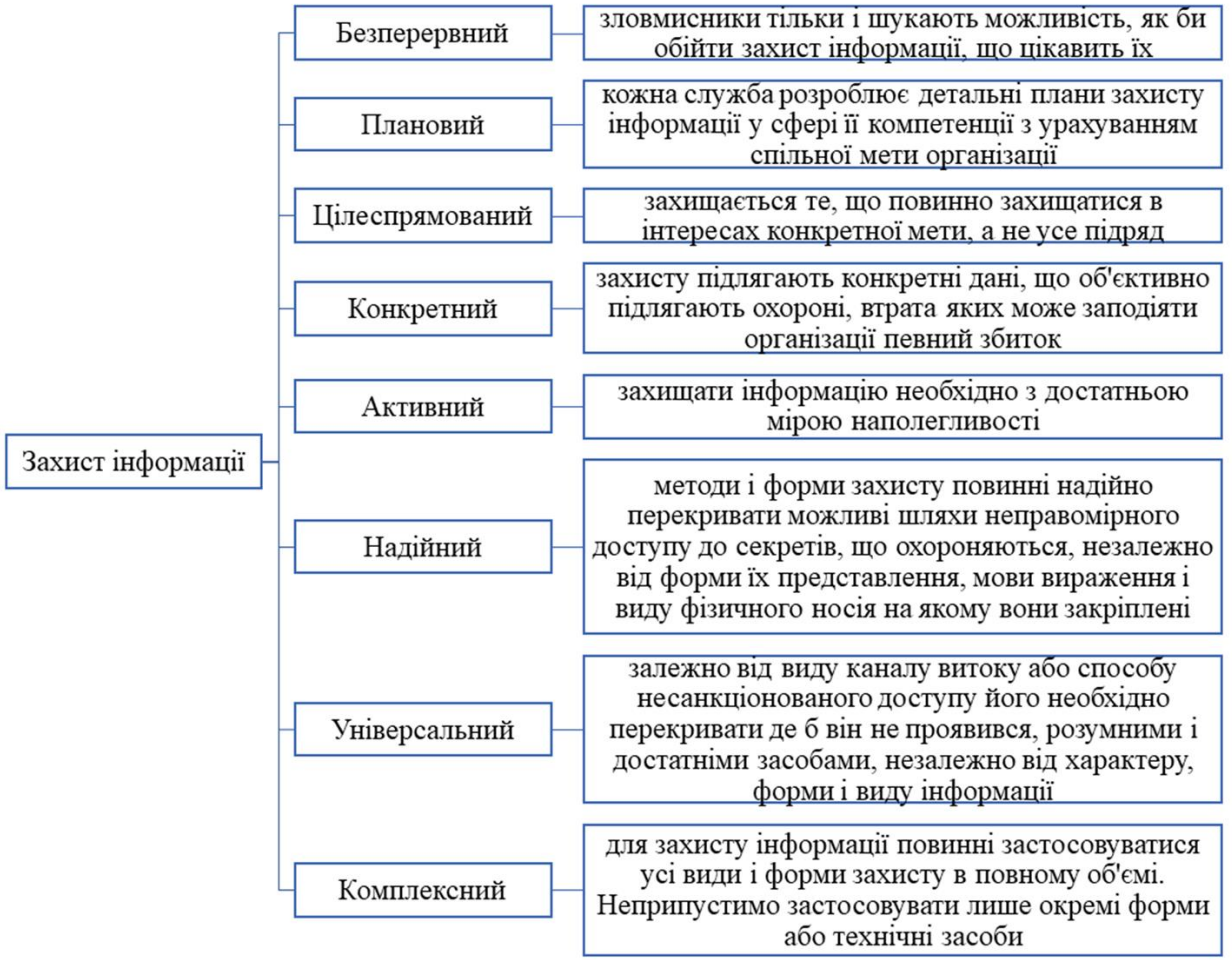
- **Система захисту інформації** (СЗІ) – це організована сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Концептуальні положення СЗІ

- Основні концептуальні положення системи захисту інформації:
  - Забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення і розвитку системи захисту, безперервному контролі її стану, виявленні її вузьких і слабких місць і протиправних дій.
  - Безпека інформації може бути забезпечена лише при комплексному використанні усього арсеналу наявних засобів захисту в усіх структурних елементах організації і на усіх етапах технологічного циклу обробки інформації.

Комплексний характер СЗІ

- **Комплексний характер захисту виникає з того, що захист** – це специфічне явище, що є складною системою нерозривно взаємозв'язаних і взаємозалежних процесів, кожен з яких у свою чергу має безліч різних сторін, які взаємно обумовлюють один одного, властивостей, тенденцій.



Умови СЗІ

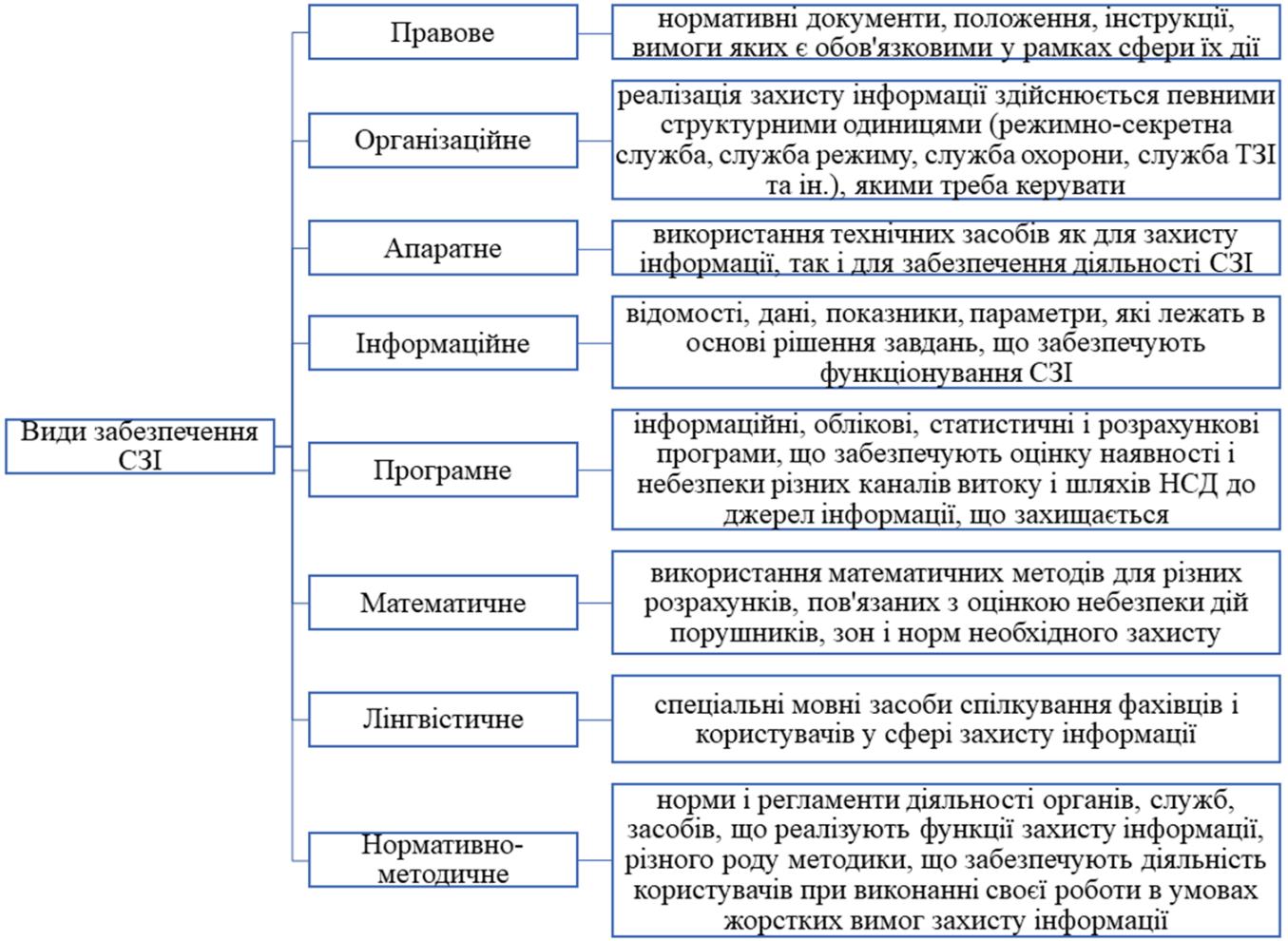
- Для забезпечення виконання вимог безпеки СЗІ повинна задовольнятися певними умовами:
  - охоплювати увесь технологічний комплекс інформаційної діяльності;
  - бути різноманітною по використанню засобів, багаторівневою з ієрархічною послідовністю доступу;
  - бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
  - бути нестандартною, різноманітною (при вибиранні засобів захисту не можна розраховувати на непоінформованість зловмисників відносно її можливостей);
  - бути простою для технічного обслуговування і зручною для експлуатації користувачами;
  - бути надійною (поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації);
  - бути комплексною, мати цілісність, яка означає, що жодна її частина не може бути вилучена без збитку для усієї системи.

Вимоги до систем безпеки інформації

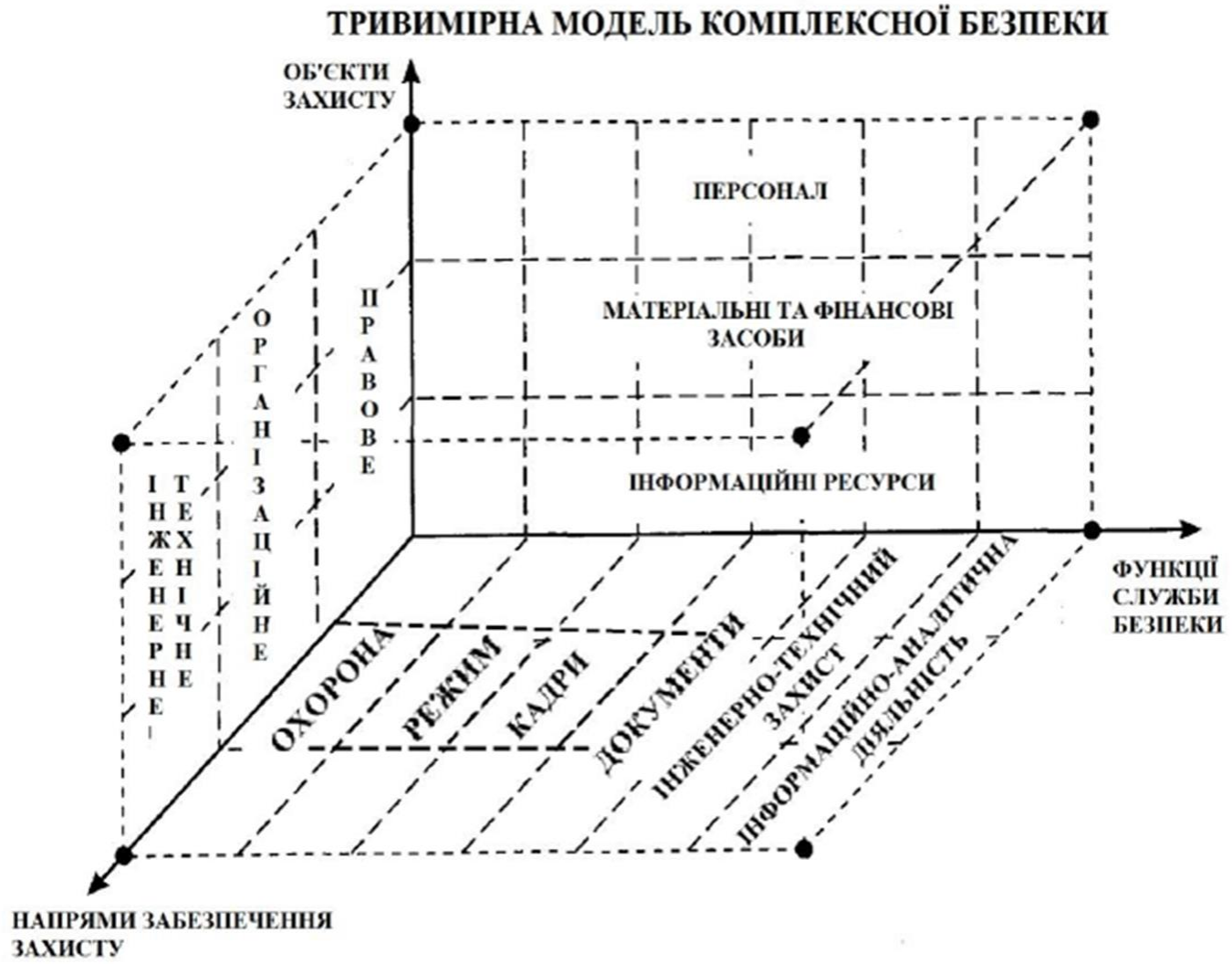
- До системи безпеки інформації пред'являються також певні вимоги:
  - чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
  - надання користувачеві мінімальних повноважень, необхідних йому для виконання дорученої роботи;
  - зведення до мінімуму числа засобів захисту, загальних для декількох користувачів;
  - облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
  - забезпечення оцінки ступені конфіденційності інформації;
  - забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу.

Види забезпечення СЗІ

- СЗІ повинна мати власне забезпечення, спираючись на яке вона виконуватиме свою цільову функцію.



Тривимірна модель комплексної безпеки



Вихідні дані для побудови СЗІ

- Для побудови СЗІ потрібно:
  - визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації і цілі, а також інші умови і дії, що порушують безпеку;
  - розглянути заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.
- Для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання, при яких формується як би «заступник» реальних ситуацій.

Модель безпеки інформації, загрози

Концептуальна модель безпеки інформації



Загрози конфіденційної інформації

- Концепція безпеки є основним правовим документом, який визначає захищеність організації від внутрішніх і зовнішніх загроз.
- **Загрози конфіденційної інформації** – це потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння відомостями, які охороняються. Такими діями є:
  - ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
  - модифікація інформації в кримінальних цілях як часткова або значна зміна складу і змісту відомостей;
  - руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

Загрози інформації



Класифікація загроз



Дії, які призводять до неправомірного оволодіння інформації з обмеженим доступом (ІзОД)

- Відношення об'єкта (організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності в діях, що призводять до оволодіння ІзОД. В цьому випадку можливі такі ситуації:
  - власник не приймає ніяких заходів до збереження ІзОД, що дозволяє зловмисникові легко отримати ті відомості, що цікавлять його;
  - власник інформації строго дотримується заходів інформаційної безпеки, тоді зловмисникові доводиться докладати значних зусиль до здійснення доступу до відомостей, що охороняються, використовуючи для цього усю сукупність способів несанкціонованого проникнення: легальне або нелегальне, заходове або без заходове;
  - проміжна ситуація – це виток інформації технічними каналами, при якій власник ще не знає про це, а зловмисник без особливих зусиль може їх використовувати у своїх інтересах

Незаконне оволодіння ІзОД

- Дії, які призводять до незаконного оволодіння ІзОД:
  - **розголошення** – умисні або необережні дії осіб, яким відповідні відомості були довірені в установленому порядку, що привели до ознайомлення з ними осіб, не допущених до них.
  - **витік** – безконтрольний вихід ІзОД за межі організації або кола осіб, яким вона була довірена.
  - **несанкціонований доступ** – протиправне умисне оволодіння ІзОД особою, яка не має права доступу до відомостей, що охороняються.

Правовий захист інформації, основні НПА

Правовий захист інформації

- **Правовий захист інформації** – це спеціальні правові акти, правила, процедури та заходи, які забезпечують захист інформації на правовій основі.

- Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.

Система нормативно-правових документів в Україні, що регламентують питання захисту інформації



Структура законодавства України в області захисту інформації

- Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу і змісту, співвідношення його з усією системою законів і правових актів України.



Основні НПА

- Конституція України (Відомості Верховної Ради України, 1996, № 30, ст. 141): «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» (ст. 17).
- Закон України «Про інформацію» (Відомості Верховної Ради України, 1992, № 48, ст. 650) регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Основні напрями державної інформаційної політики

- Основні напрями державної інформаційної політики (ст. 3):
  - забезпечення доступу кожного до інформації;
  - забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
  - забезпечення інформаційної безпеки України;
  - забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
  - сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору;
  - створення умов для формування в Україні інформаційного суспільства;
  - постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
  - створення інформаційних систем і мереж інформації, розвиток електронного урядування.

Суб’єкт та об’єкт інформаційних відносин

- Суб’єкти інформаційних відносин (ст. 4)):
  - фізичні особи;
  - юридичні особи;
  - об’єднання громадян;
  - суб’єкти владних повноважень.
- Об'єкт інформаційних відносин – **інформація** (ст. 4).

Класифікація інформації за порядком доступу



ЗУ «Про державну таємницю»

- Закон України «Про державну таємницю» (Відомості Верховної Ради України, 1994, № 16, ст. 93) регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.
- Сфери, у яких інформація може бути віднесена до державної таємниці (ст.8):
  - оборони;
  - зовнішніх відносин;
  - економіки, науки і техніки;
  - державної безпеки та охорони правопорядку.

Організаційно-правові засади щодо охорони державної таємниці

- Основні організаційно-правові заходи щодо охорони державної таємниці (ст. 18):
  - єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
  - дозвільний порядок провадження діяльності, пов'язаної з державною таємницею (ДТ);
  - обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
  - обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до ДТ, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;
  - режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;
  - спеціальний порядок допуску та доступу громадян до ДТ;
  - технічний та криптографічний захисти секретної інформації.

ЗУ «Про основи національної безпеки України»

- Закон України «Про основи національної безпеки України» (Відомості Верховної Ради України, 2003, № 39, ст. 351) визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Загрози національним інтересам та безпеці України в інформаційній сфері

- Загрози національним інтересам і національній безпеці України в інформаційній сфері (ст. 7):
  - комп'ютерна злочинність та комп'ютерний тероризм;
  - розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
  - намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основні напрямки держполітики нацбезпеки в інформаційній сфері

- Основні напрями державної політики з питань національної безпеки в інформаційній сфері (ст. 8):
  - забезпечення інформаційного суверенітету України;
  - вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері;
  - вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

ЗУ «Про захист інформації в інформаційно-комунікаційних системах»

- Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України, 1994, № 31, ст. 286) регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Об’єкти та суб’єкти захисту в ІТС



- Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю (ст. 8).

ЗУ «Про ліцензування видів господарської діяльності»

- Закон України «Про ліцензування видів господарської діяльності» (Відомості Верховної Ради України, 2015, № 23, ст. 158) визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування, встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування.

Кодекси

- Кодекс України про адміністративні правопорушення (Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст. 1122).
- Кримінальний кодекс України (Відомості Верховної Ради України, 2001, № 25-26, ст. 131).

Укази президента

- Указ Президента України «Про Положення про технічний захист інформації в Україні» (від 27 вересня 1999 р. № 1229/99). Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.
- Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» (від 22 травня 1998 р. № 505/98). Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі.

Постанови Уряду

- Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» (від 8 жовтня 1997 р. № 1126). Концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації (ТЗІ) є складовою частиною забезпечення національної безпеки України.

Національні стандарти України

- ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва
- ДСТУ 3396 0-96 Технічний захист інформації. Основні положення.
- ДСТУ 3396 1-96 Технічний захист інформації. Порядок проведення робіт.
- ДСТУ 3396.2-97 Технічний захист інформації. Терміни та визначення.
- ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка

Міжнародні стандарти, прийняті в Україні як національні$_1$

- ДСТУ ISO/IEC 9798-4:2015 Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Механізми, що використовують криптографічну перевірочну функцію (ISO/IEC 9798-4:1999, Cor 1:2009, Cor 2:2012, IDT) (budstandart.com)
- ДСТУ ISO/IEC 10118-1:2018 Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO/IEC 10118-1:2016, IDT) (budstandart.com)
- ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT) (budstandart.com)

Міжнародні стандарти, прийняті в Україні як національні$_2$

- ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту (ISO/IEC TR 13335-4:2000, IDT) (budstandart.com)
- ДСТУ ISO/IEC 14888-2:2015 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел (ISO/IEC 14888-2:2008, IDT) (budstandart.com)
- ДСТУ ISO/IEC 15946-1:2006. Інформаційні технології. Методи захисту. Криптографічні методи, що грунтуються на еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946-1:2002, IDT) (budstandart.ua)

Міжнародні стандарти, прийняті в Україні як національні$_3$

- ДСТУ ISO/IEC 18014-1:2006 Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 1. Основні положення (ISO/IEC 18014-1:2002, IDT) (budstandart.ua)
- ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) (budstandart.com)

Донецький національний технічний університет



Тема 2. Побудова комплексу технічного захисту інформації. Лекція 2. Види інформації. Загрози інформації. Технічний захист інформації. Мета та етапи ТЗІ.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

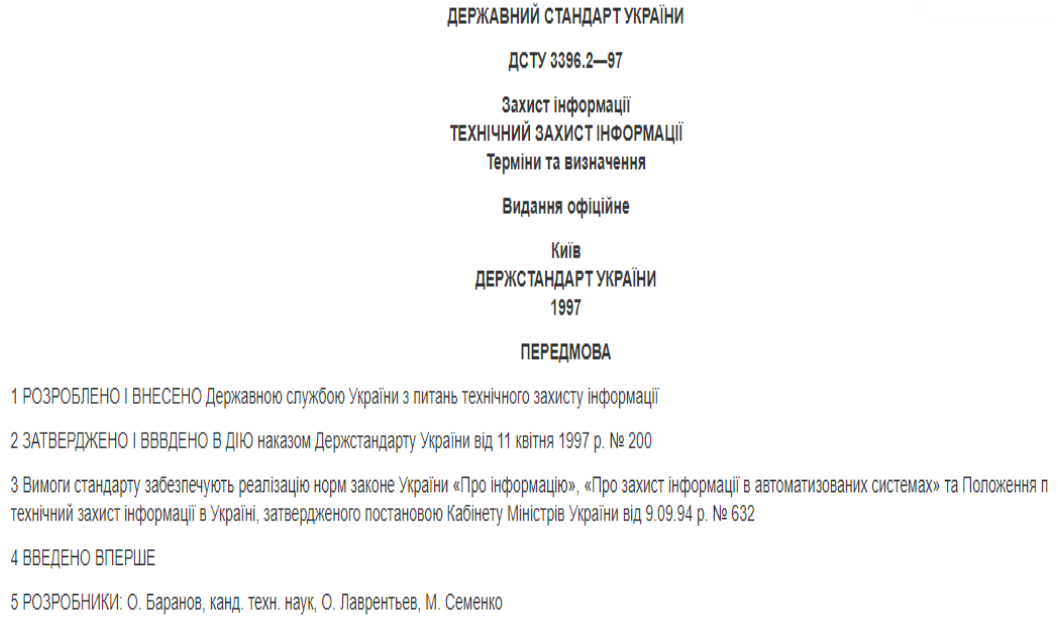
Лекційні питання

- Види інформації, які підлягають технічному захисту
- Загрози для інформації

Види інформації, які підлягають технічному захисту

Види інформації, які підлягають технічному захисту[1]

- **інформація** – відомості про суб'єкти, об'єкти, явища та процеси
- **інформація з обмеженим доступом** – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами
- **таємна інформація** – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю
- **конфіденційна інформація** – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними



ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

ДСТУ 3396.2—97

Захист інформації
ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ
Терміни та визначення

Видання офіційне

Київ
ДЕРЖСТАНДАРТ УКРАЇНИ
1997

ПЕРЕДМОВА

1 РОЗРОБЛЕНО І ВНЕСЕНО Державною службою України з питань технічного захисту інформації

2 ЗАТВЕРДЖЕНО І ВВВДЕНО В ДІЮ наказом Держстандарту України від 11 квітня 1997 р. № 200

3 Вимоги стандарту забезпечують реалізацію норм законе України «Про інформацію», «Про захист інформації в автоматизованих системах» та Положення п технічний захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9.09.94 р. № 632

4 ВВЕДЕНО ВПЕРШЕ

5 РОЗРОБНИКИ: О. Баранов, канд. техн. наук, О. Лаврентьев, М. Семенко

Види інформації, які підлягають технічному захисту$_2$

- **військова таємниця –** це вид таємної інформації, який охоплює відомості у сфері оборони, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди інтересам державної безпеки, бойовій готовності Збройних сил України та інших військових формувань, їх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно із законодавством України



Види інформації, які підлягають технічному захисту$_3$

- **державна таємниця (секретна інформація) –** вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому Законом України “Про державну таємницю”, державною таємницею і підлягають охороні державою.



Загрози для інформації

Загроза для інформації

- **витік інформації** – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання
- **порушення цілісності інформації** – спотворення інформації, її руйнування або знищення
- **блокування інформації** – унеможливлення санкціонованого доступу до інформації
- **загроза для інформації** – витік, можливість блокування або порушення цілісності інформації

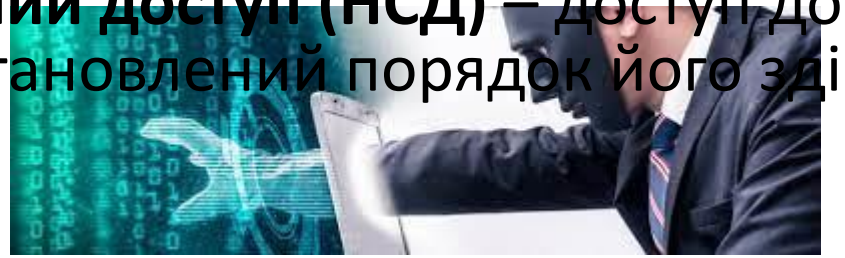


Доступ до інформації

- **модель загроз для інформації** – формалізований опис методів і засобів здійснення загроз для інформації
- **доступ до інформації** – можливість одержання, оброблення інформації та (чи) порушення її цілісності



- **несанкціонований доступ (НСД)** – доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми



Закладний пристрій

- **Закладний пристрій (з а к л а д к а)** - потай встановлюваний технічний засіб, який створює загрозу для інформації





- Під час холодної війни США і СРСР витрачали колосальні кошти на шпигунство, в тому числі і на розробку та впровадження на об'єкти, що охороняються, прослуховуючої апаратури. В 1945 СРСР вдалося сховати жучок в кабінеті американського посла, пристрій виявили лише через сім років.

Програмна закладка

- Програмна закладка - потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері



- Шпигунське програмне забезпечення дозволяє зловмиснику компілювати повідомлення зі сторонніх поштових додатків, таких як вміст та повідомлення WhatsApp, електронні листи Gmail, Facebook або Telegram

Шкідливе програмне забезпечення

- Зловмисне програмне забезпечення (Malware) - це код або програмне забезпечення, яке спеціально розроблено для пошкодження, руйнування, викрадення або загалом виконання інших «поганих» або незаконних дій щодо даних, хостів або мереж.
- Кінцеві пристрої особливо схильні до атак шкідливих програм.
- Три найпоширеніші типи шкідливих програм:
  - вірус
  - хробак
  - троянський кінь

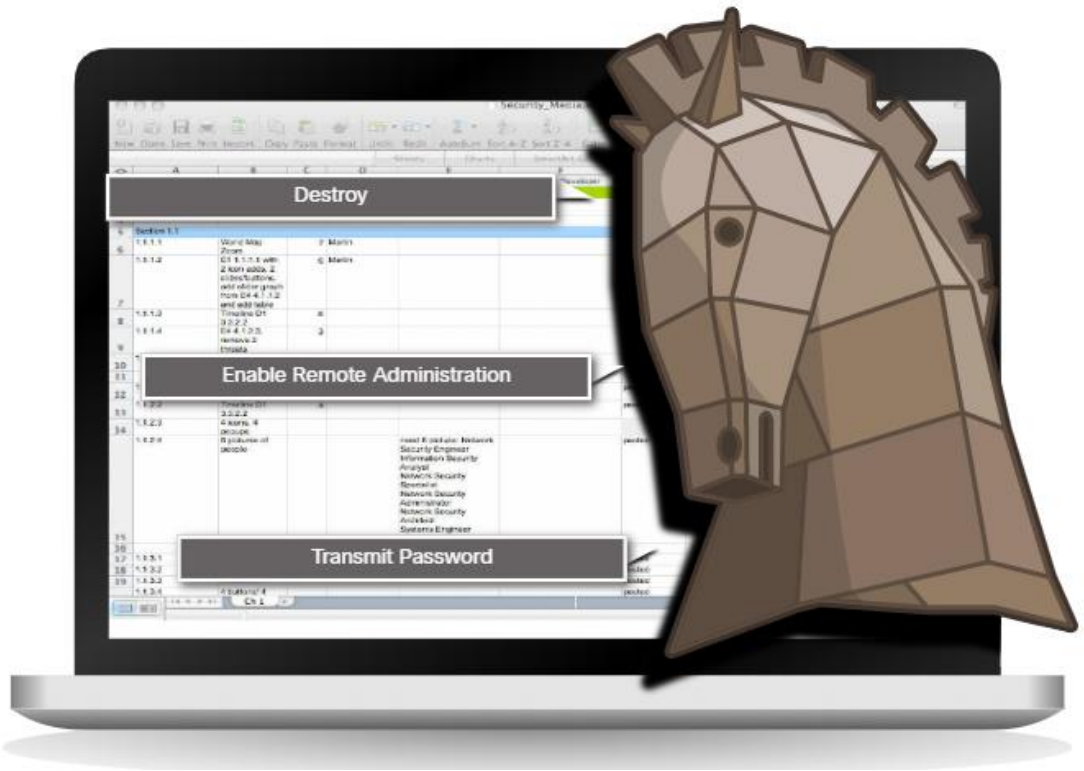
Віруси

- Вірус — це тип зловмисного програмного забезпечення, яке поширюється, вставляючи свою копію в іншу програму. Після запуску програми віруси поширюються з одного комп’ютера на інший, заражаючи комп’ютери. Для поширення більшості вірусів потрібна допомога людини.
- Простий вірус може встановити себе в першому рядку коду виконуваного файлу. Після активації вірус може перевірити диск на наявність інших виконуваних файлів, щоб заразити всі файли, які він ще не інфікував.
- Віруси також можна запрограмувати на мутацію, щоб уникнути виявлення.
- Зараз більшість вірусів поширюється через USB-накопичувачі, компакт-диски, DVD-диски, спільні мережеві ресурси та електронну пошту.

65

Троянські коні

- Шкідливе програмне забезпечення «Троян» — це програмне забезпечення, яке виглядає легітимним, але воно містить шкідливий код, який використовує привілеї користувача, який його запускає.
- Часто трояни зустрічаються прикріпленими до онлайн-ігор. Користувачів зазвичай обманом змушують завантажити та запустити троянського коня у своїх системах. Граючи в гру, користувач не помітить проблеми. У фоновому режимі в системі користувача встановлено троянський кінь. Шкідливий код троянського коня продовжує працювати навіть після закриття гри.
- Концепція троянського коня є гнучкою. Він може завдати миттєвої шкоди, забезпечити віддалений доступ до системи або доступ через чорний хід. Він також може виконувати дії за вказівками віддалено, наприклад «надсилати мені файл паролів раз на тиждень».

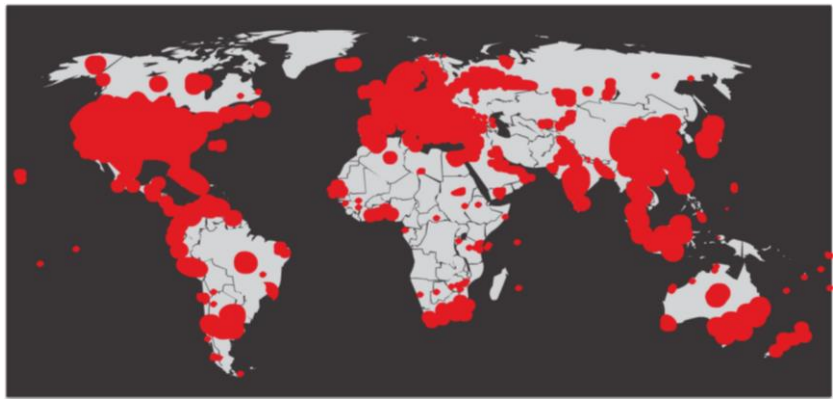


Хробаки

- Комп’ютерні хробаки схожі на віруси, оскільки вони розмножуються, самостійно використовуючи вразливі місця в мережах.
- Хробаки можуть сповільнювати роботу мереж, коли вони поширюються від системи до системи.
- Хробаки можуть працювати без хост-програми.
- Однак після зараження хоста хробак швидко поширюється мережею.
- У 2001 році хробак Code Red спочатку заразив 658 серверів. Протягом 19 годин хробак заразив понад 300 000 серверів.



Початковий код - зараження червоним хробаком



Червоний код інфекції через 19 годин

Технічна розвідка

- **технічна розвідка** – несанкціоноване здобування інформації за допомогою технічних засобів та її аналіз
- **модель технічної розвідки** – формалізований опис методів, засобів і можливостей технічної розвідки



Технічні канали витоку інформації

Носій інформації

- **носій інформації** – матеріальний об’єкт, що містить інформацію, яка підлягає захисту від загроз



Інформативний сигнал

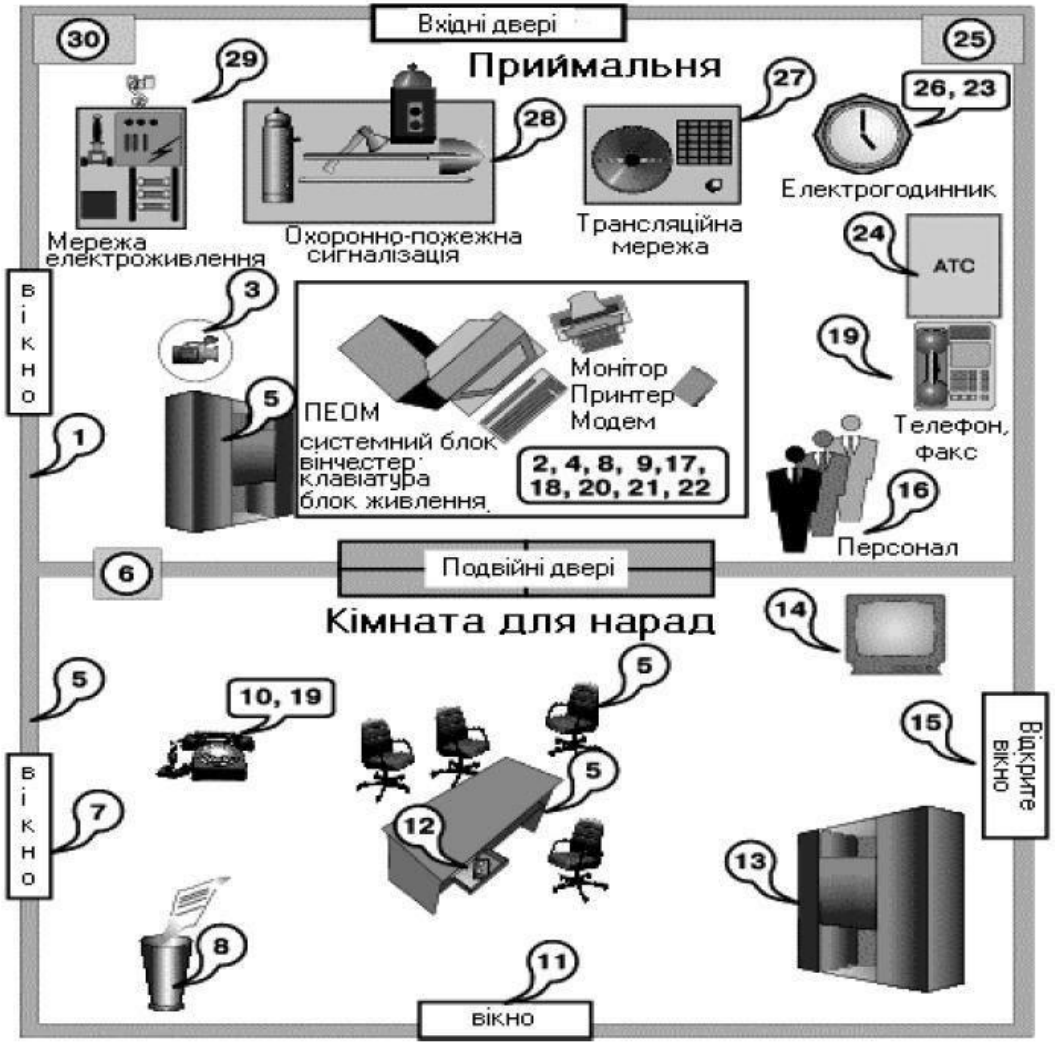
- **інформативний сигнал** – фізичні поля та (чи)хімічні речовини, що містять інформацію з обмеженим доступом





Технічний канал витоку інформації

- **(технічний) канал витоку інформації** – сукупність носіїв інформації, середовища її поширення та засобів технічної розвідки



Самочинний канал витоку інформації

- **самочинний (технічний) канал витоку інформації (ненавмисний канал витоку інформації)** – технічний канал витоку інформації, в якому носії інформації та (чи) середовище їх поширення формуються самочинно

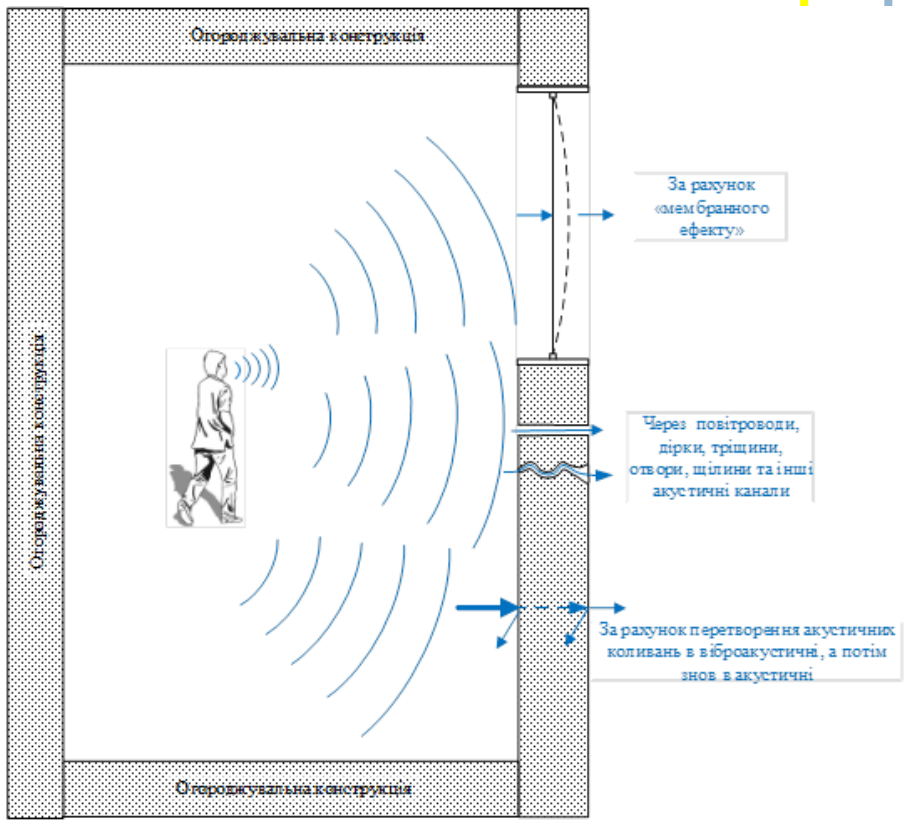


Рис. 1. Три можливих шляхи витоку акустичної інформації за межі огороджувальних конструкцій

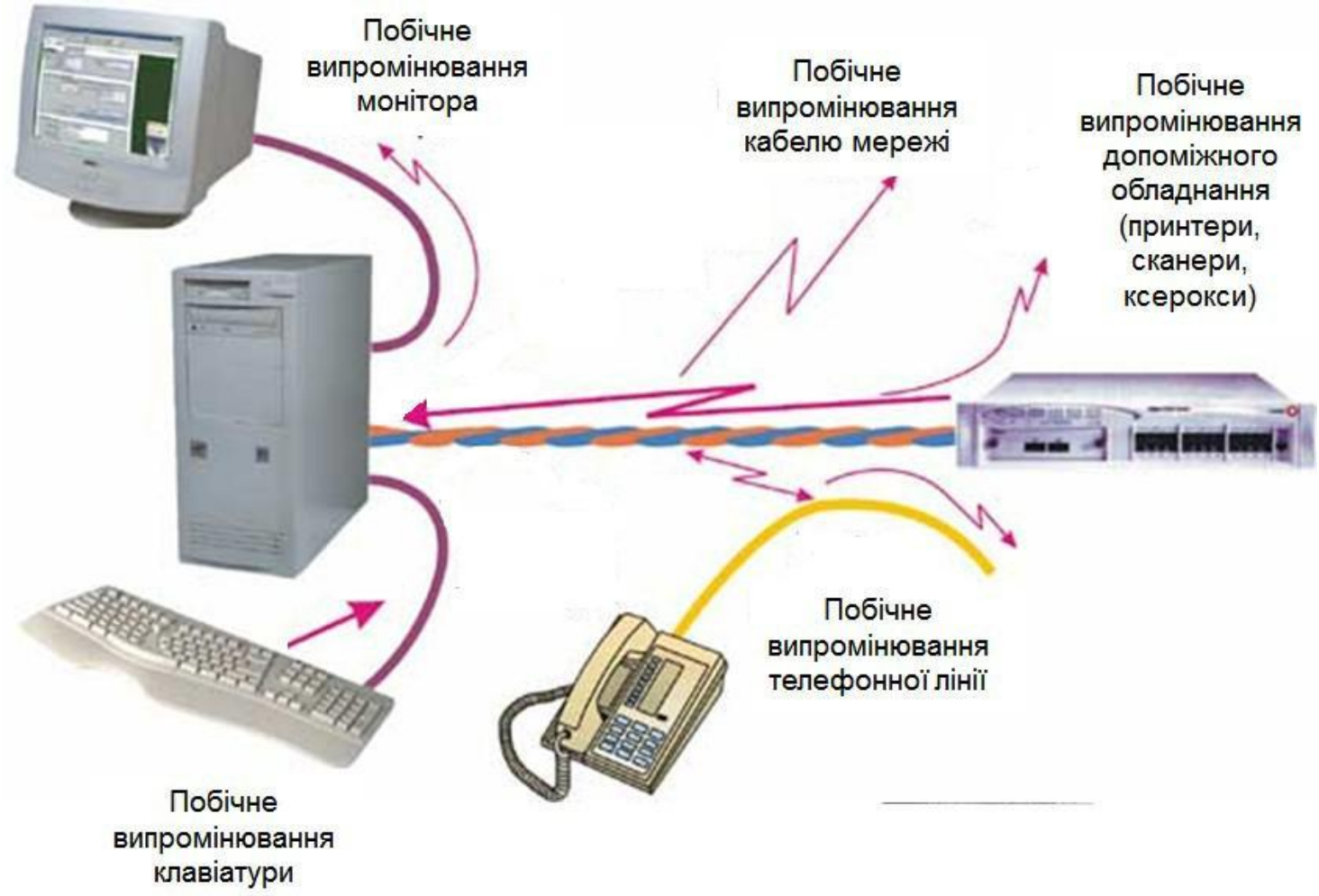
Штучний канал витоку інформації

- **штучний (технічний) канал витоку інформації** (навмисний канал витоку інформації) – технічний канал витоку інформації, створений за допомогою спеціальних технічних засобів



Побічне електромагнітне випромінювання і наведення (ПЕМВН)

- **побічне електромагнітне випромінювання і наведення (ПЕМВН)** – електромагнітне випромінювання і наведення, що є побічним результатом функціонування технічних засобів і може бути носієм інформації



Технічний захист інформації (ТЗІ)

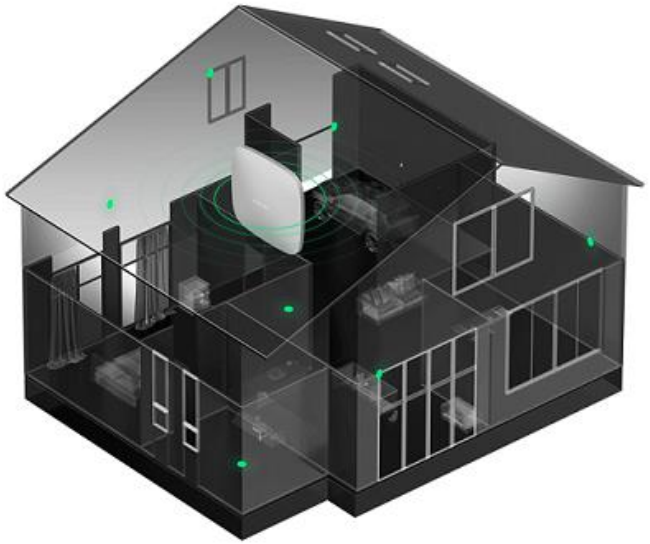
Технічний захист інформації

- **технічний захист інформації (ТЗІ)** – діяльність, спрямована на запобігання витоку інформації технічними каналами, її блокування та (чи) порушення цілісності
- **(технічний) засіб із захистом; захищений (технічний) засіб; захищена техніка; (ТЗІ)** – технічний засіб, в якому функція захисту інформації від загроз є додатковою до основної
- **засіб технічного захисту інформації** – пристрій та (чи) програмний засіб, в яких функція захисту інформації є основною
- **система технічного захисту інформації** – сукупність організаційних структур, нормативно-правових документів та матеріально-технічної бази



Рівень захисту інформації

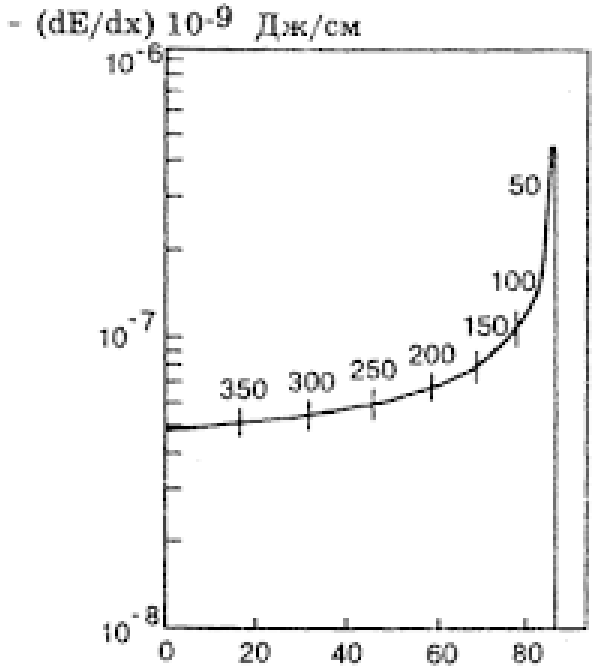
- **зона безпеки інформації** – простір, у межах якого інформація знаходиться в безпеці
- **рівень (технічного) захисту інформації** – сукупність вимог, у тому числі нормованих, що визначаються режимом доступу до інформації та загрозами її безпеці
- **ефективність (технічного) захисту інформації** – ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам





Пасивне приховування інформації

- **пасивне приховування інформації** - приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин



Активне приховування інформації

- **активне приховування інформації** – приховування інформації створенням таких фізичних полів та речовин, які утруднюють здобування інформації або спричиняють невизначеність її змісту



Дезінформування

- **дезінформування** – спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації



Об'єкт ТЗІ

- **Об’єктом технічного захисту є інформація**, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (**інформація з обмеженим доступом – ІзОД**).
- **Об’єкт захисту, мету і завдання ТЗІ визначають** і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами з ТЗІ.

Згідно з вимогами стандарту України „Про інформацію”, „Про державну таємницю”, „Про захист інформації в автоматизованих системах”, затвердженого постановою Кабінету Міністрів України від 11.10.96 р. № 423: ДСТУ 3396.0-96, існують наступні положення щодо технічного захисту інформації.



Носій ІзОД

- **Носіями ІзОД** можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва та експлуатації продукції різного призначення (інформаційна діяльність)

Згідно з вимогами стандарту України „Про інформацію”, „Про державну таємницю”, „Про захист інформації в автоматизованих системах”, затвердженого постановою Кабінету Міністрів України від 11.10.96 р. № 423: ДСТУ 3396.0-96, існують наступні положення щодо технічного захисту інформації.

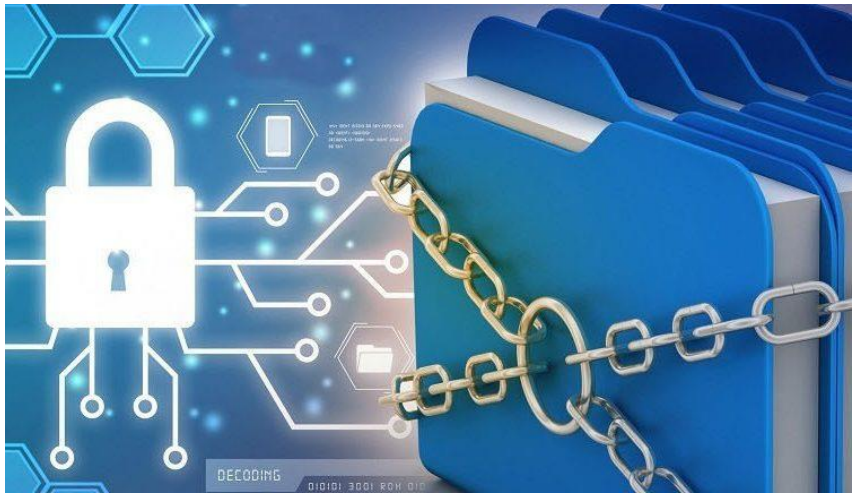


Мета та етапи ТЗІ

Мета та етапи ТЗІ

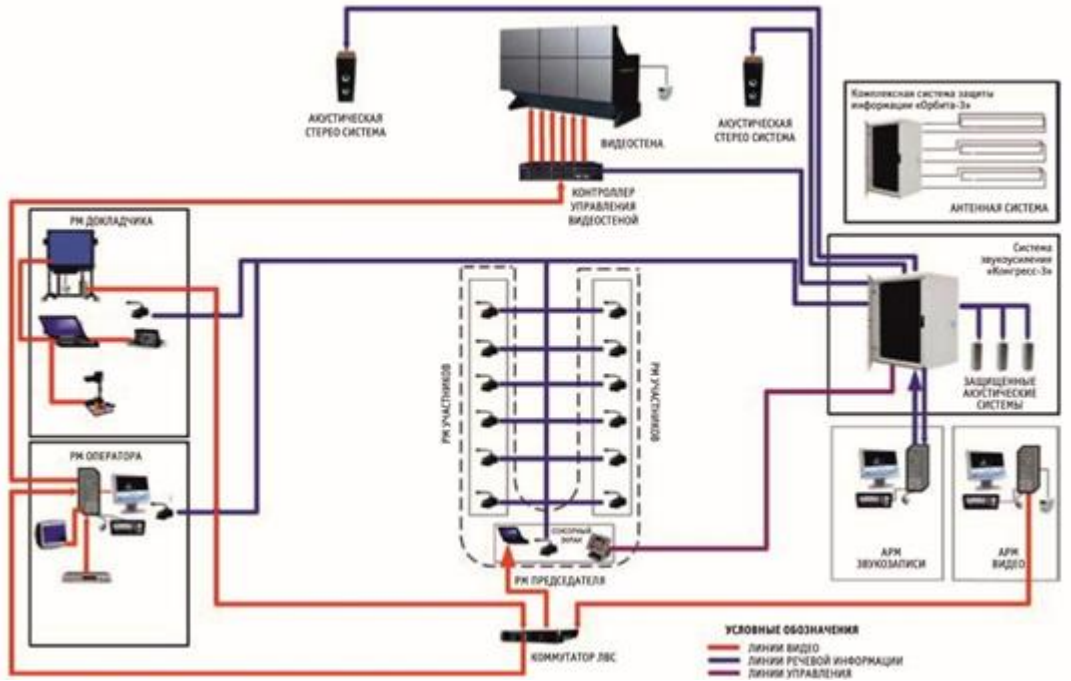
- **Метою ТЗІ** є запобігання витоку або порушенню цілісності ІзОД, що може бути досягнуто шляхом побудови системи захисту інформації з організованою сукупністю методів і засобів забезпечення ТЗІ.
- Технічний захист інформації здійснюється поетапно:
  - **перший етап** – визначення та аналіз загроз
  - **другий етап** – розроблення системи захисту інформації
  - **третій етап** – реалізація плану захисту інформації
  - **четвертий етап** – контроль функціонування та керування системою захисту інформації

Згідно з вимогами стандарту України „Про інформацію”, „Про державну таємницю”, „Про захист інформації в автоматизованих системах”, затвердженого постановою Кабінету Міністрів України від 11.10.96 р. № 423: ДСТУ 3396.0-96, існують наступні положення щодо технічного захисту інформації.



Перший етап ТЗІ – визначення та аналіз загроз$_1$

- На першому етапі необхідно здійснити аналіз об’єктів ТЗІ, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.



Перший етап ТЗІ – визначення та аналіз загроз$_2$

- **Джерелами загроз** може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб



Перший етап ТЗІ – визначення та аналіз загроз$_3$

- Загрози можуть здійснюватися:
  - технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;
  - каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
  - несанкційованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.



Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз

Другий етап ТЗІ – розроблення системи захисту інформації$_1$

- **На другому етапі** слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.
- **Організаційні заходи** регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об’єкта ТЗІ.
- **Первинні технічні заходи** передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.
- **Основні технічні заходи** передбачають захист інформації з використанням засобів забезпечення ТЗІ.



Другий етап ТЗІ – розроблення системи захисту інформації$_2$

- Для технічного захисту інформації слід застосовувати спосіб приховування або спосіб технічної дезінформації.
- Заходи захисту інформації повинні:
  - бути відповідними загрозам;
  - бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;
  - забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.



Другий етап ТЗІ – розроблення системи захисту інформації$_3$

- Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.
- Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.



Другий етап ТЗІ – розроблення системи захисту інформації$_4$

- Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами системи ТЗІ.

Закони України
"Про Національну систему конфіденційного зв'язку" (2919-14)
"Про захист інформації в інформаційно-телекомунікаційних системах",
"Про інформацію" (2657-12).

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

Третій етап ТЗІ – реалізація плану захисту інформації$_1$

- **На третьому етапі** слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.



ЕКСПЕРТНИЙ ВИСНОВОК

Пристрої мережевої безпеки серії WatchGuard XTM виробництва компанії WatchGuard Technologies, Inc., США

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України "01" березня 2013 р. за № 424
Дійсний до "01" березня 2016 р.
Перший заступник Голови Служби О.Г. Цуркан
м. п.

За результатами експертизи встановлено, що
функції захисту від несанкціонованого доступу пристроїв
назва засобу технічного захисту інформації
мережевої безпеки серії WatchGuard XTM
(моделі 2x, 3x, 3xx, 5xx, 8xx, 10xx. 20xx) під керуванням
операційної системи Fireware XTM (Fireware XTM Pro) версії 11.4,

які надано на експертизу ТОВ "ІТ Ленд",
назва та адреса організації
04111, м. Київ, вул. Щербакова, 45-А,
відповідають
відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Пристрої мережевої безпеки серії "WatchGuard XTM" (моделі 2x, 3x, 3xx, 5xx, 8xx, 10xx. 20xx). Технічні вимоги за критеріями технічного захисту інформації", сукупність яких визначається функціональним профілем захищеності: **КА-1, КА-2, ЦА-1, ЦА-2, ЦО-2, ДР-1, ДВ-1, НР-1, НИ-1, НИ-2, НК-1, НО-2, НЦ-1** з рівнем гарантій **Г-2** коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.

Вимоги до умов експлуатації та сфери використання об'єкта експертизи визначені у відповідному розділі цього експертного висновку.

«ТЗІ»

Директор ТОВ "ТЗІ" М.П. Майструк
керівник організатора експертизи підпис ініціали, прізвище
м.п.

Третій етап ТЗІ – реалізація плану захисту інформації$_2$

- **Технічний захист інформації забезпечується** застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (засоби ТЗІ) та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженернотехнічних споруд, засобів і систем (засоби забезпечення ТЗІ).



ЛАВИНА-Е

КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ

Детальніше



ТРИТОН-Е

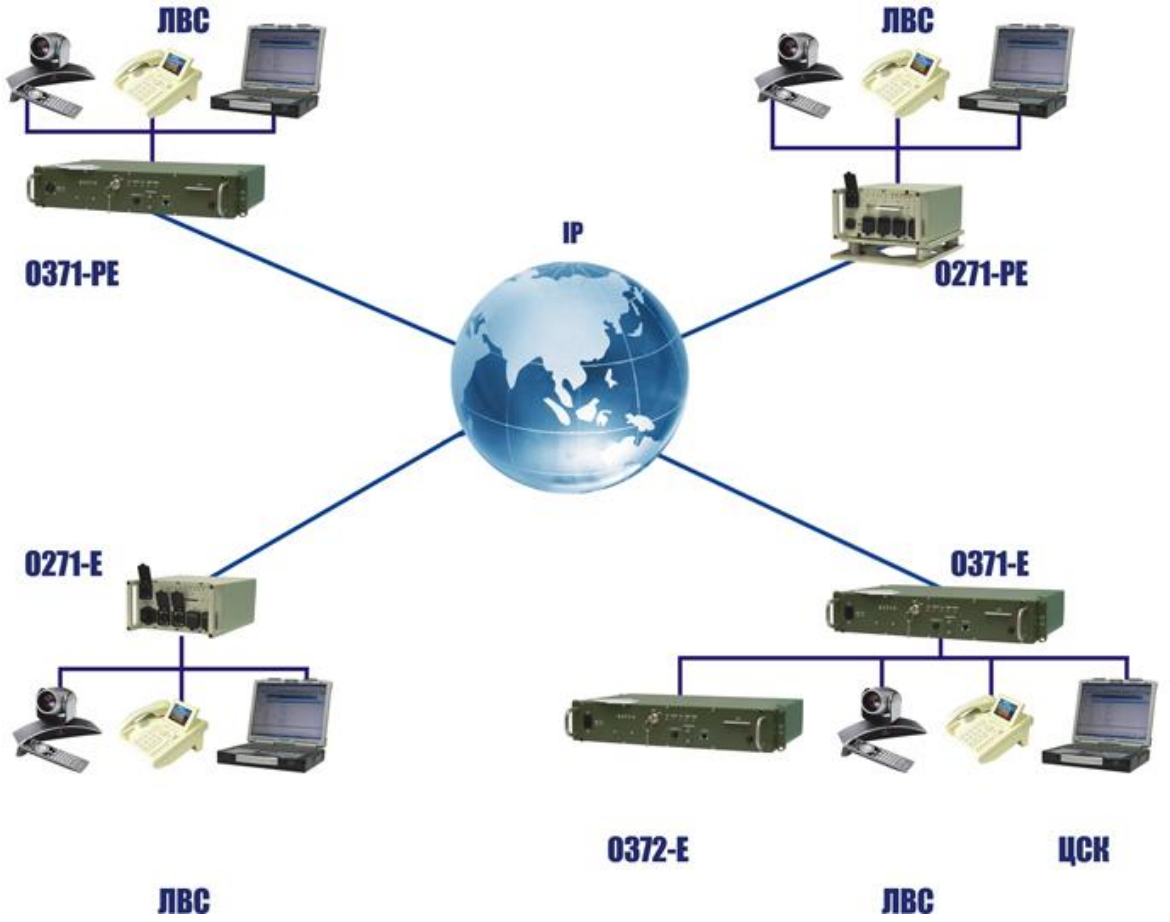
ШИФРАТОР З ІНТЕГРОВАНИМ МОДУЛЕМ КОМУТАЦІЇ

Детальніше



Третій етап ТЗІ – реалізація плану захисту інформації$_3$

- Засоби ТЗІ можуть функціювати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.



Третій етап ТЗІ – реалізація плану захисту інформації$_4$

- Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.
- Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.



ЕКСПЕРТНИЙ ВИСНОВОК

Пристрої мережевої безпеки серії WatchGuard XTM виробництва компанії WatchGuard Technologies, Inc., США

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України "01" березня 2013 р. за № 424
Дійсний до "01" березня 2016 р.
Перший заступник Голови Служби О.Г. Цуркан
м. п.

За результатами експертизи встановлено, що
функції захисту від несанкціонованого доступу пристроїв
назва засобу технічного захисту інформації
мережевої безпеки серії WatchGuard XTM
(моделі 2x, 3x, 3xx, 5xx, 8xx, 10xx. 20xx) під керуванням
операційної системи Fireware XTM (Fireware XTM Pro) версії 11.4,

які надано на експертизу ТОВ "ІТ Ленд",
назва та адреса організації
04111, м. Київ, вул. Щербакова, 45-А,
відповідають
відповідає, не відповідає

вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Пристрої мережевої безпеки серії "WatchGuard XTM" (моделі 2x, 3x, 3xx, 5xx, 8xx, 10xx. 20xx). Технічні вимоги за критеріями технічного захисту інформації", сукупність яких визначається функціональним профілем захищеності: КА-1, КА-2, ЦА-1, ЦА-2, ЦО-2, ДР-1, ДВ-1, НР-1, НИ-1, НИ-2, НК-1, НО-2, НЦ-1 з рівнем гарантій Г-2 коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.

Вимоги до умов експлуатації та сфери використання об'єкта експертизи визначені у відповідному розділі цього експертного висновку.

«ТЗІ»

Директор ТОВ "ТЗІ" М.П. Майструк
керівник організатора експертизи підпис ініціали, прізвище
м. п.

Четвертий етап ТЗІ – контроль функціонування та керування системою захисту інформації

- **На четвертому етапі** слід провести аналіз функціювання системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати засадничі дані для керування системою захисту інформації.
- **Керування системою захисту інформації** полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.
- У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації.
- Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами.



Донецький національний технічний університет



Тема 2. Побудова комплексу технічного захисту інформації. Лекція 3. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. НД ТЗІ 1.1-005-07.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Визначення та загальні положення
- ДБН А.2.2-2-96
- НД ТЗІ 1.1-005-07

Визначення та загальні положення

Посилання на НПД

- 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.
- ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.
- ДБН А.2.2-3-2004 Проектування. Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
- НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні 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 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

Визначення$_1$

- **АТЕСТАЦІЯ** – визначення відповідності виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності вимогам нормативних документів з питань ТЗІ.
- **Випробування (комплексу ТЗІ)** – сукупність аналітичних, експериментальних та вимірювальних робіт, які проводяться з метою визначення повноти виконання вимог щодо захисту від витоку інформації з обмеженим доступом технічними каналами, а також перевірки (контролю) повноти та достатності реалізованих заходів із захисту інформації на об'єктах інформаційної діяльності.
- **Інформація з обмеженим доступом** – інформація, що становить державну або іншу передбачену законом таємницю, а також службова інформація, а також конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”, та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом.

Визначення$_2$

- **Комплекс ТЗІ** – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності.

- **Об’єкт інформаційної діяльності** – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом.

Загальні положення$_1$

- Захисту від витоку технічними каналами на ОІД підлягає інформація, що становить державну таємницю.
- Захист іншої ІзОД від витоку технічними каналами на ОІД здійснюється за рішенням розпорядника цієї інформації.
- Створення комплексу ТЗІ передбачає проведення організаційних, інженерних і технічних заходів на ОІД, а саме:
  - озвучення ІзОД (при проведенні нарад, під час показів зі звуковим супроводженням кіно- і відеофільмів тощо);
  - здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);
  - обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

Загальні положення$_2$

- У СТВОРЕННІ КОМПЛЕКСУ ТЗІ БЕРУТЬ УЧАСТЬ:
  - установа, яка є замовником створення комплексу ТЗІ (замовник або установа-замовник);
  - виконавець робіт зі створення комплексу ТЗІ (виконавець робіт з ТЗІ);
  - виконавець проведення випробувань щодо створення комплексу ТЗІ (виконавець випробувань);
  - виконавець проведення атестації комплексу ТЗІ (виконавець атестації).
- УСТАНОВА-ЗАМОВНИК може бути виконавцем робіт з ТЗІ і виконавцем випробувань або може залучати до виконання таких робіт і випробувань суб'єктів господарської діяльності, що мають ліцензії на провадження діяльності у сфері ТЗІ.
- Атестацію комплексу ТЗІ здійснює виконавець, що має відповідну ліцензію або дозвіл на провадження діяльності у сфері ТЗІ.
- У створенні комплексу ТЗІ (залежно від характеру, складності та обсягу робіт) можуть брати участь один або декілька виконавців. У цьому разі замовник визначає головного виконавця.

Загальні положення$_3$

- УСТАНОВА-ЗАМОВНИК ДЛЯ СТВОРЕННЯ КОМПЛЕКСУ ТЗІ ТАКОЖ ЗАЛУЧАЄ:
  - свої структурні підрозділи, діяльність яких пов’язана з ІзОД та які обґрунтовують необхідність і заявляють про створення комплексу ТЗІ (підрозділи-заявники створення комплексу ТЗІ);
  - призначену за необхідністю посадову особу з відповідною фаховою підготовкою для організації та координації робіт на всіх етапах створення комплексу ТЗІ, а також для організації експлуатації цього комплексу;
  - підрозділ або посадові особи з відповідною фаховою підготовкою, яким доручено супроводження робіт з ТЗІ в установі (підрозділ ТЗІ), службу захисту інформації в ІТС;
  - інші підрозділи установи, які залучаються для формування положень щодо використання в інформаційній діяльності ІзОД, проведення обстеження, категорування об'єктів тощо.

Загальні положення$_4$

- Рішення щодо необхідності створення (модернізації) комплексу ТЗІ готує замовник на стадіях проектування, нового будівництва, розширення, реконструкції (будівництво) ОІД (об'єкт інформаційної діяльності), а також у разі змін умов функціонування ОІД.
- Будівництво ОІД може виконуватися за відповідною проектнокошторисною документацією.
- При цьому повинні бути враховані вимоги ДБН А.2.2-2 і ДБН А.2.2-3.

ДБН А.2.2-2-96

Рішення щодо заходів ТЗІ

- Рішення щодо заходів ТЗІ приймає замовник проектної документації для будівництва (далі -замовник) на підставі чинних вимог і норм.
- На етапі проектування здійснюється розроблення організаційних і технічних заходів захисту ІзОД, що адекватні загрозам і забезпечують заплановані техніко-економічні показники для встановлених рівнів захисту інформації протягом часу обмеження доступу до неї або здійснення загроз її безпеці.
- Технічний захист ІзОД передбачає застосування систем інженерно-технічних споруд разом із засобами забезпечення ТЗІ.

Вимоги ТЗІ

- Вимоги ТЗІ повинні бути викладені в завданні на проектування заходів ТЗІ і враховуватися в процесі проектування об'єкта, зокрема під час розробки:
  - ситуаційного плану розміщення об'єкта;
  - технології виробництва;
  - принципових схем виробничих технологічних процесів;
  - схеми генерального плану виробничого комплексу;
  - архітектурно-будівельних рішень щодо об'єкта;
  - принципових рішень з організації систем зв'язку, сигналізації, управління, автоматизованих та інших систем;
  - основних рішень з організації будівництва.
- Завдання на проектування заходів ТЗІ повинно бути складовою частиною загального завдання на проектування об'єкта.

Урахування вимог ТЗІ при проектуванні та будівництві

- Відомості про ліцензії на проведення проектних робіт, зміст загального завдання на проектування об'єкта, стадії розроблення проектної документації наведені в державних будівельних нормах (ДБН) про порядок розробки, узгодження і затвердження проектної документації для будівництва.
- Під час розроблення проектної документації для будівництва з урахуванням вимог ТЗІ необхідно керуватися чинним законодавством України, державними стандартами, будівельними нормами і нормативними документами системи ТЗІ.
- Витрати на проектування і будівництво, що пов'язані з реалізацією заходів ТЗІ, включаються до загального кошторису на проектування та будівництво об'єкта.

Підготовчі роботи з ТЗІ

- Необхідність розробки проектної документації для будівництва об'єкта з урахуванням вимог ТЗІ повинна бути визначена після виконання наступних підготовчих робіт:
  - визначення переліку приміщень, в яких циркулює інформація, що підлягає технічному захисту;
  - обгрунтування необхідності розроблення заходів захисту ІзОД з урахуванням шкоди від її витоку або порушення цілісності;
  - уточнення меж контролюємої території на основі аналізу загроз безпеці інформації;
  - визначення головних задач технічного захисту ІзОД;
  - визначення шляхів і засобів реалізації заходів ТЗІ з урахуванням технічної та економічної доцільності.

Завдання на проектування заходів ТЗІ

- До початку виконання проектних робіт замовник, при необхідності, готує перелік вихідних даних для вирішення питань з ТЗІ.
- Підсумки підготовчих робіт і вихідні дані є підставою для розроблення завдання на проектування заходів ТЗІ.
- У цьому завданні мають бути викладені:
  - мета, задачі, вимоги ТЗІ;
  - вихідні дані для проектування комплексного ТЗІ;
  - вимоги до контролю за реалізацією передбачених заходів ТЗІ.
- Завдання на проектування заходів ТЗІ розробляється замовником і узгоджується з проектною організацією і, при необхідності, із організацією, якій підпорядкований замовник.
- Завдання на проектування заходів ТЗІ для особливо важливих об'єктів узгоджуються з уповноваженим Кабінетом Міністрів України органом.
- У випадку висування замовником у ході проектування додаткових вимог технічного захисту ІзОД, що потребують коректування прийнятих рішень чи кошторисної вартості будівництва, завдання на проектування заходів ТЗІ коректується згідно з встановленим порядком.

Розроблення проектної документації$_1$

Розроблення документації передпроектних досліджень

- Зміст робіт з ТЗІ при виконанні передпроектних досліджень:
  - виявлення характерних особливостей об'єкта, які впливають на вибір проектних рішень з ТЗІ;
  - оцінка умов реалізації заходів ТЗІ;
  - орієнтовний вибір основних проектних рішень з ТЗІ та їх економічне обґрунтування;
  - обґрунтування вибору майданчика для будівництва.
- Під час вибору майданчика для будівництва з урахуванням заходів ТЗІ беруть до уваги специфічні вимоги до об'єкта та оточуючої місцевості.
- До складу комісії (комплексної бригади) з вибору майданчика для будівництва включаються фахівці з ТЗІ від замовника та від проектної організації.
- Прийняті рішення з ТЗІ викладаються в окремому розділі документації передпроектних досліджень, що має назву **<Заходи ТЗІ>**.
- Проектні рішення з ТЗІ є складовою частиною технологічних, планувальних, архітектурних і конструкторських рішень і повинні розроблятися відповідними підрозділами проектної організації без розкриття їх призначення.

Розроблення проектної документації$_2$

Розроблення проектної документації для будівництва

- Проектна документація для будівництва об'єкта виконується на підставі завдання на проектування та затвердженого ескізного проекту або техніко-економічного обґрунтування (документація передпроектних досліджень).
- У проектній документації повинні бути враховані вимоги ТЗІ при розробці:
  - технології виробництва;
  - генерального плану;
  - будівель і споруд;
  - систем інженерного забезпечення виробництва та технічних засобів.
- Проектна документація розробляється авторами рішень з ТЗІ, які розробляли ескізний проект або техніко-економічне обґрунтування.
- До складу проектної документації на здійснення заходів з ТЗІ повинні входити:
  - робочі креслення;
  - кошторисна документація;
  - специфікація устаткування і матеріалів.
- Обґрунтування рішень з ТЗІ, що передбачені у розділах проектної документації, викладаються в окремому розділі **<Заходи ТЗІ>** загальної пояснювальної записки. У решті розділів проектної документації, при необхідності, слід робити посилання на розділ **<Заходи ТЗІ>**.

Розроблення проекту організації будівництва

- Необхідність включення заходів ТЗІ до проекту організації будівництва об'єкта визначається потребою реалізації додаткових заходів ТЗІ під час його будівництва.

- Забезпечення виконання передбачених проектом організації будівництва рішень з ТЗІ на об'єктах покладається на їх керівників.

Експертиза проектної документації

- Проектна документація з ТЗІ підлягає експертизі на загальних підставах згідно з визначеним порядком проведення державної експертизи інвестиційних проектів і програм та допуску посадових осіб до матеріалів з ТЗІ.
- Під час експертизи проектної документації на будівництво перевіряються:
  - відповідність технічних рішень затвердженому завданню на проектування заходів ТЗІ;
  - дотримання вимог нормативних документів системи ТЗІ;
  - відповідність рівня виконаних розробок сучасному стану науки і техніки в галузі ТЗІ.
- У висновку експертизи повинні бути зазначені результати виконання вимог ТЗІ в проектній документації на будівництво.
- Висновки експертизи заносяться до окремого розділу експертної документації.
- Експертизу проектної документації на будівництво особливо важливих об'єктів необхідно проводити у встановленому порядку за участю спеціалістів з питань ТЗІ.
- Висновки експертизи повинні бути подані в орган, що погодив завдання на проектування заходів ТЗІ.

Авторський нагляд

- Авторський нагляд за реалізацією заходів ТЗІ, що передбачені проектною документацією, здійснюється проектною організацією згідно з вимогами чинного положення про авторський нагляд за будівництвом об'єктів.
- Авторський нагляд проводиться в процесі будівництва об'єкта та прийняття його до експлуатації.
- Результати авторського нагляду мають бути відображені в об'єктовому журналі і доведені до відома представників замовника і підрядника.

Основні функції замовника

- ЗАМОВНИК ПОВИНЕН:
  - приймати рішення щодо необхідності ТЗІ;
  - готувати і передавати у визначеному порядку проектній організації завдання на проектування заходів ТЗІ;
  - видавати проектній організації, при необхідності, додаткові дані для прийняття рішень з ТЗІ;
  - організовувати перевірку якості робіт з ТЗІ;
  - висувати, при необхідності, додаткові вимоги ТЗІ та вносити відповідні зміни (доповнення) до завдання на проектування заходів ТЗІ;
  - брати участь у розробленні заходів ТЗІ;
  - контролювати хід виконання робіт з ТЗІ;
  - зупиняти виконання робіт, якщо є відхилення від проектних рішень з ТЗІ.

Основні функції проектної організації

- ПРОЕКТНА ОРГАНІЗАЦІЯ ПОВИННА:
  - організовувати й виконувати проектні роботи згідно із завданням та цим ДБН;
  - видавати субпідрядним організаціям завдання на проведення інженерно-вишукувальних робіт з урахуванням вимог ТЗІ;
  - коректувати проектно-кошторисну документацію за результатами експертизи;
  - організовувати та здійснювати авторський нагляд за реалізацією проектних рішень з ТЗІ в процесі виконання будівельно-монтажних робіт;
  - зупиняти проведення будівельно-монтажних робіт, якщо вони мають відхилення від проектних рішень з ТЗІ;
  - подавати замовнику пропозиції про внесення до завдання змін (доповнень), якщо в ході проектування з'явилась можливість підвищити ефективність проектних рішень з ТЗІ або значно знизити кошторисну вартість;
  - дотримуватись відповідних режимних вимог під час вишуку, проектування, авторського нагляду за будівництвом об'єкта.

Основні функції будівельно-монтажної організації

- БУДІВЕЛЬНО-МОНТАЖНА ОРГАНІЗАЦІЯ ПОВИННА:
  - своєчасно та якісно виконувати роботи щодо реалізації передбачених проектною документацією заходів ТЗІ;
  - вносити у визначеному порядку пропозиції щодо покращання техніко-економічних показників робіт.

НД ТЗІ 1.1-005-07

Загальні положення$_1$

- Комплекс ТЗІ повинен створюватися виходячи із перспектив модернізації і розвитку інших комплексів ТЗІ установи, охоронних, протипожежних чи загальних систем безпеки установи, спеціальних систем енергоживлення, життєзабезпечення тощо, а також забезпечувати виконання норм ефективності захищеності інформації, відповідати експлуатаційним вимогам щодо необхідності та періодичності перевірок цієї захищеності.
- Засоби забезпечення захисту інформації застосовують у складі комплексу ТЗІ за наявності сертифіката відповідності Системи УкрСЕПРО вимогам НД з питань ТЗІ або позитивного висновку державної експертизи у сфері ТЗІ.

Загальні положення$_2$

- Застосування імпортних засобів забезпечення захисту інформації можливе лише за умови відсутності вітчизняних аналогів при наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або одержання позитивного експертного висновку.
- Джерела фінансування робіт зі створення комплексу ТЗІ визначає замовник.
- Витрати на проектування, будівельно-монтажні роботи, проведення випробувань щодо ТЗІ, атестації комплексу ТЗІ вносяться до кошторису на будівництво та експлуатацію (утримання) ОІД.

Основні заходи щодо організації створення комплексу ТЗІ$_1$

- Підрозділ-заявник створення комплексу ТЗІ (або призначена посадова особа щодо організації та координації робіт на всіх етапах створення, а також експлуатації комплексу) разом з підрозділом ТЗІ готує і подає на затвердження керівнику установи-замовника:
  - протокол про визначення вищого ступеня обмеження доступу до інформації (додаток А);
  - проект рішення щодо створення комплексу ТЗІ на ОІД (основою для проведення робіт щодо створення комплексу може бути затверджений Протокол про визначення вищого ступеня обмеження доступу до інформації).

Основні заходи щодо організації створення комплексу ТЗІ$_2$

Додаток А
(довідковий)

Форма та зміст протоколу про визначення вищого ступеня обмеження доступу до інформації

Ступінь обмеження доступу
Прим. № __

ЗАТВЕРДЖЕНО
Керівник установи-замовника
_____
____. ____. 20__

ПРОТОКОЛ
про визначення вищого ступеня обмеження доступу до інформації

_____
(назва, належність структурного підрозділу установи, де буде створюватися комплекс ТЗІ)

1. Відомості про інженерно-технічну споруду (належність, склад, дислокація), в межах якої планується створення комплексу ТЗІ, опис об'єкта інформаційної діяльності (межі об'єкта, схеми тощо).
2. Результати проведення аналізу особливостей функціонування об'єкта інформаційної діяльності (табл. 1).

Таблиця 1

Найменування приміщень, де ІзОД озвучується та/або обробляється технічними засобами тощо	Характеристика ІзОД (сфера діяльності, зміст відомостей, умови озвучення, засоби оброблення тощо)	Стаття, пункт ЗВДТ, ВДТ, ВДСК	Ступінь обмеження доступу до інформації
1	2	3	4

Примітки.
1 Ступінь обмеження доступу до інформації встановлюється згідно з даними:
- Зводу відомостей, що становлять державну таємницю (ЗВДТ), або затверджених розгорнутих відомчих переліків відомостей, які за режимом доступу віднесені до державної таємниці (ВДТ);
- затверджених відомчих переліків відомостей, які за режимом доступу належать до службової інформації (ВДСК).
2 Протокол підписують представники від підрозділу-заявника на створення комплексу ТЗІ. У разі необхідності, протокол також підписують представники підрозділу ТЗІ, служби захисту інформації в АС, режимно-секретного органу, секретаріату (канцелярії).
3 Протокол може бути поданий на розгляд комісією з категорування, що призначена наказом керівника установи (№, дата надання чинності).

Роль установи-замовника

- Установа-замовник також:
  - готує пропозиції щодо термінів проведення обстеження на ОІД (оформлення відповідних протоколів, актів), проведення категорування об'єктів;
  - створює модель загроз для ІзОД (стосовно забезпечення захисту від витоку ІзОД можливими технічними каналами);
  - організовує розроблення технічних завдань щодо створення комплексу ТЗІ на ОІД (технічних вимог з питань ТЗІ);
  - узгоджує зміни до прийнятих рішень з ТЗІ, якщо необхідність їх внесення обґрунтована результатами випробувань комплексу ТЗІ, надає виконавцю атестації комплексу ТЗІ дані про його створення на ОІД, а також висновки за результатами випробувань;
  - створює необхідні умови для виконання випробувань і проведення атестації комплексу ТЗІ.

Роль виконавця робіт ТЗІ$_1$

- Виконавець робіт з ТЗІ та виконавець випробувань забезпечують:
  - проведення заходів щодо недопущення встановлення закладних пристроїв несанкціонованого отримання інформації під час виконання будівельних та монтажно-налагоджувальних робіт, прокладення нових інженерних комунікацій, встановлення технологічного обладнання, засобів оргтехніки, елементів інтер'єру, меблів тощо;
  - проведення випробувань (у т.ч. спеціальних досліджень технічних засобів, які оброблятимуть ІзОД) з метою визначення повноти та достатності виконання вимог щодо захисту від витоку ІзОД технічними каналами на ОІД і формування рішень з ТЗІ;
  - обґрунтування необхідності впровадження на ОІД заходів із захисту від витоку інформації технічними каналами, розроблення проектнокошторисної та конструкторської документації;
  - підготовку пропозицій щодо необхідності залучення співвиконавців для створення комплексу ТЗІ;

Роль виконавця робіт ТЗІ$_2$

- Виконавець робіт з ТЗІ та виконавець випробувань забезпечують:
  - розроблення проектів програм і методик випробувань;
  - придбання (закупівлю) технічних засобів забезпечення ТЗІ та іншого обладнання;
  - впровадження на ОІД заходів з ТЗІ;
  - проведення відповідних випробувань згідно із затвердженими програмами і методиками;
  - здійснення (у разі необхідності) будівельних, монтажноналагоджувальних робіт та післяопераційного технічного контролю щодо повноти їх виконання;
  - розроблення проектів паспортів на комплекс ТЗІ (у т.ч. паспортів на приміщення, де ІзОД озвучується та/або обробляється технічними засобами тощо);
  - здійснення (на договірних засадах) гарантійного та післягарантійного обслуговування комплексу ТЗІ;
  - проведення інструктажів щодо особливостей функціонування та експлуатації комплексу ТЗІ.

Дозволи

- Дозвіл на здійснення озвучення та/або оброблення технічними засобами ІзОД (окрім оброблення ІзОД в ІТС) надається керівником установи-замовника на підставі наявності Акта атестації та паспорта на комплекс ТЗІ.
- Дозвіл на експлуатацію ІТС, технічні засоби яких розміщуються на ОІД, надається керівником установи-замовника на підставі наявності Атестата відповідності на комплексну систему захисту інформації в ІТС, який оформляється за результатами проведення державної експертизи у сфері ТЗІ.

Етапи створення КТЗІ

- Створення комплексу ТЗІ на ОІД передбачає такі основні етапи:
  - виконання передпроектних робіт (1 етап);
  - розроблення та впровадження заходів із захисту інформації (2 етап);
  - випробування та атестація комплексу ТЗІ (3 етап).

НД ТЗІ щодо порядку виконання робіт на етапах створення КТЗІ

- Порядок виконання робіт на етапах створення комплексу ТЗІ на ОІД визначено НД ТЗІ 3.1-001-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07.
- Державні стандарти України ДСТУ 3396.0, ДСТУ 3396.1 при виконанні робіт з ТЗІ використовуються в частині, що не суперечать вимогам зазначених НД ТЗІ.
- Норми ефективності захисту від витоку ІзОД технічними каналами, методики контролю їх виконання (випробувань), вимоги із забезпечення ТЗІ, порядок створення моделі загроз для інформації, порядок проведення категорування об'єктів тощо викладено у відповідних НД з питань ТЗІ.

Донецький національний технічний університет



Тема 2. Побудова комплексу технічного захисту інформації. Лекція 4. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Визначення та загальні положення
- Порядок розроблення та оформлення паспорта на комплекс ТЗІ
- Додатки паспорту

Визначення та загальні положення

НПА в НД ТЗІ 3.3-001-07

- 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.
- ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.
- НД ТЗІ 3.3-001-07 Створення комплексу технічного захисту інформації. порядок розроблення та впровадження заходів із захисту інформації
- ДБН А.2.2-3-2004 Проектування. Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
- НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні 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 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

Загальні положення$_1$

- На другому етапі виконавець робіт з ТЗІ відповідно до вимог затвердженого технічного завдання на створення комплексу ТЗІ організовує розроблення пояснювальної записки з ТЗІ, де зазначає перелік, зміст, терміни виконання робіт щодо цього створення, склад документів, що розробляються під час його створення тощо.
- ТАКОЖ МОЖУТЬ БУТИ ЗАЗНАЧЕНІ:
  - результати розгляду варіантів заходів із захисту від витоку інформації технічними каналами та орієнтовні техніко-економічні показники щодо цього захисту;
  - схеми комплексу ТЗІ;
  - пропозиції щодо визначення співвиконавців робіт з ТЗІ на ОІД;
  - обґрунтування необхідності організації розроблення проектно-кошторисної документації щодо створення комплексу ТЗІ на ОІД;
  - висновки та пропозиції.

Загальні положення$_2$

- ПРИ ЦЬОМУ МАЮТЬ БУТИ ВРАХОВАНІ:
  - пропозиції від підрозділу-заявника на створення комплексу ТЗІ щодо організації проведення робіт з ТЗІ;
  - відомості про ОІД;
  - результати проведення категорування об'єктів;
  - відомості про вже створені (діючі) комплекси ТЗІ;
  - перспективи подальших робіт з ТЗІ;
  - технічні і економічні можливості установи із впровадження організаційних, інженерних і технічних заходів з ТЗІ на ОІД.

Загальні положення$_3$

- ВИКОНАВЕЦЬ РОБІТ З ТЗІ ТАКОЖ ОРГАНІЗОВУЄ:
  - розроблення (у разі необхідності) згідно з вимогами ДБН(державні будівельні норми) А.2.2-2 і ДБН А.2.2-3 проектно-кошторисної документації;

    ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.

    ДБН А.2.2-3-04 Проектування. Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
  - здійснення (у разі необхідності) відповідних будівельних, монтажно-налагоджувальних робіт та післяопераційного технічного контролю щодо повноти їх виконання;
  - придбання (закупівлю) технічних засобів забезпечення ТЗІ та іншого обладнання;
  - впровадження на ОІД заходів з ТЗІ;
  - розроблення проектів паспортів на комплекс ТЗІ.

Загальні положення$_4$

- У проектно-кошторисній документації щодо будівництва ОІД заходи з ТЗІ відображаються за відповідними напрямами: в будівельних кресленнях, планах території, споруд, приміщень, схемах електроживлення, зв’язку, вентиляції тощо.
- Розроблену проектно-кошторисну документацію в частині ТЗІ затверджує замовник встановленим порядком (згідно з ДБН А 2.2-3).
- Відповідно до пояснювальної записки з ТЗІ або проектної документації виконавець організовує впровадження заходів з ТЗІ.
- За результатами впровадження заходів з ТЗІ і проведення випробувань здійснюють (за необхідності) відповідне коригування проектно-кошторисної, конструкторської, експлуатаційної та іншої технічної документації.

Загальні положення$_5$

- ОРГАНІЗАЦІЙНІ, ІНЖЕНЕРНІ І ТЕХНІЧНІ ЗАХОДИ ЩОДО СТВОРЕННЯ КОМПЛЕКСУ ТЗІ НА ОІД ПОВИННІ ВІДПОВІДАТИ ВИМОГАМ НД З ПИТАНЬ ТЗІ ТА МОЖУТЬ МІСТИТИ:
  - архітектурно-будівельні заходи;
  - заходи з пасивного захисту ІзОД (оптичне, акустичне, електромагнітне екранування, засоби захисту інформації в телефонних, інших проводових лініях, засоби у захищеному виконанні тощо);
  - заходи з активного захисту ІзОД (генератори віброакустичного, просторового, акустичного та електромагнітного зашумлення, лінійного електромагнітного зашумлення тощо).
- Під час створення комплексу ТЗІ перевага має надаватися архітектурно-будівельним заходам та заходам пасивного захисту ІзОД.

Порядок розроблення та оформлення паспорта на комплекс ТЗІ

Паспорт на комплекс ТЗІ

- Основним експлуатаційним документом на комплекс ТЗІ є паспорт і його складові – паспорти на приміщення, де ІзОД озвучується та/або обробляється технічними засобами (далі – паспорти).
- ПАСПОРТИ ПРИЗНАЧЕНО ДЛЯ:
  - ознайомлення з відомостями про інформацію, що підлягає захисту від витоку технічними каналами;
  - ознайомлення з проектними і технічними рішеннями, що реалізовані у комплексі ТЗІ;
  - встановлення правил експлуатації (використання за призначенням, технічне обслуговування, перевірки основних характеристик, ремонт, перевірки за умови виявлення порушень правил експлуатації приміщення та технічних засобів, а також у разі порушення пломб на технічних засобах та засобах захисту тощо);
  - відображення відомостей про технічне обслуговування комплексу, його основні характеристики (визначені під час приймання комплексу), планові перевірки, атестації, а також про ремонт та утилізацію.
- Паспорти затверджує керівник установи-замовника. Кожен паспорт повинен мати окремий обліковий (інвентарний, архівний) номер.

Структура паспорта на КТЗІ

- ПАСПОРТ НА КОМПЛЕКС ТЗІ МАЄ ТИТУЛЬНИЙ АРКУШ (ДОДАТОК А) І МІСТИТЬ ТАКІ РОЗДІЛИ:
  1) Загальні вказівки.
  2) Загальні відомості.
  3) Технічні характеристики комплексу ТЗІ.
  4) Гарантії.
  5) Відомості про випробування і атестацію комплексу ТЗІ.
  6) Облік технічного обслуговування.
  7) Відомості про проведені роботи під час експлуатації комплексу ТЗІ.
  8) Особливі відмітки.
  9) Додатки.

Титульний аркуш паспорта на КТЗІ

Додаток А
(довідковий)

Форма титульного аркуша паспорта на комплекс технічного захисту інформації

Ступінь обмеження доступу
Прим. №

ЗАТВЕРДЖЕНО
Керівник установи-замовника

_____

—

____. ____. 20____

Паспорт
на комплекс технічного захисту інформації

(назва, належність об'єкта інформаційної діяльності, на якому розташований комплекс ТЗІ)

_____

(назва підрозділів установи, що заявляли створення комплексу ТЗІ)

Документ підписують:
– керівник підрозділу установи, що заявляв створення комплексу ТЗІ;
– посадова особа, призначена для організації експлуатації комплексу ТЗІ;
– представник від підрозділу, якому доручено організацію і супроводження робіт з ТЗІ в установі;
– інші особи ознайомлені з паспортом, у частині, що їх стосується.

Розділ паспорта «Загальні вказівки»

- Під час оформлення паспорта на комплекс ТЗІ перелік та зміст його розділів допускається уточнювати залежно від складу ОІД, кількості приміщень, де циркулюватиме ІзОД, призначення приміщень, місць розміщення на ОІД засобів ТЗІ та технічних характеристик комплексу ТЗІ.
- Розділ “Загальні вказівки” містить вказівки щодо експлуатації комплексу ТЗІ на ОІД та заповнення і ведення паспорта.
- ЗОКРЕМА У ЦЬОМУ РОЗДІЛІ МАЄ БУТИ ЗАЗНАЧЕНО:
  - фаховий рівень посадової особи, яка організовує експлуатацію комплексу ТЗІ на ОІД;
  - порядок заміни обладнання, проведення ремонтних робіт на ОІД, внесення змін до паспорта на комплекс ТЗІ;
  - порядок використання радіотелефонів, кінцевих пристроїв рухомого (мобільного, сотового, пейджингового, транкінгового тощо) зв'язку.
- Затверджений паспорт на комплекс ТЗІ допускається коригувати, вносити до нього зміни, при цьому у записах не допускається проводити підчищення, попередній запис має бути закреслений і поруч зроблено новий, що завіряється встановленим порядком.

Розділ паспорта «Загальні відомості»$_1$

- У РОЗДІЛІ “ЗАГАЛЬНІ ВІДОМОСТІ” НАВОДЯТЬ:
  - назву та дислокацію підрозділу, що замовляв створення комплексу ТЗІ;
  - відомості про інформацію з обмеженим доступом (табл.1);

Таблиця 1

Характеристика ІзОД (умови озвучення, засоби оброблення тощо)	Найменування приміщень, де ІзОД озвучується та/або обробляється технічними засобами тощо	Ступінь обмеження доступу до інформації
1	2	3

  - витяг із затвердженого керівником установи рішення (наказу, розпорядження) щодо створення комплексу ТЗІ на ОІД, у т.ч. інформацію про посаду та прізвище відповідальної особи, що призначена керівником установи для організації, супроводження та координації робіт на всіх етапах створення комплексу ТЗІ;
  - дані про акт обстеження на ОІД, модель загроз для ІзОД, приписи на експлуатацію засобів оброблення інформації, технічні вимоги, завдання щодо створення комплексу ТЗІ, розроблену проектно-кошторисну документацію тощо, дані про їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги (у разі необхідності) з них;

Розділ паспорта «Загальні відомості»$_2$

- У РОЗДІЛІ “ЗАГАЛЬНІ ВІДОМОСТІ” НАВОДЯТЬ:
  - опис конструкцій ОІД, де створено комплекс ТЗІ, а саме: будинків, споруд, салонів транспортних засобів тощо (конструкція та матеріали стін, перекриттів, вікон, дверей, інженерних комунікацій тощо), їх особливості;
  - перелік технічних засобів, що обробляють ІзОД, а також засобів забезпечення ТЗІ (вказують інвентарні номери і дані про наявність сертифікатів або експертних висновків з ТЗІ);
  - відомості про виконані випробування (у т.ч. спеціальні дослідження технічних засобів, які обробляють ІзОД).
  - назви документів, їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги з них;
  - місця виходу за межі контрольованої зони елементів технологічного обладнання, систем зв’язку, радіофікації, телебачення, сигналізації, автоматизації, керування, заземлення, електро-, газо-, водопостачання, опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, огороджувальних будівельних конструкцій тощо.

Розділ паспорту «Технічні характеристики КТЗІ»

- У розділі “Технічні характеристики комплексу ТЗІ” наводять перелік технічних засобів як складових комплексу ТЗІ, що можуть впливати на ефективність захищеності інформації і бути середовищем поширення носіїв інформації, та їх технічні характеристики (табл. 2).

Таблиця 2

Технічна характеристика (параметр)	Номінальне значення параметра відповідно до норм, вимог	Значення параметра під час випробування комплексу	Значення параметра під час експлуатації комплексу ТЗІ			
			За результатами контролю	Вид контролю	Дата	Посада, прізвище, підпис, висновки
1	2	3	4	5	6	7

Розділ паспорту «Гарантії»

- Розділ “Гарантії” складають у разі наявності відповідних зобов’язань розробника технічних засобів або виконавця впровадження заходів із захисту інформації щодо гарантійних термінів.
- Наводять пропозиції щодо терміну проведення чергової атестації.

Розділ паспорту «Відомості про випробування і атестацію комплексу ТЗІ»

- У РОЗДІЛІ “ВІДОМОСТІ ПРО ВИПРОБУВАННЯ І АТЕСТАЦІЮ КОМПЛЕКСУ ТЗІ” НАВОДЯТЬ:
  - види інформації, стосовно яких проводили випробування і атестацію комплексу ТЗІ;
  - терміни проведення випробування та атестації комплексу ТЗІ, їх виконавців;
  - дані про протоколи випробування та акти атестації комплексу ТЗІ (назви документів, їх склад, реквізити, реєстраційні номери, місце зберігання, короткі витяги з них);
  - терміни проведення чергової атестації і відповідних випробувань.
  - Висновки про результати випробувань наводять у вигляді таблиці 3.

Таблиця 3

Перелік висновків про результати випробувань	Дата	Виконавець проведення випробувань	Примітка
1	2	3	4

Розділ паспорту «Облік технічного обслуговування»

- Розділ “Облік технічного обслуговування” складають у разі, якщо такі види робіт передбачені.
- У РОЗДІЛІ НАВОДЯТЬ:
  - відомості про технічне обслуговування комплексу ТЗІ, його види;
  - дату проведення технічного обслуговування;
  - відомості про виконавців технічного обслуговування.
  - Зазначені відомості наводять у вигляді таблиці 4.

Таблиця 4

Дата	Вид технічного обслуговування	Напрацювання		Підстава (найменування, номер і дата докумен-та)	Установа, посада, прізвище і підпис		Примітка
		з початку експлуатації	після останнього ремонту		хто виконав роботу	хто перевірив виконання роботи	
1	2	3	4	5	6	7	8

Розділ паспорту «Відомості про проведені роботи під час експлуатації комплексу ТЗІ»$_1$

- У РОЗДІЛІ “ВІДОМОСТІ ПРО ПРОВЕДЕНІ РОБОТИ ПІД ЧАС ЕКСПЛУАТАЦІЇ КОМПЛЕКСУ ТЗІ” НАВОДЯТЬ:
  - облік робіт, що виконано під час експлуатації комплексу ТЗІ на ОІД (містить записи про незаплановані роботи з усунення відмов під час експлуатації, перевірку відсутності закладних пристроїв тощо).
  - Записи про ці роботи наводять у вигляді таблиць 5, 6;

Таблиця 5

Дата	Найменування роботи і причина її виконання	Посада, прізвище і підпис		Примітка
		роботу виконав	перевірив виконання роботи	
1	2	3	4	5

Таблиця 6

Періодичний контроль відсутності закладних пристроїв, підстава для контролю	Дата	Посада, прізвище, підпис виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

Розділ паспорту «Відомості про проведені роботи під час експлуатації комплексу ТЗІ»$_2$

- періодичні та інші перевірки стану комплексу ТЗІ та правильності ведення паспорта (реєструються за формою таблиць 7, 8);

Таблиця 7

Дата, тема періодичного контролю стану технічних характеристик, підстави для контролю (посилання на пункти табл. 2)	Резуль-тати контролю	Посади, прізвища, підписи виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

Таблиця 8

Дата	Вид перевірки	Результати перевірки	Прізвища і підписи осіб, що перевіряють	Відмітка про усунення недоліків
1	2	3	4	5

Розділ паспорту «Відомості про проведені роботи під час експлуатації комплексу ТЗІ»$_3$

- дані щодо повірки засобів вимірювань (містить перелік засобів вимірювань, які підлягають періодичній повірці, із зазначенням їх заводських номерів, періодичності повірки та дати проведення повірок).
- Підрозділ вводиться у разі наявності засобів вимірювань у складі комплексу ТЗІ.
- Відомості щодо повірки засобів вимірювань наводять у вигляді таблиці 9;

Таблиця 9

Найменування та позначення засобів вимірювання	Заводський номер	Дата виготов-лення	Періо-дичність повірки	Дата повірки (термін чергової повірки)	Примітка
1	2	3	4	5	6

- дані про інспекційні перевірки.

Розділ паспорту «Особливі відмітки»

- Розділ “Особливі відмітки” містить декілька чистих аркушів для записів, що можуть бути здійснені під час експлуатації комплексу ТЗІ.

Додатки паспорту

Додатки паспорту

- До додатків (за необхідності) додають паспорти на кожне приміщення, де циркулює інформація з обмеженим доступом.

Паспорт на приміщення

- Паспорт на приміщення, де інформація з обмеженим доступом озвучується та/або обробляється технічними засобами (як складова частина технічного паспорта на комплекс тзі), має титульний аркуш (додаток б) і містить такі розділи:
  1) Загальні вказівки.
  2) Технічні характеристики приміщення.
  3) Відомості про проведені роботи з ТЗІ під час експлуатації приміщення.

Титульний аркуш паспорта на приміщення

(довідковий)

Форма титульного аркуша паспорта на приміщення, де інформація з обмеженим доступом озвучується та/або обробляється технічними засобами

Ступінь обмеження доступу
Прим. №

ЗАТВЕРДЖЕНО
Керівник установи-замовника

_____

____. ____. 20____

Паспорт
на приміщення, де інформація з обмеженим доступом озвучується та/або обробляється технічними засобами
(складова частина паспорта на комплекс ТЗІ)

(назва, призначення приміщення)

(назва підрозділу установи, що заявляв створення комплексу ТЗІ)

Документ підписують:
– керівник підрозділу установи, що заявляв створення комплексу ТЗІ;
– посадова особа, призначена для організації експлуатації комплексу ТЗІ.

Розділ паспорту на приміщення «Загальні вказівки»

- Перелік та зміст розділів паспорта на приміщення також допускається уточнювати залежно від того, які дані будуть наведені в технічному паспорті на комплекс ТЗІ.
- Розділ “Загальні вказівки” містить вказівки щодо експлуатації комплексу ТЗІ в конкретному приміщенні, заповнення і ведення паспорта.

Розділ паспорту на приміщення «Технічні характеристики приміщення»$_1$

- У РОЗДІЛІ “ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ПРИМІЩЕННЯ” НАВОДЯТЬ:
  - назву приміщення і структурного підрозділу в установі, до якого воно відноситься, відомості про його дислокацію;
  - план приміщення, план розміщення пристроїв зв’язку, кабельних і телекомунікаційних мереж, інженерних комунікацій та координати точок із властивостями нелінійності, план-схеми або опис затвердженої контрольованої зони, зон безпеки інформації стосовно кожного технічного каналу її витоку;
  - загальний опис приміщення, інженерних комунікацій та інші відомості; характеристику приміщення: його розташування в будинку, споруді (поверх, архітектурні осі, ряди); інформацію про суміжні приміщення (у т.ч. поверхом вище і нижче); особливості розташування вікон, дверей, інших будівельних отворів;

Розділ паспорту на приміщення «Технічні характеристики приміщення»$_2$

- витяг із затвердженої моделі загроз для ІзОД (або посилання на модель загроз), у т.ч. щодо даних про можливі місця розміщення засобів технічної розвідки (стаціонарних або автономних автоматичних), що можуть використовуватися для тривалого перехоплення оброблюваної ІзОД, а також найменших відстаней від технічних засобів, що оброблятимуть інформацію, до межі контрольованої зони тощо;
- дані про технічні характеристики складових комплексу ТЗІ (у разі необхідності розгортання, доповнення або окремого наведення, ці дані оформляють у вигляді таблиці 2).

Таблиця 2

Технічна характеристика (параметр)	Номінальне значення параметра відповідно до норм, вимог	Значення параметра під час випробування комплексу	Значення параметра під час експлуатації комплексу ТЗІ			
			За результатами контролю	Вид контролю	Дата	Посада, прізвище, підпис, висновки
1	2	3	4	5	6	7

Розділ паспорту на приміщення «Відомості про проведені роботи з ТЗІ під час експлуатації приміщення»$_1$

- У РОЗДІЛІ “ВІДОМОСТІ ПРО ПРОВЕДЕНІ РОБОТИ З ТЗІ ПІД ЧАС ЕКСПЛУАТАЦІЇ ПРИМІЩЕННЯ” НАВОДЯТЬ:
  - облік робіт, що виконано під час експлуатації комплексу ТЗІ у приміщенні. Записи про зазначені роботи наводять у вигляді таблиць 5,6;

Таблиця 5

Дата	Найменування роботи і причина її виконання	Посада, прізвище і підпис		Примітка
		роботу виконав	перевірив виконання роботи	
1	2	3	4	5

Таблиця 6

Періодичний контроль відсутності закладних пристроїв, підстава для контролю	Дата	Посада, прізвище, підпис виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

Розділ паспорту на приміщення «Відомості про проведені роботи з ТЗІ під час експлуатації приміщення»$_2$

- періодичні, інші перевірки стану комплексу ТЗІ та правильності ведення паспорта реєструються за формою таблиць 7, 8;

Таблиця 7

Дата, тема періодичного контролю стану технічних характеристик, підстави для контролю (посилання на пункти табл. 2)	Резуль-тати контролю	Посади, прізвища, підписи виконавців контролю	Відмітка про усунення недоліків
1	2	3	4

Таблиця 8

Дата	Вид перевірки	Результати перевірки	Прізвища і підписи осіб, що перевіряють	Відмітка про усунення недоліків
1	2	3	4	5

Розділ паспорту на приміщення «Відомості про проведені роботи з ТЗІ під час експлуатації приміщення»$_3$

- проведену повірку засобів вимірювальної техніки (реєструється за формою таблиці 9).

Таблиця 9

Найменування та позначення засобів вимірювання	Заводський номер	Дата виготов-лення	Періо-дичність повірки	Дата повірки (термін чергової повірки)	Примітка
1	2	3	4	5	6

Донецький національний технічний університет



Тема 2. Побудова комплексу технічного захисту інформації. Лекція 5. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- НД ТЗІ 2.1-001-2001. Загальні положення
- Порядок організації та проведення атестації
- НД ТЗІ 2.1-002-07. Загальні положення
- Порядок розроблення та оформлення програм і методик випробувань
- Атестація КТЗІ

НД ТЗІ 2.1-001-2001. Загальні положення

Визначення

- **Об’єкт інформаційної діяльності** - інженерно-технічна споруда, приміщення, де здійснюється адміністративна, виробнича та інша діяльність, пов□язана з інформацією, що підлягає захисту від витоку технічними каналами.
- **Комплекс ТЗІ** - сукупність заходів та засобів, призначених для реалізації ТЗІ на ОІД.
- **Атестація комплексу ТЗІ** - оцінювання ефективності комплексу технічного захисту інформації, що циркулюватиме на ОІД, на відповідність вимогам нормативних документів з ТЗІ.
- **Особливо важливий ОІД** - ОІД, на якому циркулює інформація, захист якої забезпечується згідно з вимогами 1 категорії.

Атестація КТЗІ

- Атестація комплексу ТЗІ (атестація) здійснюється за відповідними програмою і методиками випробувань.
- На підставі результатів випробувань складається висновок щодо відповідності стану ТЗІ, який забезпечується комплексом, вимогам нормативних документів з ТЗІ.
- Атестація може бути **первинною, черговою та позачерговою**.
  - **Первинна атестація** здійснюється після (або під час) приймання робіт із створення комплексу ТЗІ.
  - Термін проведення **чергової атестації** визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації.
  - **Позачергову атестацію** проводять у разі змін умов функціонування ОІД, що приводять до змін загроз для інформації, та за висновками органів, які контролюють стан ТЗІ.

Етапи атестації

ЕТАПИ АТЕСТАЦІЇ:

- визначення організації-виконавця атестації та оформлення відповідних організаційних документів;
- аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ та розроблення і оформлення Програми і методик атестації (ПМА);
- проведення випробувань відповідно до ПМА та оформлення протоколів випробувань і підсумкового документа – **акта атестації**.

Суб’єкти атестації

❑СУБ'ЄКТИ АТЕСТАЦІЇ:

- Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України (далі - Департамент);
- організації-замовники атестації;
- організації-виконавці атестації.

❑ДЕПАРТАМЕНТ:

- організує розроблення та удосконалення нормативних документів з атестації;
- контролює виконання вимог щодо атестації та розглядає апеляції;
- узгоджує вибір організації-виконавця атестації, програми і методики атестації (ПМА) та результати атестації на особливо важливих ОІД, витрати на проведення атестації включаються до кошторису на проектування, будівництво та експлуатацію (утримання) ОІД.

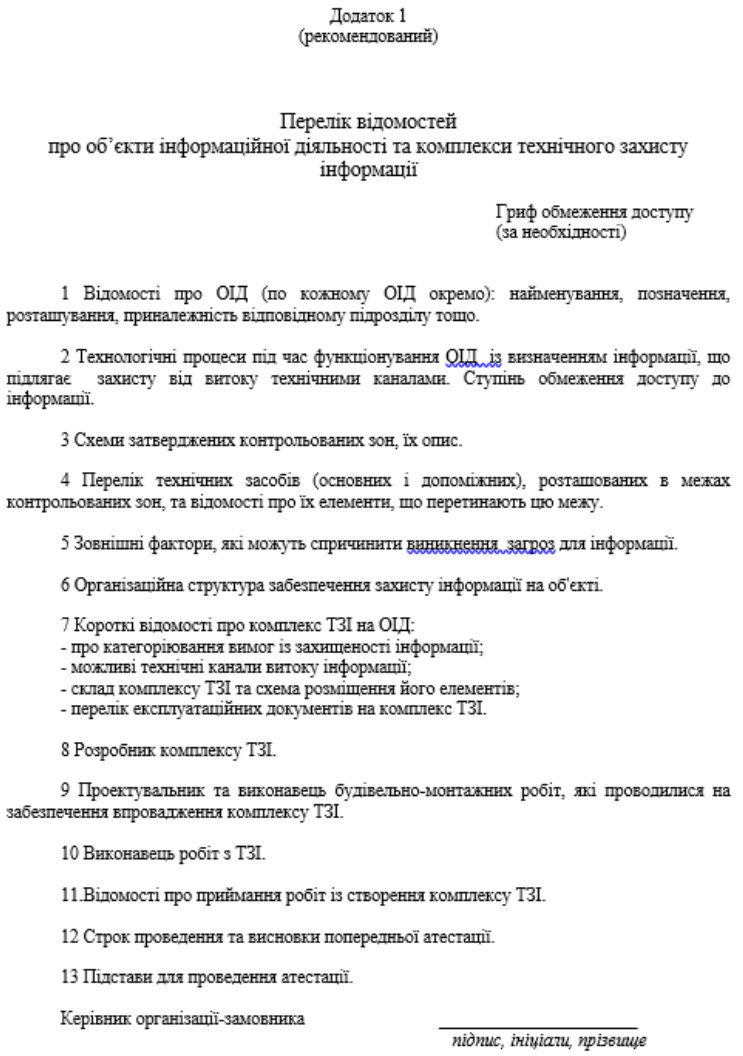
Порядок організації та проведення атестації

Організація-замовник

- Організація-замовник на засадах, передбачених законодавством щодо закупівель послуг за рахунок державних коштів, визначає організацію-виконавця атестації.
- Організацією-виконавцем атестації може бути підприємство, установа чи організація, які мають відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.
- Відносини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентуються укладеним між ними договором.
- У разі проведення атестації на особливо важливих ОІД визначення організації-виконавця атестації узгоджується з Департаментом.

Організація-виконавець

- Організація-виконавець за результатами аналізу відомостей (додаток 1), наданих організацією-замовником, та, за необхідності, за результатами аналізу умов функціонування ОІД і загроз для інформації безпосередньо на ОІД, розробляє проект програм і методик атестації (ПМА) та подає його на узгодження організації-замовнику.
- Узгоджений організацією-замовником проект ПМА затверджує організація-виконавець.
- У разі атестації комплексу ТЗІ на особливо важливих ОІД проект ПМА узгоджується також з Департаментом.



Додаток 1
(рекомендований)

Перелік відомостей
про об'єкти інформаційної діяльності та комплекси технічного захисту інформації

Гриф обмеження доступу
(за необхідності)

1 Відомості про ОІД (по кожному ОІД окремо): найменування, позначення, розташування, приналежність відповідному підрозділу тощо.

2 Технологічні процеси під час функціонування ОІД із визначенням інформації, що підлягає захисту від витоку технічними каналами. Ступінь обмеження доступу до інформації.

3 Схеми затверджених контрольованих зон, їх опис.

4 Перелік технічних засобів (основних і допоміжних), розташованих в межах контрольованих зон, та відомості про їх елементи, що перетинають цю межу.

5 Зовнішні фактори, які можуть спричинити виникнення загроз для інформації.

6 Організаційна структура забезпечення захисту інформації на об'єкті.

7 Короткі відомості про комплекс ТЗІ на ОІД:
- про категоріювання вимог із захищеності інформації;
- можливі технічні канали витоку інформації;
- склад комплексу ТЗІ та схема розміщення його елементів;
- перелік експлуатаційних документів на комплекс ТЗІ.

8 Розробник комплексу ТЗІ.

9 Проектувальник та виконавець будівельно-монтажних робіт, які проводилися на забезпечення впровадження комплексу ТЗІ.

10 Виконавець робіт з ТЗІ.

11.Відомості про приймання робіт із створення комплексу ТЗІ.

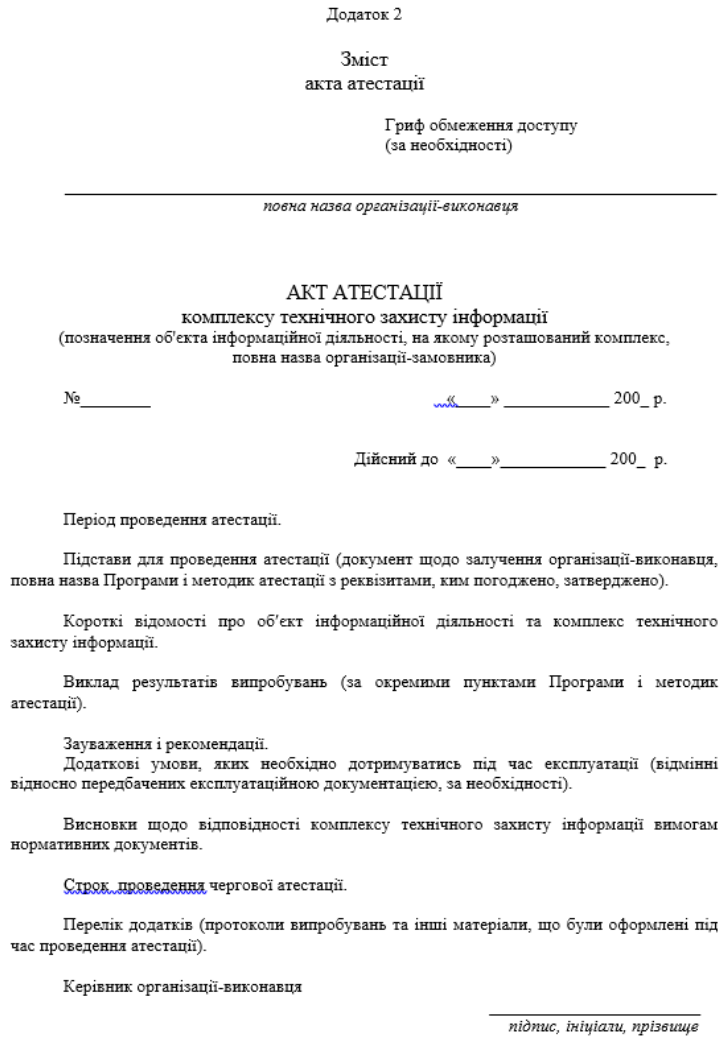
12 Строк проведення та висновки попередньої атестації.

13 Підстави для проведення атестації.

Керівник організації-замовника _____
підпис, ініціали, прізвище

Порядок атестації

- **Організація-замовник створює умови** проведення атестації, передбачені договором та ПМА.
- **Організація-виконавець проводить випробування** відповідно до ПМА та оформляє акт атестації за формою додатку 2 у 2-х примірниках (1-й надається організації-замовнику, 2-й – зберігається у організації-виконавця).
  - До акту атестації додаються протоколи випробувань, передбачених ПМА.
  - За результатами атестації заповнюється технічний паспорт на комплекс ТЗІ.



Додаток 2

Зміст
акта атестації

Гриф обмеження доступу
(за необхідності)

_____
повна назва організації-виконавця

АКТ АТЕСТАЦІЇ
комплексу технічного захисту інформації
(позначення об'єкта інформаційної діяльності, на якому розташований комплекс,
повна назва організації-замовника)

№_____ «____» _____ 200_ р.

Дійсний до «____»_____ 200_ р.

Період проведення атестації.

Підстави для проведення атестації (документ щодо залучення організації-виконавця, повна назва Програми і методик атестації з реквізитами, ким погоджено, затверджено).

Короткі відомості про об'єкт інформаційної діяльності та комплекс технічного захисту інформації.

Виклад результатів випробувань (за окремими пунктами Програми і методик атестації).

Зауваження і рекомендації.
Додаткові умови, яких необхідно дотримуватись під час експлуатації (відмінні відносно передбачених експлуатаційною документацією, за необхідності).

Висновки щодо відповідності комплексу технічного захисту інформації вимогам нормативних документів.

Строк проведення чергової атестації.

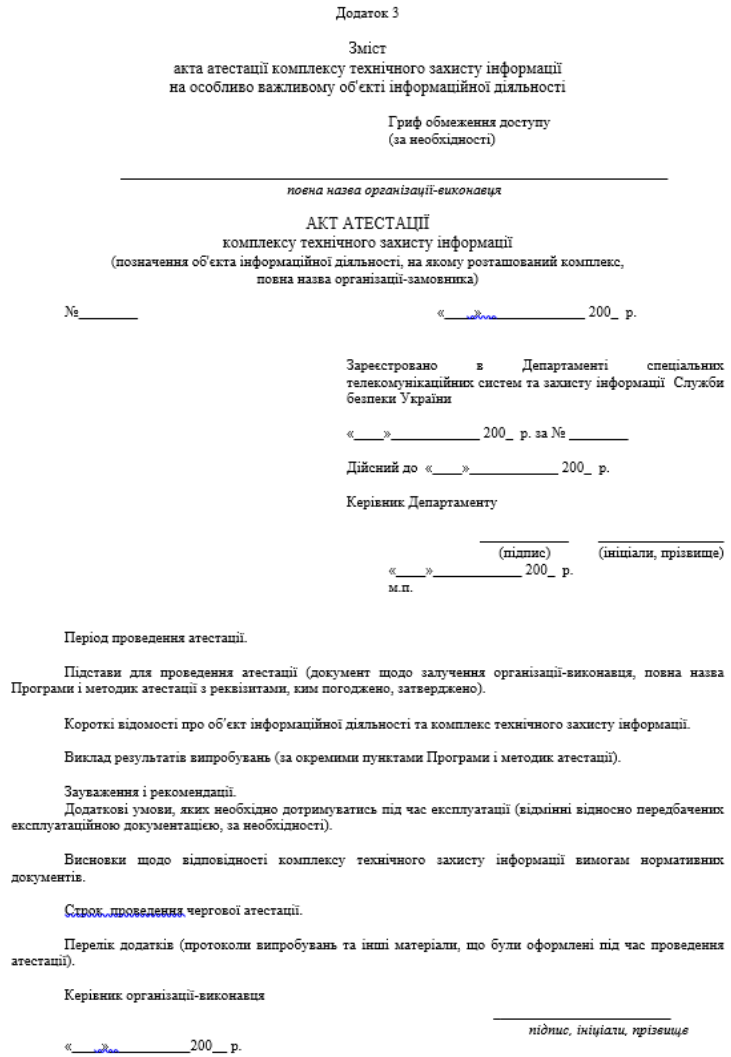
Перелік додатків (протоколи випробувань та інші матеріали, що були оформлені під час проведення атестації).

Керівник організації-виконавця

_____
підпис, ініціали, прізвище

Повторна атестація

- У разі проведення атестації на особливо важливих ОІД матеріали з атестації **у 5-денний термін** організація-виконавець надає Департаменту.
- **Департамент у 2-тижневий термін** розглядає результати атестації, приймає рішення щодо можливості їх узгодження, реєструє акт атестації (додаток 3) та надсилає його організації-замовнику, одночасно інформуючи про це організацію-виконавця.
- У разі незгоди з результатами атестації організація-замовник має право направити до Департаменту апеляцію.
- Департамент у **місячний термін** за апеляцією приймає відповідні рішення.
- **Повторна атестація проводиться за рахунок винного**.



Додаток 3

Зміст
акта атестації комплексу технічного захисту інформації
на особливо важливому об'єкті інформаційної діяльності

Гриф обмеження доступу
(за необхідності)

_____
повна назва організації-виконавця

АКТ АТЕСТАЦІЇ
комплексу технічного захисту інформації
(позначення об'єкта інформаційної діяльності, на якому розташований комплекс,
повна назва організації-замовника)

№_____ «___»_____ 200_ р.

Зареєстровано в Департаменті спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

«____»_____ 200_ р. за № _____

Дійсний до «____»_____ 200_ р.

Керівник Департаменту

_____ _____
(підпис) (ініціали, прізвище)
«____»_____ 200_ р.
м.п.

Період проведення атестації.

Підстави для проведення атестації (документ щодо залучення організації-виконавця, повна назва Програми і методик атестації з реквізитами, ким погоджено, затверджено).

Короткі відомості про об'єкт інформаційної діяльності та комплекс технічного захисту інформації.

Виклад результатів випробувань (за окремими пунктами Програми і методик атестації).

Зауваження і рекомендації.
Додаткові умови, яких необхідно дотримуватись під час експлуатації (відмінні відносно передбачених експлуатаційною документацією, за необхідності).

Висновки щодо відповідності комплексу технічного захисту інформації вимогам нормативних документів.

Строк проведення чергової атестації.

Перелік додатків (протоколи випробувань та інші матеріали, що були оформлені під час проведення атестації).

Керівник організації-виконавця

_____
підпис, ініціали, прізвище

«___»_____200__ р.

НД ТЗІ 2.1-002-07. Загальні положення

Етап «Випробування та атестація КТЗІ»

- **ЕТАП «ВИПРОБУВАННЯ ТА АТЕСТАЦІЯ КОМПЛЕКСУ ТЗІ» Є ТРЕТІМ ЕТАПОМ СТВОРЕННЯ КОМПЛЕКСУ, ЯКИЙ ПЕРЕДБАЧАЄ:**
  - затвердження програм і методик випробувань;
  - проведення випробувань відповідно до затверджених програм і методик, оформлення протоколів випробувань;
  - підготовка документа «Висновки за результатами випробувань комплексу ТЗІ»;
  - підготовка пропозицій і вимог до вибору (уточнення) рішень щодо впровадження необхідних заходів із захисту ІзОД на ОІД (за необхідності);
  - проведення атестації комплексу ТЗІ, оформлення протоколів (за необхідності), актів атестації;
  - заповнення паспорта на комплекс ТЗІ (в т.ч. паспортів на приміщення, де ІзОД озвучується та/або обробляється технічними засобами).

Висновки за результатами випробувань КТЗІ

- **У «ВИСНОВКАХ ЗА РЕЗУЛЬТАТАМИ ВИПРОБУВАНЬ КОМПЛЕКСУ ТЗІ» ВКАЗУЮТЬ:**
  - мету, призначення, вид, обсяг випробувань, місце і термін їх проведення;
  - дані про затверджені програми і методики випробувань;
  - склад технічних засобів, обладнання, необхідних для випробувань;
  - результати випробувань щодо їх відповідності вимогам НД з питань ТЗІ.
- Документ «Висновки за результатами випробувань комплексу ТЗІ» затверджує керівник установи, яка виконувала випробування, підписують їх виконавці.

Забезпечення проведення атестації

- При проведенні випробувань **необхідне матеріально-технічне і метрологічне забезпечення здійснюють їх виконавці**.
- Засоби вимірювальної техніки мають відповідати вимогам методик випробувань (не допускається застосовувати засоби, які не пройшли метрологічну атестацію або термін повірки прострочено).
- **Установа-замовник** створення комплексу ТЗІ **забезпечує умови** проведення його атестації.
- **Виконавець атестації** комплексу ТЗІ аналізує дані про його створення на ОІД, висновки за результатами випробувань, інші відомості.
- У процесі проведення випробувань і атестації комплексів ТЗІ їх виконавці заповнюють відповідні паспорти, порядок розроблення та оформлення яких наведено в **НД ТЗІ 3.3-001-07**.

Порядок розроблення та оформлення програм і методик випробувань

Види документів методик

- Залежно від особливостей створення комплексу ТЗІ на ОІД, обсягу робіт, умов проведення випробувань, програми і методики можуть бути оформлені у вигляді двох самостійних документів:
  - «Програми випробувань …»
  - «Методики випробувань …»
- Допускається об’єднувати або вилучати окремі розділи за умови викладення їх змісту в документах, а також вносити до них додаткові розділи (за необхідності).

Структура документів методик

- ПРОГРАМИ І МЕТОДИКИ ВИПРОБУВАНЬ МОЖУТЬ МІСТИТИ ТАКІ РОЗДІЛИ:

  Загальні положення.

  2) Обсяг робіт.

  3) Методики випробувань.

  4) Умови та порядок проведення випробувань.

  5) Матеріально-технічне і метрологічне забезпечення.

  6) Аналіз і оцінка результатів випробувань.

  7) Вимоги щодо забезпечення охорони державної таємниці та іншої інформації з обмеженим доступом.

- Нижче наведено зміст розділів програм і методик випробувань.

Розділ «Загальні положення»

- **У РОЗДІЛІ «ЗАГАЛЬНІ ПОЛОЖЕННЯ» НАВОДЯТЬ**:
  - повну назву установи, підрозділу, ОІД, де створюється комплекс ТЗІ;
  - підстави для проведення випробувань;
  - відомості про виконавців випробувань;
  - мету і основні завдання;
  - види інформації (ІзОД, що озвучується та/або обробляється технічними засобами тощо), для яких впроваджуються відповідні заходи із захисту від витоку інформації технічними каналами;
  - терміни проведення випробувань.

Розділ «Обсяг робіт»

- Під час проведення випробувань здійснюють перевірку повноти та достатності реалізованих заходів із захисту інформації на ОІД (перевірку виконання вимог щодо захисту від витоку ІзОД можливими технічними каналами).
- Обсяг випробувань та посилання на відповідні методики можуть бути викладені у вигляді таблиці 1.

Таблиця 1

№ з/п	Найменування робіт	Вимоги, норми (відповідний документ)	Методики за п. 6.3.3 цього НД	При-мітки
1	2	3	4	5

Розділ «Методики випробувань»

- У розділі «МЕТОДИКИ ВИПРОБУВАНЬ» наводять відомості про методи проведення випробувань.

- УМОВИ ТА ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ:
  - умови щодо початку і завершення робіт з випробувань;
  - послідовність проведення перевірок комплексу ТЗІ на відповідність вимогам НД з питань ТЗІ;
  - особливості функціонування складових частин комплексу ТЗІ, що підлягають випробуванню;
  - заходи, що забезпечують безпеку проведення випробувань.

Розділ «Матеріально-технічне і метрологічне забезпечення»

- У Розділі наводять:
  - перелік заходів з метрологічного забезпечення випробувань із розподілом завдань і відповідальності підрозділів, що беруть участь у випробуваннях;
  - склад засобів вимірювальної техніки із зазначенням ознак їх придатності до застосування, вимоги до них;
  - перелік необхідної конструкторської та іншої документації;
  - порядок підготовки і використання матеріально-технічних засобів у процесі випробувань.
- Дані про вимірювальне обладнання можуть бути викладені у вигляді таблиці 2.

Таблиця 2

№ з/п	Найменування вимірювального обладнання	Тип	Заводський номер	Виробник	Дані про повірку
1	2	3	4	5	6

Розділ «Аналіз і оцінка результатів випробувань»

- У Розділі наводять:
  - обсяг вихідних даних, які необхідні для оцінки результатів випробувань;
  - показники та критерії, за якими комплекс ТЗІ вважається таким, що пройшов випробування.
- За результатами випробувань складаються протоколи, де надаються висновки про відповідність вимогам НД з питань ТЗІ. Висновки повинні містити конкретні формулювання, що забезпечують їх однозначне трактування.

Розділ «Вимоги...»

- У РОЗДІЛІ «ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА ІНШОЇ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ» вказують організаційні заходи, які мають бути проведені при виконанні робіт з випробувань.

Атестація КТЗІ

Атестація

- Атестація комплексу ТЗІ проводиться з метою визначення відповідності вимогам НД з питань ТЗІ виконаних робіт зі створення комплексу ТЗІ на ОІД та повноти проведених випробувань.
- Атестація може проводитися окремо щодо кожного виду ІзОД, що підлягає технічному захисту (ІзОД, що озвучуватиметься та/або оброблятиметься технічними засобами тощо).
- Вимоги щодо проведення атестації мають бути передбачені у технічному завданні на створення комплексу ТЗІ.

Основні етапи атестації КТЗІ

- Основні етапи атестації КТЗІ:
  - визначення виконавця атестації;
  - аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ, результатів випробувань;
  - аналіз та оцінка відповідності проектної, конструкторської, експлуатаційної та іншої технічної документації на комплекс ТЗІ вимогам НД з питань ТЗІ;
  - перевірка відповідності вихідних даних щодо створення комплексу ТЗІ реальним умовам розміщення ОІД;
  - перевірка складу комплексу ТЗІ на відповідність даним, зазначеним у проектній, конструкторській, експлуатаційній та іншій технічній документації;
  - перевірка наявності сертифікатів або експертних висновків на засоби забезпечення ТЗІ загального призначення;
  - перевірка відповідності монтажу та умов експлуатації засобів забезпечення ТЗІ вимогам експлуатаційної документації;
  - перевірка оформлення проекту паспорта на комплекс ТЗІ і паспорта на кожне приміщення;
  - розгляд висновків за результати випробувань;
  - оформлення підсумкового документа – акта атестації комплексу ТЗІ;
  - оформлення актів пломбування.

Зміст акту атестації

- АКТ АТЕСТАЦІЇ КОМПЛЕКСУ ТЗІ МАЄ МІСТИТИ:
  - підстави для проведення атестації;
  - дані про виконавця атестації;
  - дату проведення атестації;
  - результати атестації;
  - зауваження і рекомендації (додаткові умови, яких потрібно дотримуватися під час експлуатації ОІД);
  - висновки щодо відповідності комплексу ТЗІ вимогам технічних завдань і НД з питань ТЗІ;
  - термін проведення чергової атестації (строк дії акта атестації);
  - перелік додатків.
- Виконавець атестації оформляє акт атестації комплексу ТЗІ, який затверджує керівник установи-виконавця атестації.

Виконавець атестації

- Виконавцем атестації комплексу ТЗІ може бути установа, яка має відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.

- Відносини між замовником створення та виконавцем атестації комплексу ТЗІ регламентуються укладеним між ними договором.

Донецький національний технічний університет



Тема 3. Технічні засоби захисту інформації.
Лекція 6. Методи та засоби технічного захисту інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Класифікація технічних засобів захисту
- Технічні засоби захисту території і об'єктів
- Акустичні засоби захисту інформації
- Захист від радіозакладок
- Пристрої пошуку технічних засобів розвідки
- Пристрої постановки перешкод
- Захист від лазерних систем акустичної розвідки

Класифікація технічних засобів захисту

Переваги та недоліки ТЗ ЗІ

- **Технічними** називаються такі засоби захисту, у яких основна захисна функція реалізується технічним пристроєм (комплексом чи системою).
- Переваги технічних засобів (ТЗ) захисту інформації (ЗІ):
  - досить висока надійність;
  - достатньо широке коло задач;
  - можливість створення комплексних систем ЗІ (КСЗІ);
  - гнучке реагування на спроби несанкціонованої дії;
  - традиційність використаних методів здійснення захисних функцій.
- Недоліки ТЗ ЗІ:
  - висока вартість багатьох засобів;
  - необхідність регулярного проведення регламентних робіт та контролю;
  - можливість видачі хибних тривог.

Класифікація ТЗ $ЗІ_1$

- Класифікація ТЗ ЗІ за:
  - функціями захисту;
  - ступеню складності пристроїв;
  - сполученістю із засобами вимірювальної техніки.
- Функція захисту:
  - **Зовнішній захист** — захист від впливу факторів, що дестабілізують, що виявляються за межами зони ресурсів.
  - **Впізнання** — специфічна група засобів, призначених для розпізнавання людей за різними індивідуальними характеристиками.
  - **Внутрішній захист** — захист від впливу факторів, що дестабілізують, що виявляються безпосередньо в засобах обробки інформації.

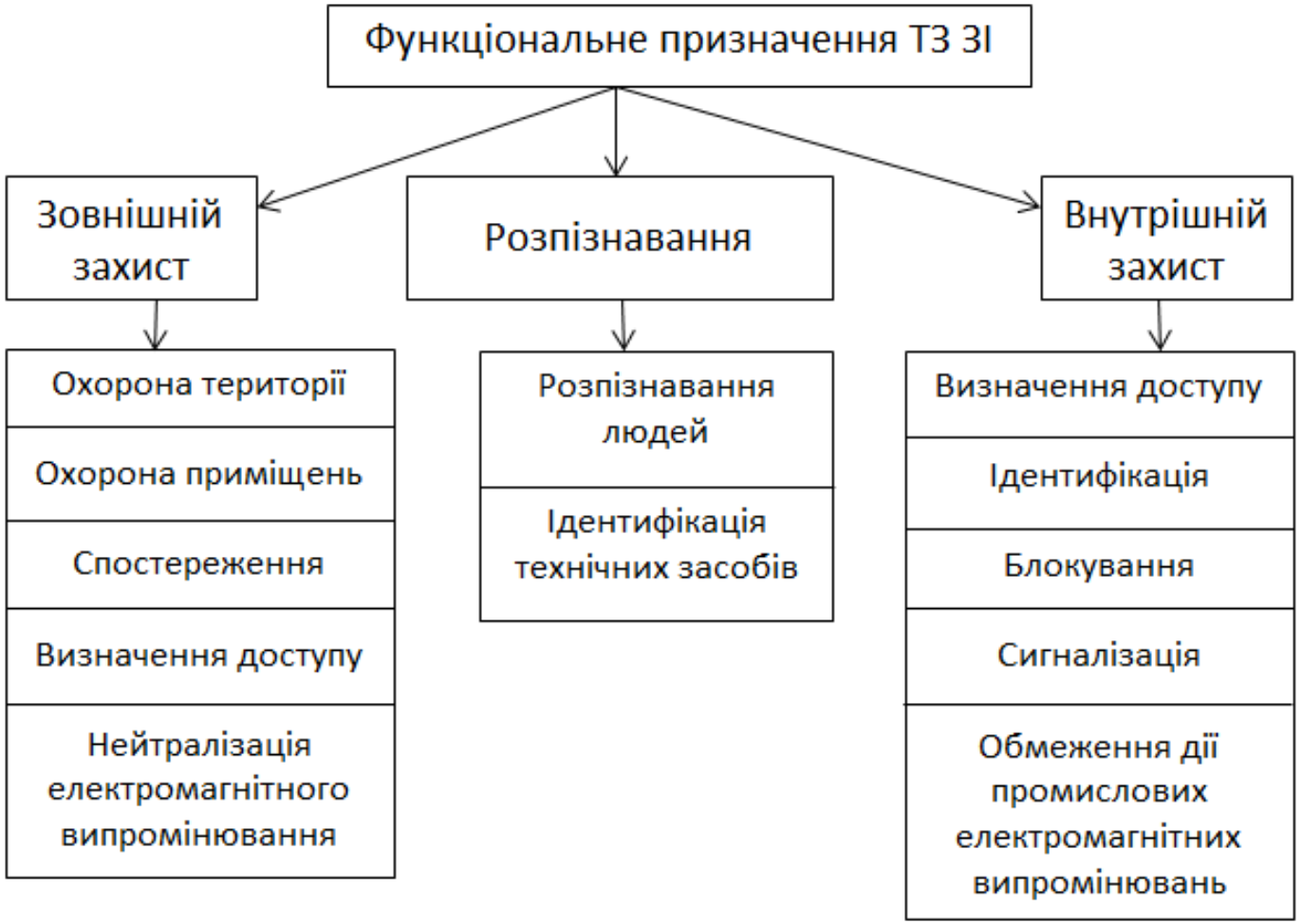
Класифікація ТЗ $ЗІ_2$

- Ступень складності пристрою:
  - **Прості пристрої** — нескладні прилади та пристрої, що виконують окремі процедури захисту.
  - **Складні пристрої** — комбіновані агрегати, які з деякої кількості простих пристроїв, здатні до здійснення складних процедур захисту.
  - **Системи** — закінчені технічні об'єкти, здатні здійснювати деяку комбіновану процедуру захисту, що має самостійне значення.

Класифікація ТЗ $ЗІ_3$

- Спряженість із засобами обчислювальної техніки (ОТ):
  - **Автономні** — засоби, що виконують свої захисні функції незалежно від функціонування засобів ОТ, тобто. повністю автономно.
  - **Парні** — засоби, виконані у вигляді самостійних пристроїв, але виконують захисні функції у поєднанні (спільно) з основними засобами ОТ.
  - **Вбудовані** — засоби, які конструктивно включені до складу апаратури ОТ.

Класифікація ТЗ ЗІ за функціональним призначенням



Технічні засоби захисту території і об'єктів

Технічні засоби захисту території і об'єктів$_1$

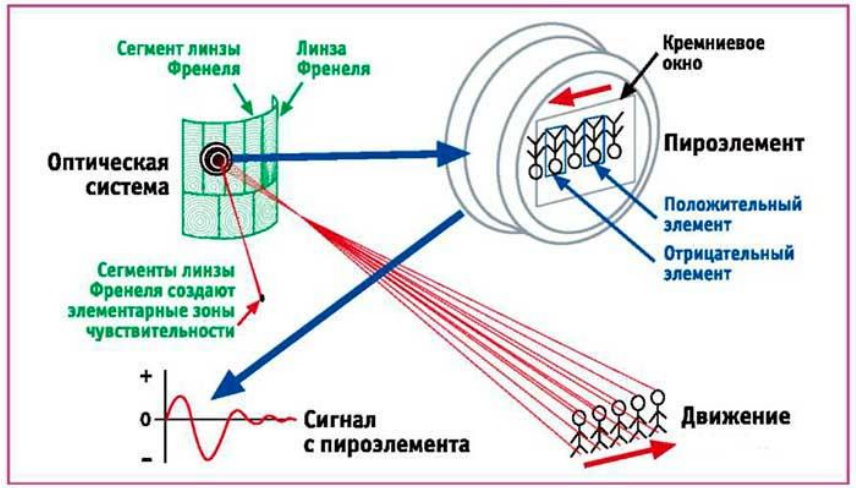
ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ТЕРИТОРІЇ І ОБ'ЄКТІВ

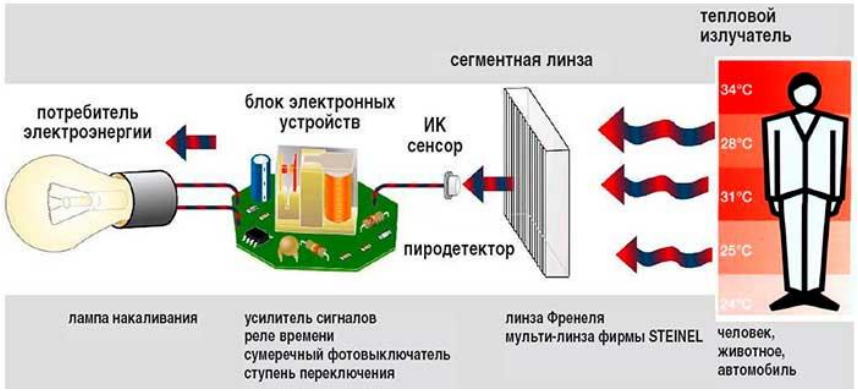
ЗАМКИ З КОДОВИМ НАБОРОМ



ДАТЧИКИ

- датчики для виявлення *спроб проникнення* на територію об'єкта або в контрольоване приміщення;
- датчики для виявлення *присутності людини* в приміщенні;
- датчики для виявлення *переміщення* предмета, що охороняється







Технічні засоби захисту території і об'єктів$_2$

Типи пожежно-захисних систем відповідно із вимогами щодо технічного захисту

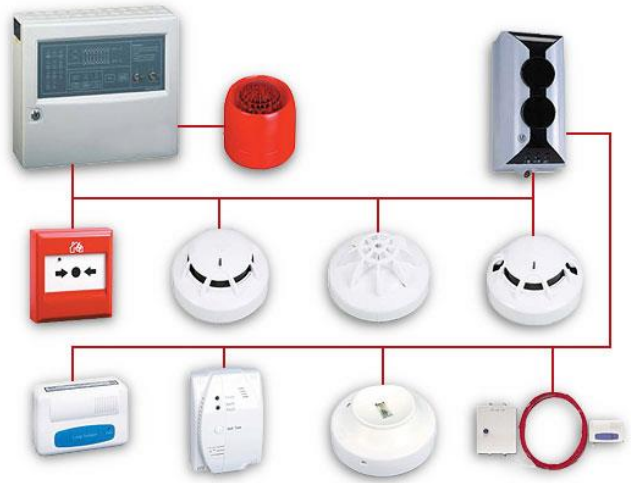
зовнішні системи сигналізації проникнення

внутрішні системи сигналізації проникнення

системи сигналізації пожежної охорони



- однорубіжні
- дворубіжні
- багатозонні



Елементи ТЗ об’єктів

- Елементами технічного захисту об'єктів є:
  - засоби виявлення;
  - засоби управління доступом до об'єкту;
  - засоби збору, обробки і відображення інформації від систем виявлення;
  - засоби постового телефонного (радіо) зв'язку і тривожно-викличної сигналізації;
  - технічні засоби спостереження;
  - засоби розвідки;
  - допоміжні засоби (система електроживлення технічних засобів охорони, кабельні мережі і комунікації, тощо);
  - електризовані загородження.





Центральний пульт управління

- На базі вищезазначених елементів будуються різноманітні системи технічних засобів охорони.
- Центральний пульт управління включає в себе:
  - автоматизовані робочі місця операторів, адміністраторів систем (комплексу), постів охорони та служби безпеки;
  - засоби збору, обробки та відображення інформації — комп'ютери, керуючі панелі, сервери, пульти, консолі управління та інша апаратура.



Система охоронної і тривожної сигналізації

- Система охоронної і тривожної сигналізації включає в себе:
  - ***засоби виявлення*** — сповіщувачі, датчики (сенсори);
  - ***засоби тривожної сигналізації*** — кнопки, педалі, сповіщувачі;
  - ***засоби збору, обробки та відображення інформації*** — контрольні панелі, концентратори, комп'ютери, розширювачі, світлові та звукові сповіщувачі, тощо.



Система охоронного відеонагляду

- Система охоронного відеонагляду включає в себе:
  - камери відеоспостереження;
  - пульти управління;
  - пристрої обробки і збереження відеоінформації.



Система контролю і управління доступом

- Система контролю і управління доступом включає в себе:
  - ***приймальні пристрої доступу*** — ідентифікатори особи, зчитувачі, пристрої введення кодів, пульти, панелі і консолі управління тощо;
  - ***виконавчі пристрої доступу*** — електромеханічні, електромагнітні і механічні кодові замки, автоматичні турнікети та шлагбауми тощо;
  - ***засоби виявлення різного типу*** - металодетектори, виявителі вибухових речовин і радіаційних матеріалів тощо;
  - ***засоби збору, обробки та відображення інформації*** — контрольні панелі, концентратори, комп'ютери, розширювачі, світлові та звукові сповіщувачі тощо.



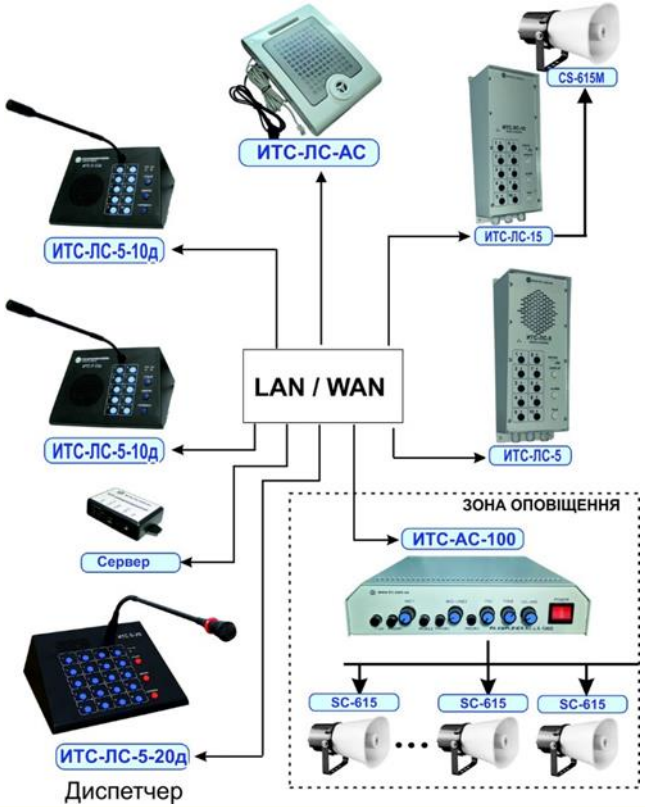
Системи безперебійного і резервного живлення

- Система безперебійного і резервного електроживлення включає в себе:
  - джерела безперебійного електроживлення;
  - генератори бензинові, дизельні;
  - випрямлячі і блоки живлення;
  - акумулятори.



Системи оперативного і постового зв’язку

- Система оперативного і постового зв'язку включає в себе:
  - засоби провідного службового зв'язку;
  - засоби гучномовного службового зв'язку;
  - засоби реєстрації службових переговорів;
  - засоби радіозв'язку охорони.



Система оповіщення та управління евакуацією

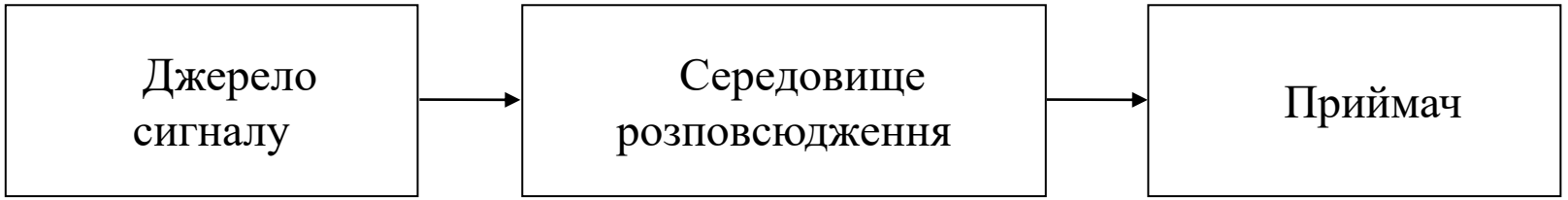
- Система оповіщення та управління евакуацією включає в себе:
  - засоби оповіщення — сирени, гучномовці, світлові табло і показчики, тощо;
  - засоби контролю і управління зонами оповіщення та аварійною автоматикою — підсилювачі, комутатори, магнітофони, мікрофони тощо.



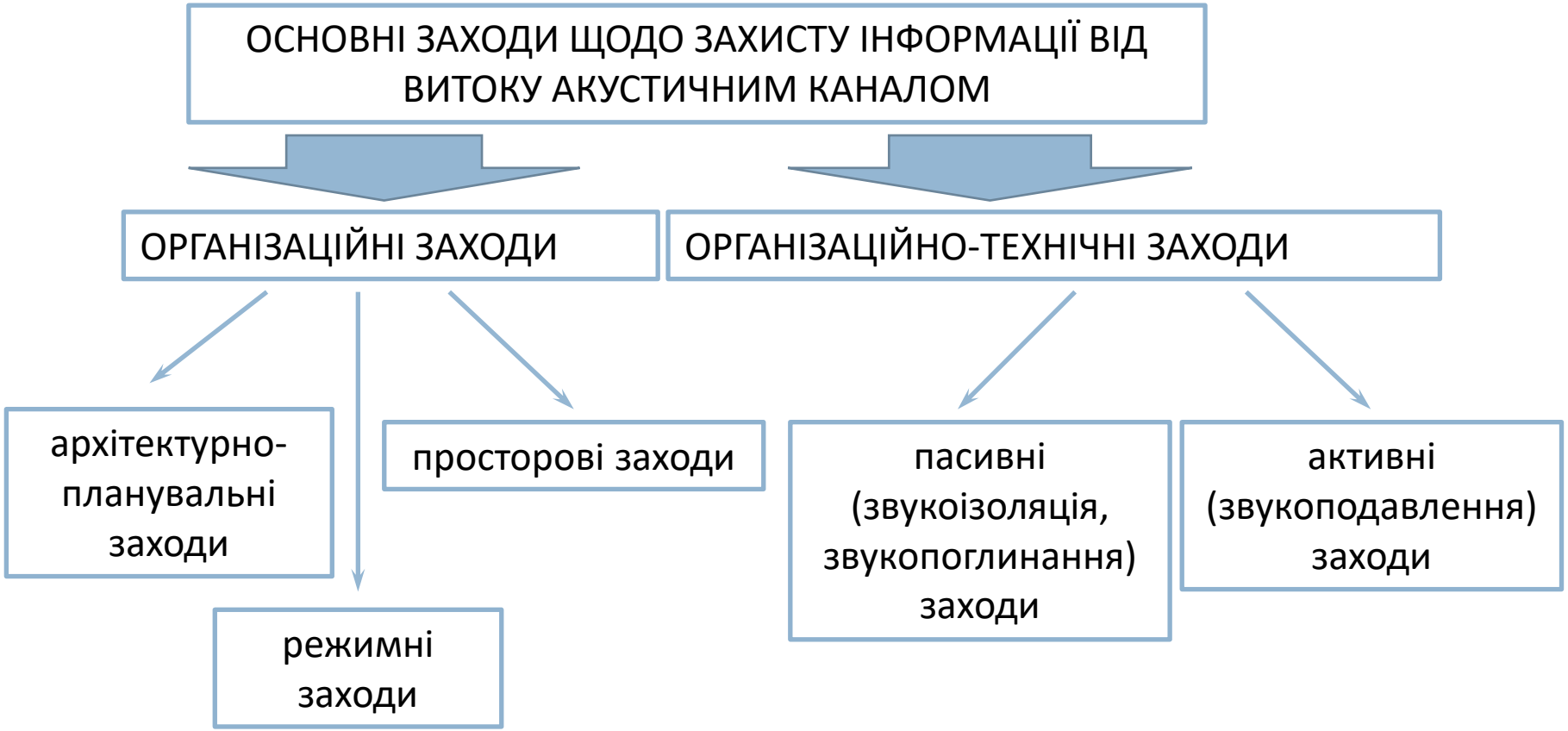
Акустичні засоби захисту

Акустичний канал

- **Захист інформації від витоку акустичним каналом** – комплекс заходів, що виключають або зменшують можливість виходу конфіденційної інформації за межі контрольованої зони за рахунок акустичних полів.



Основні заходи захисту



Реалізація захисту від витоку акустичними каналами

- Для захисту приміщення по акустичному каналу, використовуються **акустичні генератори шуму**.
- **Акустичний шум** - шум, який характеризується нормальним розподілом амплітудного спектру та сталістю спектральної щільності потужності на всіх частотах.

Технічні засоби просторового та лінійного зашумлення

Засоби створення акустичних маскуючих перешкод:

- генератори шуму в акустичному діапазоні;
- пристроїв віброакустичного захисту;
- технічні засоби ультразвукового захисту приміщень.

Засоби створення електромагнітних маскуючих перешкод:

- технічні засоби просторового зашумлення;
- технічні засоби лінійного зашумлення

засоби створення маскуючих перешкод у комунікаційних мережах

засоби створення маскуючих перешкод у мережах електроживлення

Багатофункціональні засоби захисту

Пасивні види заходів захисту

- **Архітектурно-планувальні заходи** передбачають виконання певних вимог при проектуванні чи реконструкції приміщень з метою виключення чи ослаблення неконтрольованого розповсюдження звуку. Наприклад – особливе розташування приміщень чи обладнання їх елементами акустичної безпеки (тамбури, орієнтування вікон у бік контрольованої зони)
- **Режимні заходи** – суворий контроль перебування у контрольованій зоні працівників та відвідувачів
- **Організаційно-технічні заходи** - використання звукопоглинальних засобів. Пористі та м'які матеріали типу вати, ворсисті килими, пінобетон, пориста суха штукатурка є хорошими звукоізолюючими та звукопоглинаючими матеріалами – у них дуже багато поверхонь розділу між повітрям та твердим тілом, що призводить до багаторазового відображення та поглинання звукових коливань (звукопоглинання)

Активні засоби захисту

- Коли **Пасивні заходи** не забезпечують необхідного рівня безпеки, використовуються активні засоби. До активних засобів відносяться генератори шуму - технічні пристрої, що виробляють шумоподібні сигнали. Ці сигнали подаються на датчики акустичного або вібраційного перетворення.
- **Акустичні датчики** призначені для створення акустичного шуму в приміщеннях або поза ними, а **Вібраційні** - для маскуючого шуму в огороджуючих конструкціях.
- **Вібраційні датчики** приклеюються до конструкцій, що захищаються, створюючи в них звукові коливання.
- **Генератори шуму** дозволяють захищати інформацію від витоку через стіни, стелі, підлоги, вікна, двері, труби, вентиляційні комунікації та інші конструкції з досить високим ступенем надійності

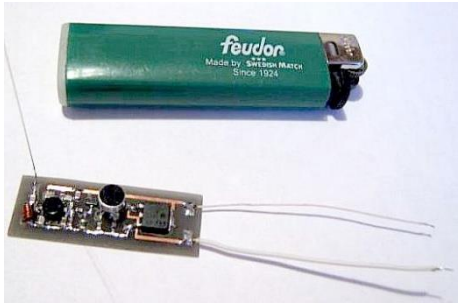
Реалізація захисту від витоку акустичними каналами

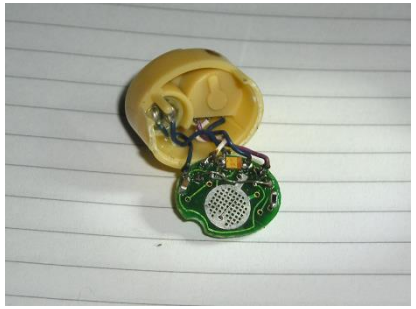
- Відбувається шляхом:
  - застосування звукопоглинаючих покриттів, спеціальних додаткових тамбурів дверей, подвійних віконних палітурок;
  - використання засобів акустичного зашумлення об'єктів та поверхонь;
  - закриття вентиляційних каналів, систем введення в приміщення опалення, електроживлення, телефонних та радіокомунікацій;
  - використання спеціальних атестованих приміщень, що виключають появу каналів витоку інформації.

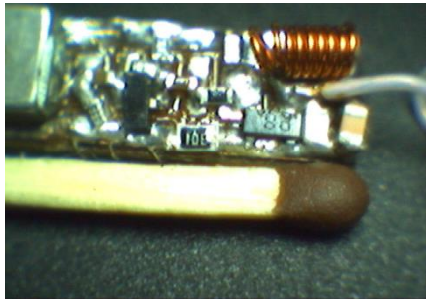
Захист від радіозакладок

Радіозакладки

- У загальному випадку пристрій працює як радіопередавач.











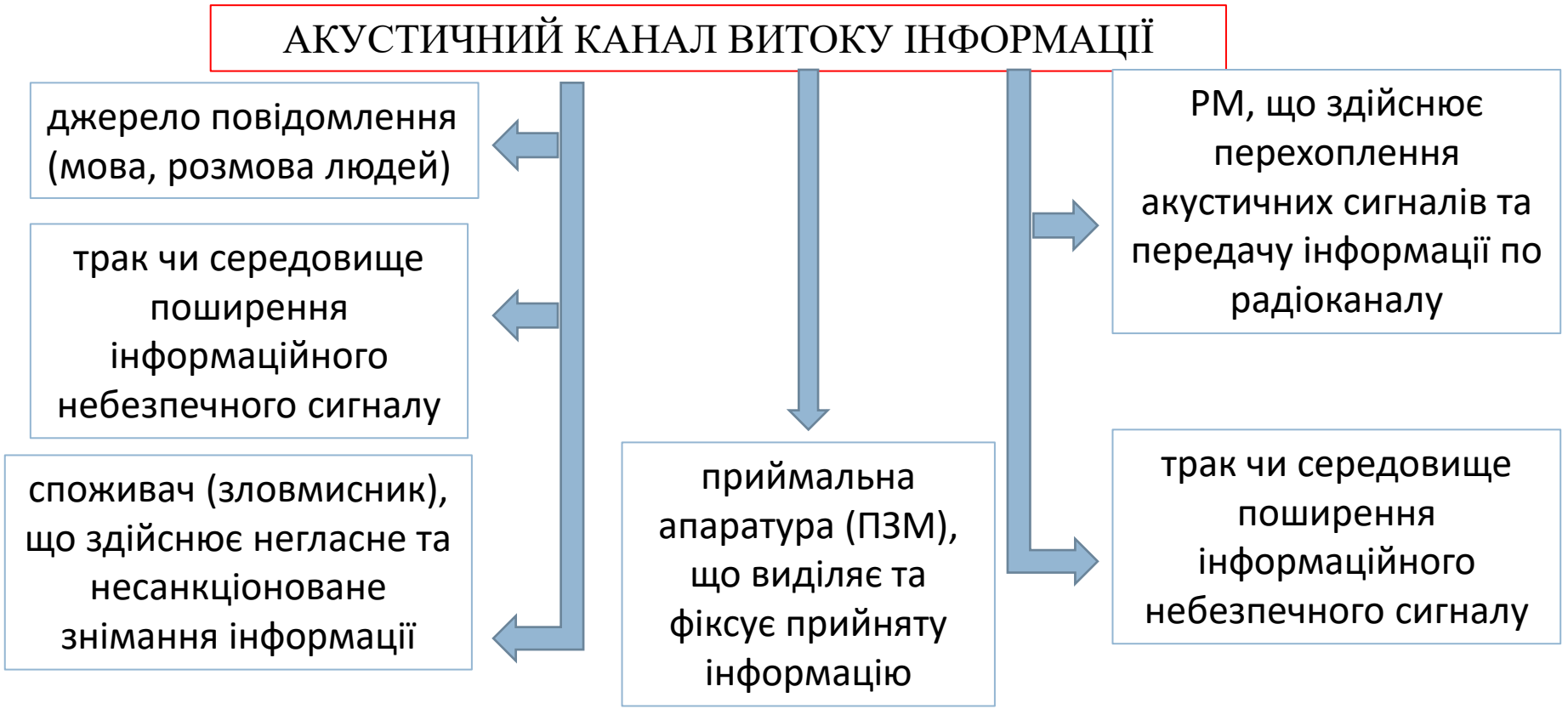


Захист від радіозакладок

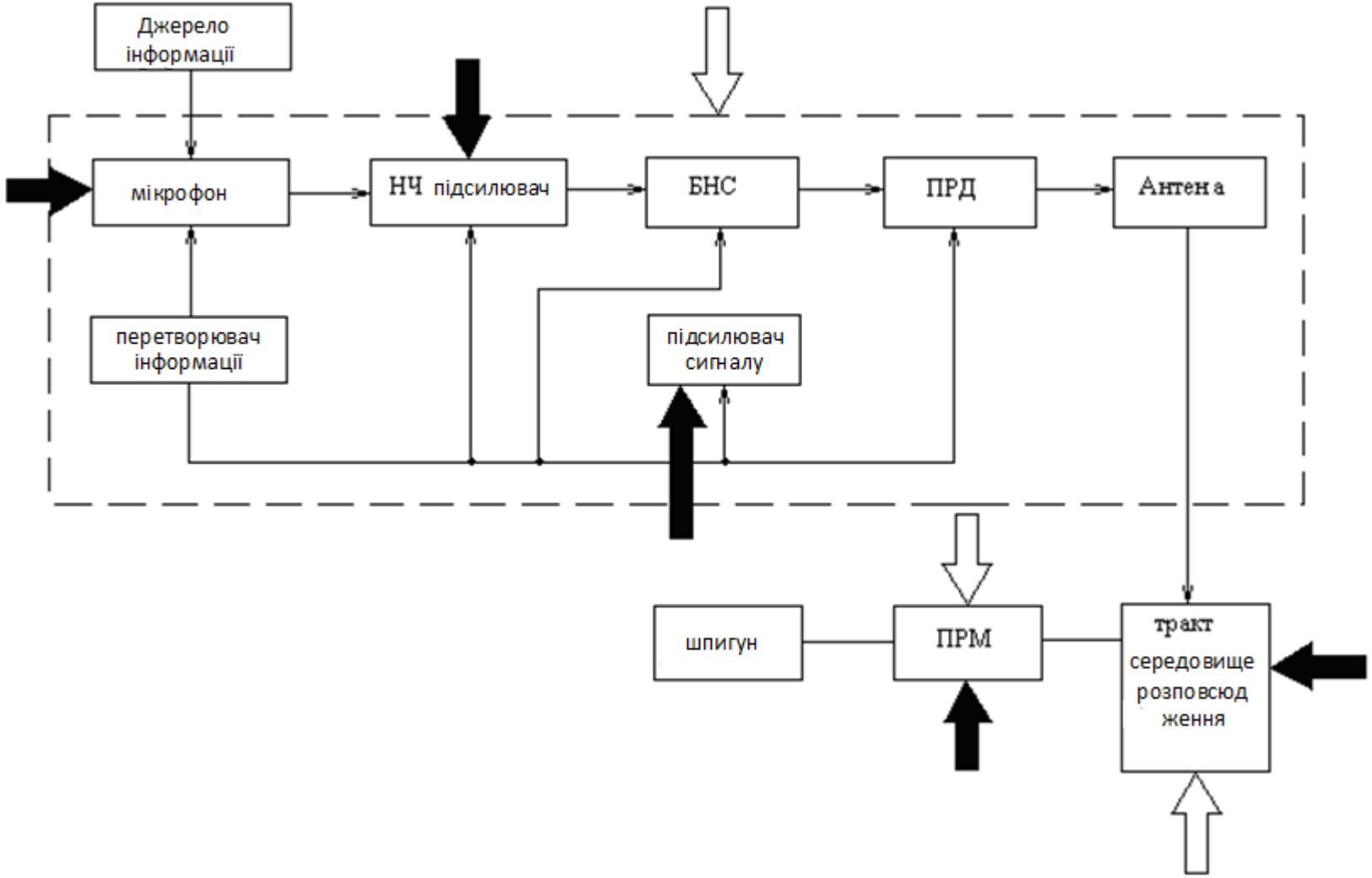
- Апаратура придушення являє собою генератор (передавач) шумових перешкод, який встановлюється в зашумлюваному приміщенні.
- При цьому відстань від радіовипромінюючих закладок до приймальних пристроїв перехоплення їх випромінювань буде практично така ж, як від передавача шумових перешкод до цих приймальних пристроїв, що пригнічуються.
- За такого тактичного застосування передавача перешкод повністю знімається невизначеність щодо розміщення приймальних пристроїв перехоплення випромінювань радіозакладок, забезпечується простота використання апаратури придушення, висока надійність та ефективність протидії

Методи і засоби захисту від радіомікрофонів

- Для аналізу і класифікації методів та засобів захисту від радіомікрофонів (РМ) доцільно розглянути акустичний канал витоку інформації (АКВІ), утворений РМ, як типовий канал передачі.



Найпростіший радіомікрофон



Пасивні і активні методи захисту від РМ

- **Пасивні методи (світлі стрілки)** реалізуються шляхом пошуку РМ як фізичних об'єктів або електронних засобів за їх подальшим усуненням або шляхом загального електромагнітного екранування виділених приміщень.
- **Активні методи (темні стрілки)** реалізуються шляхом придушення та його елементів, а також навмисного «зашумлення» тракту чи середовища розповсюдження інформаційного сигналу.
- **Універсальним пасивним методом захисту** є загальне електромагнітне екранування приміщень, що призводять до зниження інформаційних сигналів РМ (та інших випромінюючих засобів, наприклад ПЕОМ) до рівня внутрішніх шумів каналу, що еквівалентно їх локалізації або розриву АКВІ.
- **Методика виявлення РМ як фізичних об'єктів**, із цілком певними властивостями та вагогабаритними характеристиками, проводиться шляхом візуального огляду місць можливого розміщення РМ у контрольованому приміщенні із застосуванням збільшувального скла, дзеркал, засобів спеціального підсвічування тощо.

Захист від вузькоспрямованих мікрофонів

- Кімната для нарад має бути ізольованим приміщенням.
- Для проведення переговорів потрібно вибирати приміщення, стіни яких не є зовнішніми стінами будівлі.
- Контроль приміщень, що знаходяться на одному поверсі з кімнатою для нарад, а також приміщень, що знаходяться на суміжних поверхах

Технічні засоби захисту від вбудованих та вузькоспрямованих мікрофонів

- ТЗ ЗІ від РМ:
  - генератори акустичного шуму;
  - генератори шуму в радіодіапазоні;
  - сканери - спеціальні приймачі для виявлення радіовипромінювань;
  - нелінійні локатори;
  - нелінійні локатори провідних ліній;
  - детектори працюючих магнітофонів;
  - скремблер (системи захисту телефонних переговорів);
  - аналізатори спектра;
  - частотоміри;
  - детектори мережі 220 В 50Гц;
  - детектори підключень до телефонної лінії;
  - комплекси, що забезпечують виконання кількох функцій щодо “очищення приміщень”;
  - програмні засоби захисту комп'ютерів та мереж;
  - системи та засоби захисту від несанкціонованого доступу, у тому числі системи біометричного доступу

Пристрої пошуку технічних засобів розвідки

Класифікація пристроїв пошуку технічних засобів розвідки

- **ПРИСТРОЇ ПОШУКУ АКТИВНОГО ТИПУ**:
  - нелінійні локатори (досліджують відгук на вплив електромагнітного поля);
  - рентгенметри(просвічують за допомогою рентгенівської апаратури);
  - магніто-резонансні локатори (використовують явище орієнтації молекул у магнітному полі).
- **ПРИСТРОЇ ПОШУКУ ПАСИВНОГО ТИПУ**:
  - металошукачі;
  - тепловізори;
  - пристрої та системи пошуку по електромагнітному випромінюванню;
  - пристрої пошуку зміни параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);
  - пристрої пошуку зміни магнітного поля (детектори записуючої апаратури).

Нелінійні локатори



ORION 2.4 HX може з успіхом застосовуватися службами безпеки і правоохоронними органами для виявлення пристроїв негласного знімання інформації, виявлення заборонених до проносу і зберігання електронних пристроїв (стільникових телефонів, sim карт і т. п.). Вартість 1093840 грн

Особливості локатора

Відображення залежності (гістограма) гармонічних відгуків (2-а, 3-я гармоніки) від рівня випромінюваного сигналу.
•Ручне та автоматичне регулювання потужності випромінюваного сигналу (3.3Вт)
•Обробка сигналу цифровим сигнальним процесором, регулювання підсилення забезпечує збільшення дальності виявлення при незмінній потужності.
•Компактний, за рахунок полегшеного дизайну прилад має вагу 1,4 кг. Усі блоки інтегровані в єдину конструкцію.
•Кругова поляризація передавальної та приймальної антен зменшує ймовірність пропустити ціль через невідповідну орієнтацію антени.
•Запатентований алгоритм кореляції високочутливого приймача (-140 dBm) 2-ї і 3-ї гармоніки з передавачем покращує виявлення цілі, помилкові спрацьовування.
•Дисплей, змонтований на антені, робить зручним пошук та аналіз параметрів.
•Сенсорний OLED 2,7″ дисплей керування та індикації змонтований на рукоятці приладу.
•Світлодіодне підсвічування робочої ділянки.
•Наявність декількох режимів вибирання вільного каналу частот (60 каналів у діапазоні 2,404 – 2,472 ГГц): ручне вибирання частоти, автоматичне вибирання частоти, безперервне переналаштування частоти в діапазоні (Sweep), випадкова зміна частоти в діапазоні (Hop).
•П’ять режимів прослуховування: Tones, Listen (2ndAM, 2ndFM, 3rdAM, 3rdFM)
•Індикація тривоги — візуальна, звукова та вібраційна при виявленні небезпечної цілі.
•Робоча частота в діапазоні 2,4 ГГц для виявлення мініатюрних електронних компонентів.

Трьохдіапазонний індикатор поля iPROTECT 1216



Професійний трьохдіапазонний індикатор поля, створений для виявлення всіх типів радіочастотних підслуховувальних пристроїв, у тому числі аналогових і цифрових, а також тих, які передають інформацію по мобільним мережам і використовують бездротові стандарти.

Вартість 34980 грн

Характеристики

-Пошук цифрових і аналогових аудіо, відео передатчиків усіх типів, включаючи бездротові відеокамери
-Частотний діапазон: 50 МГЦ -12 ГГц
-Розподіл на 3 діапазони дозволяє уникнути втрати чутливості поблизу перешкод
-Режими відображення: "Всі діапазони" (ALL BANDS) і "Один діапазон" (ONE BAND)
-Висока чутливість до пристроїв 3G, Wi-Fi і Bluetooth
-Робочі режими: вібрація (Без звуку), звуковий (Аудіо), і Сигнал тревоги
-Регульований поріг спрацювання сигналу тривоги Alarm
-Портативний, надійний і простий у використанні
-Основний дисплей відображає поточний рівень радіочастот
-Гістограма відображає радіочастотний сигнал протягом 5 секунд (в режимі відображення «ONE BAND»)
-Відображення можливого типу сигналу на інформаційному дисплеї
-Вбудована, спрямована СВЧ-антена
-Ударостійкий дюралюмінієвий корпус
-Литий-іонна батарея з ресурсом роботи до 6 годин -- Мікропроцесорне управління
-2 OLED-дисплея електронних компонентів.

Комплект інструменту для огляду ОТК-4000



Категорія: Устаткування для виявлення каналів витоку інформації
Призначення: Пошуковий комплект інструментів для фізичного підтвердження наявності пристроїв негласного знімання інформації.

КОМПЛЕКТАЦІЯ ОТК-4000:

Тримач – для встановлення магніту або дзеркала.
Телескопічний утримувач – для магніту або дзеркала.
Магніт – для вилучення металево
УФ маркер – застосовується для маркування положення гвинтів. При наступній перевірці бачимо маркування УФ ліхтарем.
Дзеркало для огляду в корпусах приладів.
УФ-ліхтар - використовується спільно з УФ маркером.
Ліхтар – світлодіодний ліхтар.
Бороскоп з поворотним дзеркалом - свердлить у гіпсокартонній стіні невеликий отвір, вставляєте в нього бороскоп і, обертаючи дзеркало, вивчаєте простір на наявність електронних пристроїв.
Рулетка.
Мультитул - багатофункціональний складний інструмент.
Інструмент для зачищення кабелю, пасатижі, розвідний ключ.
Реверсивна викрутка – з набором біт усередині.
Маленькі викрутки.
Щупи для трасувальника - використовуються з трасувальником ліній.
Щупи для мультиметра – використовуються мультиметром.
Трасувальник ліній – для відстеження провідних ліній у стінах.
Молоток із гумовими головками.
Цвяходер.
Інструмент для закладення кабелю в крос.
Мультиметр.
Багатофункціональний детектор для виявлення в гіпсокартонних стінах металевих або дерев'яних стійок, а також проводки.

Детектор скритих камер WEGA-i



Модель: WEGA-i
Категорія: Устаткування для виявлення каналів витоку інформації
Призначення: Детектор прихованих камер відеоспостереження WEGA-i визначає наявність оптичних пристроїв незалежно від робочого стану. Якщо розглянути пошук з погляду фізичних процесів, то виявлення ґрунтується на зворотному відображенні спрямованого випромінювання оптичною системою об'єктив камер відеоспостереження. Виявляч прихованих камер відеоспостереження WEGA-i дозволяє виявляти всі типи відеокамер, включаючи «pin hole». Вартість: 19580 грн

ПОРЯДОК ПРОВЕДЕННЯ ПОШУКУ

Визначте зону можливого огляду прихованої відеокамери. Виявлення мікрооб'єктива можливе лише із зони огляду прихованої відеокамери. Увімкніть живлення приладу. Налаштуйте необхідну інтенсивність зондуючого випромінювання. Необхідна інтенсивність випромінювання визначається освітленістю, що відображає здатністю аналізованих поверхонь, а також дистанцією між ними та оператором. Використовуйте еталонну відеокамеру для налаштування приладу та перевірки його працездатності. Проведіть візуальний огляд через окуляр пристрою всіх поверхонь приміщення, елементів меблів та інтер'єру, направляючи випромінювання в зону контролю (search). Особливу увагу слід приділити верхній частині приміщення, особливо елементам підвісних стель. Ретельно огляньте датчики пожежної та охоронної сигналізації та інші елементи інтер'єру, що дозволяють установку та дають достатній огляд прихованій відеокамері. Ознакою ймовірного виявлення мікрооб'єктива служить спостереження яскравої точки, що світиться на контрольованій поверхні або елементі приміщення. Дзеркальні, добре відбивають, поверхні інтер'єру можуть давати схожі світлові відгуки. Незначне переміщення убік дає зміщення чи повне зникнення «хибного» відблиску. Спостереження яскравої стійкої точки, що світиться з різних кутів і дистанцій огляду вказує на ознаки мікрооб'єктиву і вимагає фізичного аналізу для виявлення і знешкодження прихованої відеокамери. Підвищенню ймовірності виявлення сприяє аналіз тих самих поверхонь з кількох точок цільової зони. Мікрооб'єктиви сучасних, приховано встановлюваних відеокамер мають вихідний отвір менше 1 мм. Це дозволяє здійснити їхню установку в предметах меблів, інтер'єру та електронних пристроях, що знаходяться в приміщенні.

Тепловізор FLIR E6



Характеристики

Тепловізор FLIR E6 з функцією мультиспектральної зйомки – MSX. Камера E6 дає змогу вимірювати температуру до +250 °C. Роздільна здатність ік-зображень тепловізора — 160 x 120 пікселів. MSX роздільна здатність 320 x 240 пікселів. Камери FLIR серії Ex – це швидкі тепловізійні камери, які забезпечать Ваш перехід у новий тепловізійний вимір. Тепловізор FLIR E6 є доступною заміною пірометру, тому що створює ІЧ-знімки з інформацією про температуру кожного пікселя. Збереження комбінованих зображень з функцією MSX в ІЧ та візуальному форматі значно збільшує зручність камер FLIR серії Ex.

Модель: FLIR E6 Категорія:
Устаткування для виявлення каналів витоку інформації
Призначення: FLIR E6 дозволяє отримати точну та детальну теплову карту будь-якої поверхні. Кожен піксель отриманого зображення містить дані про температуру. Інфрачервона матриця на основі мікроболометра має чутливість, що дозволяє визначати перепади температур між суміжними пікселями лише 0,06°C. Тепловізор FLIR E6 оснащений безфокусним об'єктивом, завдяки чому керування ним зводиться до натискання однієї кнопки. Функція MSX забезпечує максимальну деталізацію отриманих зображень.
Вартість 149820 грн

Аналізатор проводових ліній TALAN



Категорія: Устаткування для виявлення каналів витоку інформації
Призначення: Цифровий аналізатор дротових та телефонних ліній TALAN версії 3.0 – це професійний прилад, який дозволяє обстежити дротові лінії на наявність пристроїв негласного знімання та витоку інформації.
Талан поєднує в собі сучасні технічні методи перевірки провідних та телефонних ліній та дає розширені можливості щодо аналізу аналогових, цифрових та VoIP телефонних систем.

Особливості TALAN

-Проведення робіт з виявлення підслуховуючих пристроїв на провідних лініях.

-Пошук обривів, коротких замикань кабелю.

-Відстеження кабелів.

-Перевірка роботи телефонних ліній, апаратів, АТС (включаючи цифрові та VoIP).
-Установки та обслуговування ліній внутрішнього зв’язку, телефонних мереж, мереж передачі даних.

-Аналіз трафіку ліній внутрішнього зв’язку.

-Оцінки використання каналів зв'язку.

Аналізатор спектру OSCOR Green (OGR-24)



Модель: OSCOR Green (OGR-24)

Категорія: Устаткування для виявлення каналів витоку інформації

Призначення: У всьому світі стрімко розвивається застосування систем зв'язку в різних галузях, особливо мобільних та супутникових систем, що використовують широкосмугові канали зв'язку. OSCOR Green є серйозним інструментом для оцінки та інтеграції цих систем у радіочастотному діапазоні.

OSCOR Green OGR-24:
-Виявляє несанкціоновані сигнали в сильно завантаженому радіочастотному спектрі.

-Аналіз розподілу радіочастотних сигналів

-Оцінки використання каналів зв'язку

-Визначення зони покриття систем зв'язку (вишки стільникового зв'язку, радіорелейні системи)

-Установки та обслуговування бездротових систем передачі даних.

Аналіз та розподіл радіочастотного спектру має велике значення для багатьох організацій, таких як оператори бездротового зв'язку, аеропорти, порти, лабораторії, під час проведення проектних та розвідувальних робіт. OSCOR Green є чудовим інструментом для виявлення «складних» радіочастотних сигналів у несприятливій обстановці.

Багатофункціональний пошуковий пристрій Andre Advanced



Категорія:Устаткування для виявлення каналів витоку інформації

Багатофункціональний пошуковий пристрій ANDRE призначений для виявлення джерел радіочастотного сигналу в ближній зоні прийому. Прилад поєднує широкополосний детектор електромагнітного поля, приймач інфрачервоного діапазону, різні додаткові зонди для перевірки провідних ліній та оцінки віброакустичного захисту приміщення. ANDRE дозволяє виявляти всі основні типи пристроїв негласного знімання інформації, включаючи аудіо, відео, телефонні, інфрачервоні та передавачі, що носяться на тілі. Комплектація приладу має широкий набір пошукових зондів та аксесуарів, які дозволяють збільшити ефективність пошуку.
Вартість: 359480 грн

ОСНОВНІ МОЖЛИВОСТІ

Портативний широкосмуговий індикатор електромагнітного поля здатний миттєво аналізувати спектр радіочастот в діапазоні від 10 кГц до 6 ГГц з оптимальною дальністю виявлення.
Час відгуку під час аналізу цифрових і аналогових радіосигналів трохи більше 10 наносекунд – вище ніж в будь-якого сучасного спектроаналізатора.
Автоматичний аналіз виявлених сигналів та визначення їх належності до дозволених діапазонів.
Створення списку сигналів.
Вимірювання частоти найбільш потужного сигналу.
AM та FM демодулятори з осцилоскопом.
Локалізація джерела сигналу щодо відносного рівня, зміни потужності сигналу.
Режим моніторингу - активація сигналу тривоги (світловий, звуковий або вібраційний) при появі сигналу пристрою, що підслухує.
Можливість перевірки дротових ліній, вбудований детектор інфрачервоного та видимого діапазону.
Виявлення та аналіз акустичних витоків та ультразвукових коливань.
Збереження знімків екрана, запис списку сигналів у форматі Excel, запис аудіо файлів для складання наступної звітності
Сенсорний екран 3.5” компактний розмір приладу.
USB-порт для передачі даних.

Устаткування протидії витоку інформації PHONE SAFE SUMMIT



Модель: PHONE SAFE SUMMIT

Категорія: Устаткування протидії витоку інформації
Призначення: Пристрій блокування акустичного каналу телефону
Вартість: 41580 грн

Мобільний зв'язок та мобільний інтернет несуть нескінченний ряд переваг для спілкування та бізнесу, водночас створюючи певні загрози витоку інформації.
Одним із потенційних каналів витоку є мікрофон телефону, який може сприймати акустичну інформацію з високою чутливістю. Пристрій PHONE SAFE SUMMIT був розроблений фахівцями інформаційної безпеки для захисту від такої загрози.

У розрахунок було взято такі стандартні функції чи вразливості сучасних телефонів:
-За згодою власника телефон може транслювати акустичну інформацію через телефонний або інтернет-канал у режимі піднятої трубки.
-За згодою власника на смартфоні може бути запущено програму звукозапису «Диктофон».
-Режими можуть бути приховані, без освітлення на екрані.
-Без відома власника на смартфон може бути встановлене шпигунське програмне забезпечення (spyware), яке дозволяє зловмисникам активувати приховане прослуховування звуку навколо телефону.
-Відомі випадки передачі такого програмного забезпечення шляхом експлуатації вразливих функцій деяких месенджерів
-Акустична обстановка навколо телефону може передаватися на сервер або хмарний сервіс зловмисників у реальному режимі часу або з накопиченням та періодичним розвантаженням

Устаткування протидії витоку інформації PHONE SAFE ULTRA



Модель: PHONE SAFE ULTRA
Категорія: Устаткування протидії витоку інформації
Пристрій PHONE SAFE ULTRA призначений для захисту від витоку інформації через мікрофон телефону.
Вартість: 21780 грн

Мобільний зв'язок та мобільний інтернет несуть нескінченний ряд переваг для спілкування та бізнесу, водночас створюючи певні загрози витоку інформації.
Одним із потенційних каналів витоку є мікрофон телефону, який може сприймати акустичну інформацію з високою чутливістю. Пристрій PHONE SAFE SUMMIT був розроблений фахівцями інформаційної безпеки для захисту від такої загрози.

У розрахунок було взято такі стандартні функції чи вразливості сучасних телефонів:
-За згодою власника телефон може транслювати акустичну інформацію через телефонний або інтернет-канал у режимі піднятої трубки.
-За згодою власника на смартфоні може бути запущено програму звукозапису «Диктофон».
-Режими можуть бути приховані, без освітлення на екрані.
-Без відома власника на смартфон може бути встановлене шпигунське програмне забезпечення (spyware), яке дозволяє зловмисникам активувати приховане прослуховування звуку навколо телефону.
-Відомі випадки передачі такого програмного забезпечення шляхом експлуатації вразливих функцій деяких месенджерів
-Акустична обстановка навколо телефону може передаватися на сервер або хмарний сервіс зловмисників у реальному режимі часу або з накопиченням та періодичним розвантаженням

Комплект віброакустичного захисту DNG-KIT1

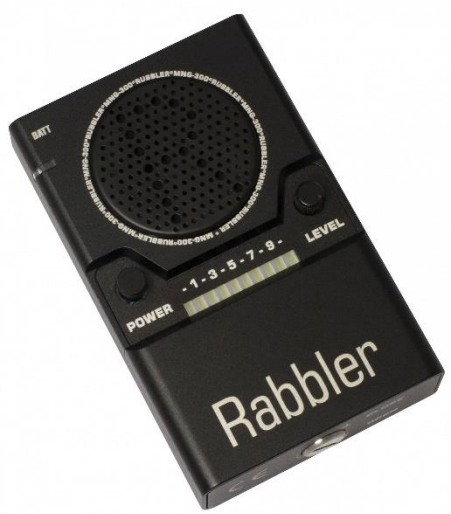


Модель: DNG-KIT1
Категорія: Устаткування протидії витоку інформації
Призначення: Протидія несанкціонованого зняття інформації через віброакустичні канали
Вартість: 85360 грн

ХАРАКТЕРНІ ОСОБЛИВОСТІ:

-Потужний захист від витоку для всіх видів віброакустики шляхом передачі нефільтрованого шуму на навколишні конструкції та порожнини.
-Перешкоджає настінним контактним мікрофонам, віконним лазерним системам та провідним мікрофонам усередині стін, порожнин та вентиляційних шахт (вентиляційних труб)
-Є ключовою частиною захисної системи, яка також включає підключені до проводів вібровипромінювачі та акустичні випромінювачі
-Генерація білого шуму – вихідні перешкоди рівномірно розподіляються за спектром людського голосу
-Має 3 незалежні вихідні канали: 2 для вібровипромінювачів та 1 для акустичного випромінювання
-Усі 3 канали можна регулювати окремо за рівнем
-Кожен канал вібровипромінювача TD2300 може живити до 12 перетворювачів, встановлених на важких або твердих конструкціях (бетон/цегла/цегла), та до 24 перетворювачів на легких конструкціях (скло, труби, гіпсокартон, дерево)
-Канал акустичного випромінювання може живити до 12 динаміків - Вхід керування режимом ПРИГЛУШЕННЯ акустичних випромінювачів дозволяє користувачеві тимчасово вимкнути динаміки.
https://www.das-ua.com/ru/katalog/obladnannya-protidii-zasobam-znimannya-informacii/komplekt-vibroakustichnogo-zaxistu-dng-kit1/

Мобільний генератор шуму MNG-300 Rabbler



Модель: MNG-300 Rabbler
Категорія: Устаткування протидії витоку інформації
Новий підхід до питання захисту від диктофонів та прослуховування.
Прилад генерує мову, яка ефективно захищає від запису.
Вміщується в кишеню або невелику сумочку (розмір пачки цигарок). Вартість: 16060 грн

ХАРАКТЕРНІ ОСОБЛИВОСТІ:

MNG-300 Rabbler створює додатковий бар'єр, який маскує вашу мову. Така перешкода виникає при досягненні певного рівня шуму. У цьому випадку підслуховувальні пристрої продовжують працювати, але сприймають лише шумову компоненту, тоді як інформаційна частина знижується до втрати розбірливості. Завдяки типу шуму «речеподібна перешкода», очищення запису або отриманої інформації неможливо, якщо було досягнуто достатній рівень шуму.

Види пристроїв, що підслуховують, від яких захищає MNG-300 Rabbler:
-диктофони
-радіомікрофони
-GSM та 3G жучки
-відеокамери, годинники, краватки і т. д. (пригнічення акустики)
-дротові мікрофони
-інші види «жучків»

Генератор шуму DNG-2300



Модель: DNG-2300
Категорія: Устаткування протидії витоку інформації
Призначення: 3-канальний генератор акустичного "білого" шуму (2 канали "вібро" + 1 канал "акусто"). Призначений для захисту периметра приміщення від знімання інформації через стетоскоп, контактні мікрофони.
Використовується з вібровипромінювачів TRN-2000. При використанні акустичного випромінювача OMS-2000 може створювати перешкоди для диктофонів та закладок усередині приміщення. Смуга частот 250-5000 Гц. Має канал зворотного зв'язку для налаштування рівня.
Вартість: 39160 грн

Генератор DNG-2300, укомплектований вібровипромінювачами та акустичними випромінювачами (динаміками), протидіє всім вищезгаданим методам прослуховування, наводячи потужні перешкоди, що не фільтруються, на структуру будівлі і всередині порожнин.

ХАРАКТЕРНІ ОСОБЛИВОСТІ:

• Потужний захист від витоку для всіх видів віброакустики шляхом передачі нефільтрованого шуму на навколишні конструкції та порожнини.
• Перешкоджає настінним контактним мікрофонам, віконним лазерним системам та провідним мікрофонам усередині стін, порожнин та вентиляційних шахт (вентиляційних труб)
• Є ключовою частиною захисної системи, яка також включає підключені до проводів вібровипромінювачі та акустичні випромінювачі
• Генерація білого шуму – вихідні перешкоди рівномірно розподіляються за спектром людського голосу
• Має 3 незалежні вихідні канали: 2 для вібровипромінювачів та 1 для акустичного випромінювання
• Усі 3 канали можна регулювати окремо за рівнем
• Кожен канал вібровипромінювача TD2300 може живити до 12 перетворювачів, встановлених на важких або твердих конструкціях (бетон/цегла/цегла), та до 24 перетворювачів на легких конструкціях (скло, труби, гіпсокартон, дерево)
• Канал акустичного випромінювання може живити до 12 динаміків • Вхід керування режимом ПРИГЛУШЕННЯ акустичних випромінювачів дозволяє користувачеві тимчасово вимкнути динаміки

Пристрій забезпечення конфіденційних переговорів DRUID D-06



Модель: DRUID D-06
Категорія: Устаткування протидії витоку інформації
Призначення: Пристрій забезпечення конфіденційних переговорів із кількістю учасників до 6 осіб.
Захищає від будь-яких пристроїв, що підслухують: мікрофонів, диктофонів або стетоскопів.
Принцип роботи ґрунтується на постановці синхронної звукової перешкоди. Живлення від вбудованого акумулятора або мережі 220 В.
У комплекті 6 гарнітур.
Вартість: 129800 грн

ХАРАКТЕРНІ ОСОБЛИВОСТІ:

Забезпечує найвищий ступінь захисту від засобів прослуховування та запису. DRUID D-06 створює потужну протидію будь-яким підслуховуючим пристроям. Навіть людина, що стоїть поруч, не розуміє про що йде розмова, якщо вона не одягла гарнітуру. Гарнітури дозволяють користувачам чути один одного з максимальною чіткістю, незважаючи на потужну перешкоду центрального блоку. Прилад живиться від мережі 220 В або вбудованого акумулятора із ресурсом 6 годин. У комплекті йде кейс для перенесення. Не всі пристрої, що підслуховують, можуть бути виявлені існуючими пошуковими методами. DRUID D-06 – це унікальна система, що забезпечує захист людської мови. Дистанційно-керовані радіомікрофони, дротові мікрофони, пасивні резонатори, міні диктофони - майже всі ці пристрої не виявляються стандартними способами. Навіть сучасний мобільний телефон може містити вбудований диктофон, а це означає, що будь-який телефон, що лежить на столі, може використовуватися для запису розмови. Тому надзвичайно важливо мати надійний захисний пристрій, щоб захищати всі розмови будь-якого ступеня важливості. Принцип роботи DRUID D-06 заснований на генерації звукової перешкоди, яка відтворюється синхронно з мовою людини. Гучність перешкоди вища за гучність розмови, тому ні «жучок» ні диктофон не здатні почути мову. Перешкода, що генерується, не може відфільтровуватися методами шумоочищення. У той же час, перешкода, що відтворюється, не створює незручності учасникам переговорів завдяки спеціальним гарнітурам. Ці гарнітури забезпечують передачу звуку із кристальною чіткістю.

Скремблер для смартфона FSM-U1



Модель: FSM-U1
Категорія: Устаткування протидії витоку інформації
Призначення: FSM-U1 — новий пристрій для кодування розмов для мобільного телефону-смартфону.
У скремблер реалізовано новий потужний алгоритм «закриття» розмови за допомогою технології «багаторазової динамічної обробки фази».
При використанні FSM-U1 підслуховування розмови, яка ведеться по телефону, стає повністю неможливим, незалежно від методики перехоплення.
Вартість: 28380 грн

МЕТОДИКА ЗАСТОСУВАННЯ

При вимкненому скремблюванні FSM-U1 може працювати як гарнітура. Коли ви додзвонилися до Вашого співрозмовника, один із вас включає режим кодування. Протягом кількох секунд Ваші пристрої обмінюватимуться первинними даними та встановлюватимуть зв'язок. Після встановлення зв'язку Ви почуєте звуковий сигнал, що підтверджує входження у «захищений режим». Займеться відповідний світлодіод. Після цього Ви можете спокійно розмовляти на таємні теми. Голос співрозмовника у режимі скремблювання дещо спотворюється. Це нормально, оскільки сигнал проходить багаторазову обробку і потім передається відносно низькоякісним GSM-каналом. Створюваний дискомфорт не можна порівняти з важливістю забезпечення конфіденційності. Для покращення розуміння говоріть повільно і розбірливо, а також використовуйте навушники (поставляються в комплекті).

Принцип роботи
Загальна кількість комбінацій алгоритму – 103,4·1015
Динамічне формування ключа (новий ключ на кожен сеанс) Принцип кодування – багаторазова динамічна обробка фази Двоетапне перетворення мовного потоку:

1. Динамічний поділ на інтервали. У той час, як у «класичного» скремблера статичний інтервал, FSM-U1 ділить мовний потік на ділянки змінної довжини. Первинна розбивка створює від 20 до 50 інтервалів за секунду, потім кожен інтервал розбивається на кількість ділянок різної довжини, що змінюється. Загальна кількість комбінацій першої стадії обробки - 1015
2. Зміна фази кожної динамічної ділянки в межах від 0 до 180° (кількість комбінацій – 180) Генерація та обмін ключами на основі технології Voiceprint

Пошукова система Delta X 2000/6 Real-Time Advanced



Модель: Delta X 2000/6 Real-Time Advanced
Категорія: Устаткування для виявлення каналів витоку інформації
Висока швидкість вимірювань, 2000-3000 МГц в секунду. Діапазон частот 9 кГц – 6000 МГц.
Час існування сигналу: 2-3 секунди.
Миттєво виявляє імпульсні цифрові сигнали.
Може одночасно виявляти та локалізувати передавач.
Поставляється з мобільним терміналом керування (ноутбоком).

ОСОБЛИВОСТІ

-Швидко та надійно виявляє всі види радіочастотних пристроїв негласного знімання інформації, включаючи аналогові, цифрові, що працюють постійно та періодично, що передають аудіо або відео, з шифруванням або без нього
-Знаходить підслуховувальні пристрої, що використовують цифрові стандарти GSM, 3G, 4G/LTE, 5G(<6GHz), Bluetooth, Wi-Fi, DECT і т.п.
-Виявляє приховану передачу інформації в мережі змінного струму, через проводи телефону, у проводах Ethernet, сигналізації та інших кабелях, а також перевіряє інфрачервоний діапазон за допомогою багатофункціонального Зонду, що поставляється в комплекті.
-Може працювати в режимі миттєвого пошуку, цілодобової охорони, локалізації та виявлення GPS маяків
-Має в 20-50 разів більшу чутливість у порівнянні з радіочастотними детекторами та приймачами ближнього поля
-Може контролювати радіочастотну обстановку 24 години на добу з реєстрацією даних
-Можливість виявлення прихованих підслуховуючих пристроїв з функцією накопичення та передавачів, захованих у спектрах інших сигналів
-Підтримує збереження необмеженої кількості сигналів.
-Вся інформація зберігається у базі даних із можливістю перегляду при виявленні чи пізніше.
-Кількість баз даних, що підтримуються, не обмежена
-Демодуляція звуку в FM, AM, USB, LSB, CW (регульована смуга 3…240 кГц)
-Система виконана в захищеному кейсі, що містить ноутбук з діагоналлю до 14″ (ноутбук не включений в комплект поставки)

Техніка для досмотру приміщень та транспорту



Модель: IRIS40-6020Q
Категорія: Техніка для фізичного огляду
Призначення: Для зручного та ефективного огляду вентиляційних каналів, меблів, ніш у конструкціях, ніш радіаторів опалення, простору за підвісними стелями тощо.

Професійне рішення для фахівців у галузі захисту інформації. Дозволяє оглядати важкодоступні місця – вентиляційні канали, меблі, ніші у конструкціях, ніші радіаторів опалення, простір підвісних стель тощо. Керована камера з круговою артикуляцією забезпечує можливість огляду по всіх напрямках, а світлодіодне підсвічування з 7 рівнями яскравості дозволяє оглядати місця з різним рівнем освітлення. Глибина чіткості камери налаштована на більший діапазон відстаней відповідно до потреб пошукових завдань. Довжина зонда 2 м і товщина 6 мм дозволяють проникати в найменші щілини і досягати найвіддаленіших місць під час проведення пошукових робіт.

ХАРАКТЕРИСТИКИ

-Професійна система для огляду важкодоступних місць, ніш та пустот.
-Важлива складова набору для пошуку заставних пристроїв
-Керована камера з дистальним кінцем, що забезпечує всі напрямки артикуляції (360 градусів) та відхилення до 160 градусів -Камера високої роздільної здатності 720P
-Глибина чіткості камери налаштована на великий діапазон відстаней
-Світлодіодне підсвічування з 7 ступенями яскравості
-Титановий зонд високої надійності, стійкий до змащення та води.
-Дисплей 3.5″
-Функція фото та відео фіксації на флеш-карті
-Відеовихід для перегляду зображення на зовнішньому екрані
-Вбудована акумуляторна батарея з ресурсом 3 години
-Зручна магнітна підставка-тримач.
-Дозволяє зручно ставити дисплейний блок на горизонтальну поверхню чи будь-яку металеву поверхню.
-Система швидкого підключення зонда забезпечує можливість легкого обслуговування
-У комплекті кейс для транспортування

Арочний металодетектор Garrett MZ 6100



Модель: Garrett MZ 6100
Категорія: Техніка для фізичного огляду
Призначення: Багатозонний арочний металодетектор для виявлення металевих предметів, що потайно проносяться.
Металодетектор GARRETT MZ 6100 має високу продуктивність, у поєднанні з чудовими характеристиками, новітніми технологіями та оптимальною вартістю.
Вартість 188980 грн.

МОЖЛИВОСТІ АРКОВОГО МЕТАЛОДЕТЕКТОРА GARRETT MZ 6100:

-20 зон виявлення - забезпечують точну вказівку місця виявлення одного або декількох предметів одночасно
Більше 15 стандартних програм для різних умов застосування
200 рівнів регулювання чутливості
Індивідуальне підстроювання чутливості кожної із зон
Автоматичний вибір оптимальної робочої частоти в залежності від навколишнього електромагнітного стану для відбудови від перешкод
Синхронізація металодетекторів — передові схемотехнічні рішення, що застосовуються, дозволяють встановлювати кілька металодетекторів поруч один з одним, на відстані в 5 см.
Технологія на основі цифрового сигнального процесора (DSP) забезпечує високу чутливість, схибленість, дискримінацію сигналу, підвищує точність виявлення, і загальну надійність металодетектора.
Світлова та звукова індикація
Світлодіодні індикатори проходу та індикатори зон виявлення підвищеної яскравості, видимі навіть при яскравому сонячному світлі Інтуїтивно зрозуміле меню налаштування
Смуга прокручування (слайдер) клавіатури керування — для швидкого налаштування значень, параметрів меню
Вибір мови меню управління з більш ніж 10 мов
Лічильник проходів - чотири налаштування для підрахунку відвідувачів: тільки на вхід, тільки на вихід, віднімання виходу, сума вхід та вихід.
Режим самодіагностики – автоматичний, безперервний.
Функція випадкової тривоги (регулюється від 0 до 100 відсотків) Захист від несанкціонованого доступу – три рівні доступу.
Доступ до налаштувань металодетектора захищений 5-значним буквенно-цифровим кодом, який має 60 мільйонів комбінацій.

Ручний металодетектор SuperWand



Модель: SuperWand
Категорія: Техніка для фізичного огляду
Призначення: Металодетектор використовується для виявлення металевих предметів під час огляду людей, багажу тощо.
Дозволяє виявляти чорні та кольорові метали. Завдяки унікальному дизайну котушки має однаково хорошу чутливість під будь-яким кутом до штанги, що сканує. Індикація наявності металу: звукова, вібраційна (дозволяє проводити огляд без привернення уваги оточуючих), світлодіодний індикатор.
Відрізняється підвищеною надійністю та тривалим терміном служби.
Вартість 10780 грн.

Нова технологія Garrett.
Відрізняється круговою діаграмою спрямованості (360 °) та наявністю віброрежиму для потайної роботи.
Ідеально підходить для казино та інших місць, де важливо дотримуватися тиші та не привертати увагу.
Виявляє середнього розміру пістолет з відривом 22 див, великий кишеньковий ніж з відривом до 18 див, шпильку — 2,5 див.

Пристрої постановки перешкод

Пристрої постановки перешкод

- Для захисту приміщень використовуються пристрої постановки перешкод.
- Постановники перешкод різного виду та діапазону є ефективними засобами для захисту переговорів від прослуховування, а також для глушіння радіомікрофонів та зашумлення провідних ліній

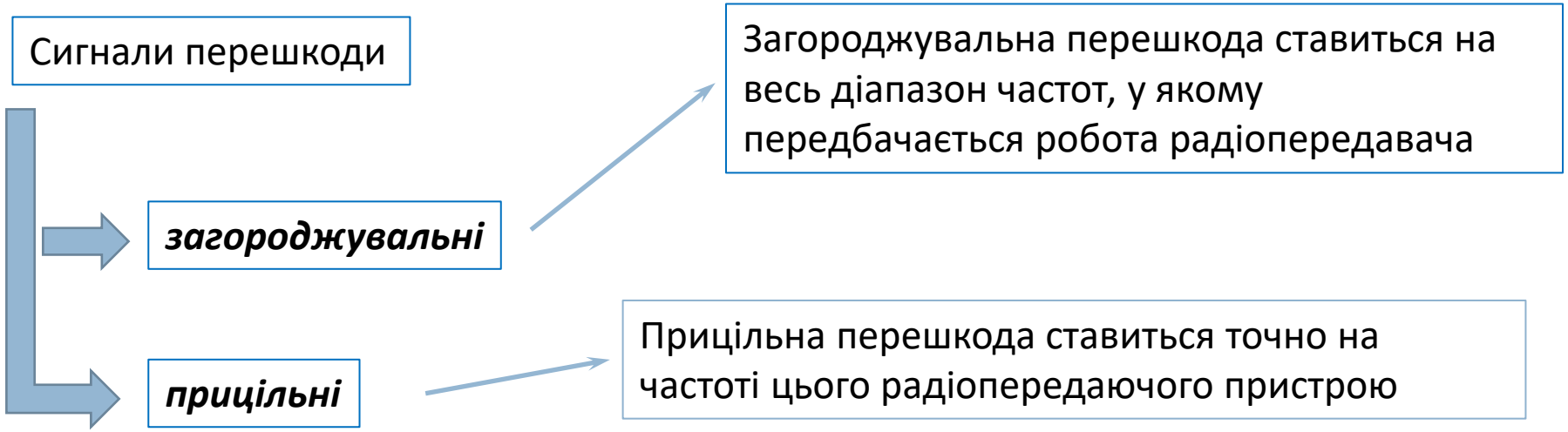
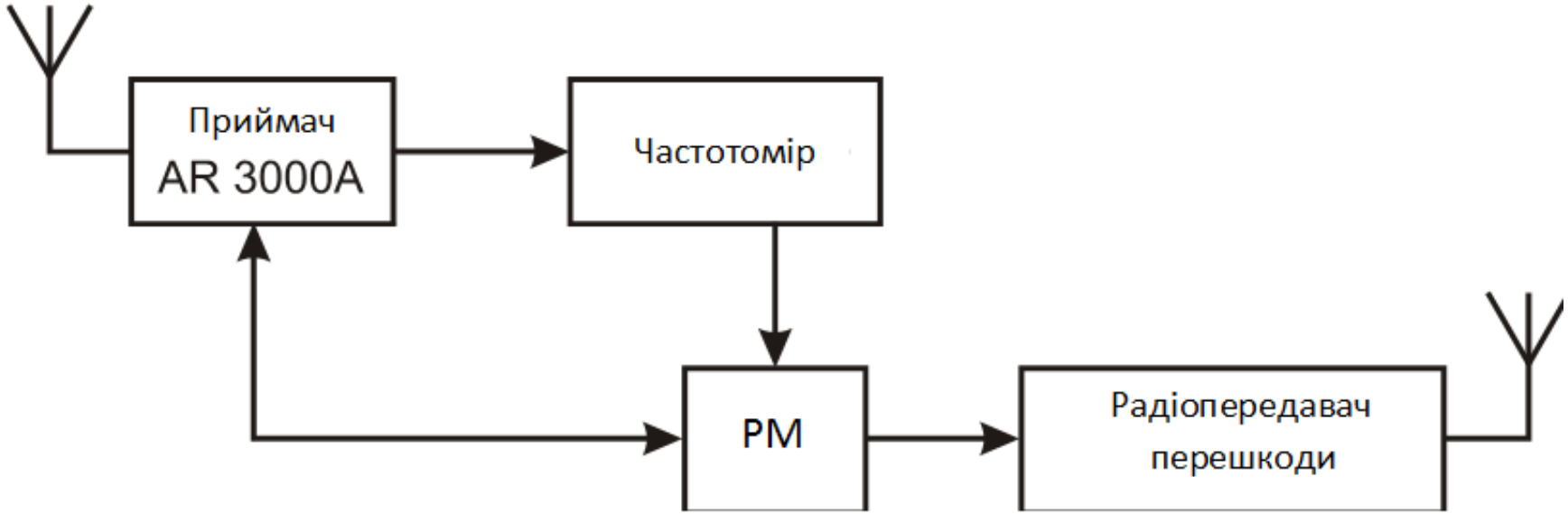


Схема автоматичного комплексу постановки прицільної перешкоди



Апаратура автоматизованого радіомоніторингу

- Апаратура автоматизованого радіомоніторингу (АРМ), призначена для вирішення завдань захисту особливо важливих об'єктів

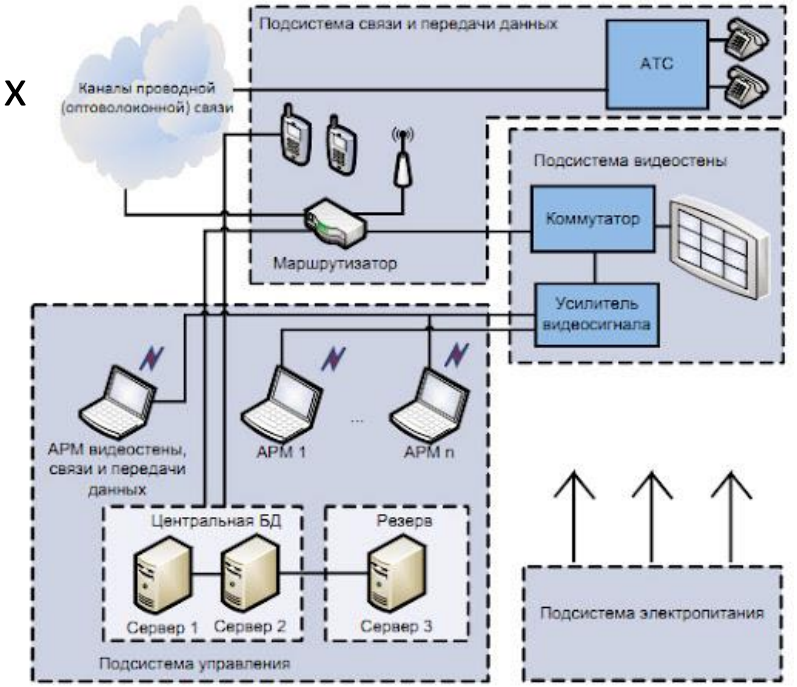
РАДІОМОНІТОРИНГ НА МІСЦЕ

- контроль ефективності заходів щодо запобігання витоку інформації на межах контрольованої зони
- виявлення спеціально організованих та технічних каналів витоку інформації в контрольованих приміщеннях (зонах)
- контроль випромінювань зареєстрованих державними органами засобів зв'язку та радіопередавачів у системах обміну інформацією
- оперативне виявлення випромінювань неліцензованих радіопередавачів, вимірювання їх параметрів та визначення їх розташування
- радіорозвідка та радіоспостереження при проведенні антитерористичних заходів та радіоелектронній протидії

Засоби АРМ

- Основним призначенням засобів АРМ є постійний або періодичний контроль завантаження радіоефіру в широкому діапазоні частот, виявлення та аналіз нових випромінювань, визначення розташування їх джерел, оцінка їх небезпеки чи цінності для користувача, виявлення потенційних або спеціально організованих радіоканалів витоку інформації. Кожне з цих завдань – багатоетапне та вирішується в умовах складної електромагнітної обстановки, вимагаючи для свого вирішення використання широкої номенклатури радіотехнічних засобів.

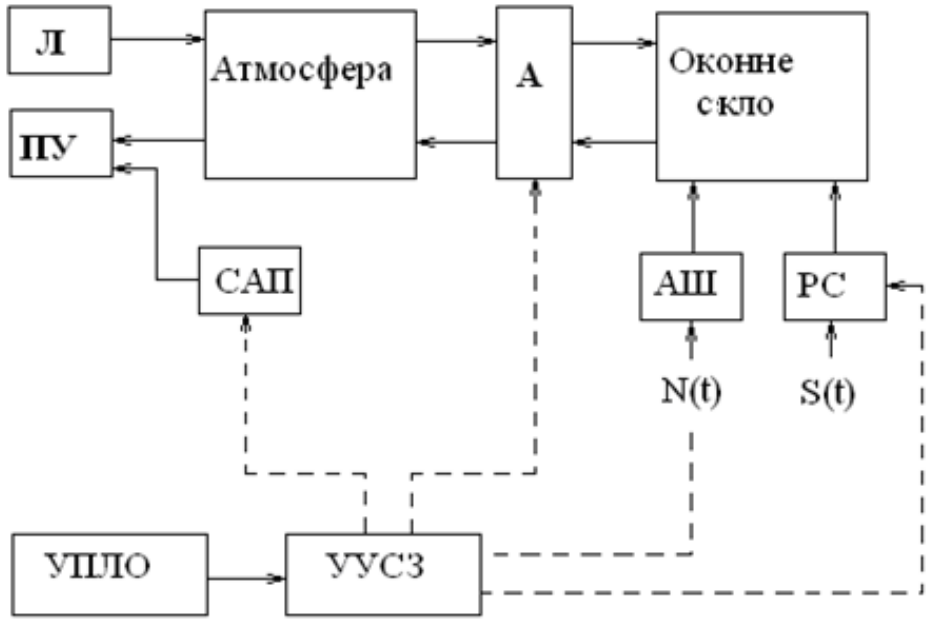




Захист від лазерних систем акустичної розвідки

Протидія активними методами в оптичному діапазоні

- Дистанційні портативні лазерні системи акустичної розвідки (ЛСАР) використовуються для несанкціонованого отримання мовної інформації



Узагальнена структурна схема оптико-акустичного каналу

Л – лазер із оптичною системою управління променем;
ПУ - Прямий пристрій;
А – еквівалентний оптичний атенюатор;
САП - станція активних перешкод в оптичному діапазоні;
АШ – еквівалентний перетворювач акустичного шуму у вібросигнал у точці знімання інформації;
РС – еквівалентний перетворювач мовного сигналу вібросигнал у точці знімання інформації;
УПЛО - пристрій попередження про лазерне опромінення;
УЦСЗ - пристрій управління засобами захисту.

Протидія пасивними методами в оптичному діапазоні$_1$

- Вплив на атмосферу з метою ослаблення лазерного випромінювання у зв'язку зі специфікою умов розташування типових об'єктів ускладнено та не розглядається.
- Видається можливим послабити зондуючий лазерний сигнал шляхом введення спеціальних пластин (А) на шляху його поширення від розташування апаратури розвідки до точки об'єкта розвідки. Очевидно, що пропонована пластина повинна розташовуватися поблизу скла, що захищається.
- З погляду на відбивач-скло (модулятор) необхідно зменшувати коефіцієнт його відображення до мінімально допустимої величини, або змінювати напрямок відбитої хвилі. Зокрема, досліджувалися можливості використання просвітлення шибки з метою зниження коефіцієнта відображення. Розрахунки показали, що таке рішення є ефективним у вузькій спектральній смузі, яка не перекриває весь діапазон лазерних засобів розвідки.

Протидія пасивними методами в оптичному діапазоні$_2$

пасивні методи протидії в акустичному діапазоні



зменшення коефіцієнта передачі еквівалентного перетворювача акустичного мовного сигналу у вібраційний у точці знімання

збільшення коефіцієнта передачі еквівалентного перетворювача акустичних шумів в віброшуми у точці знімання

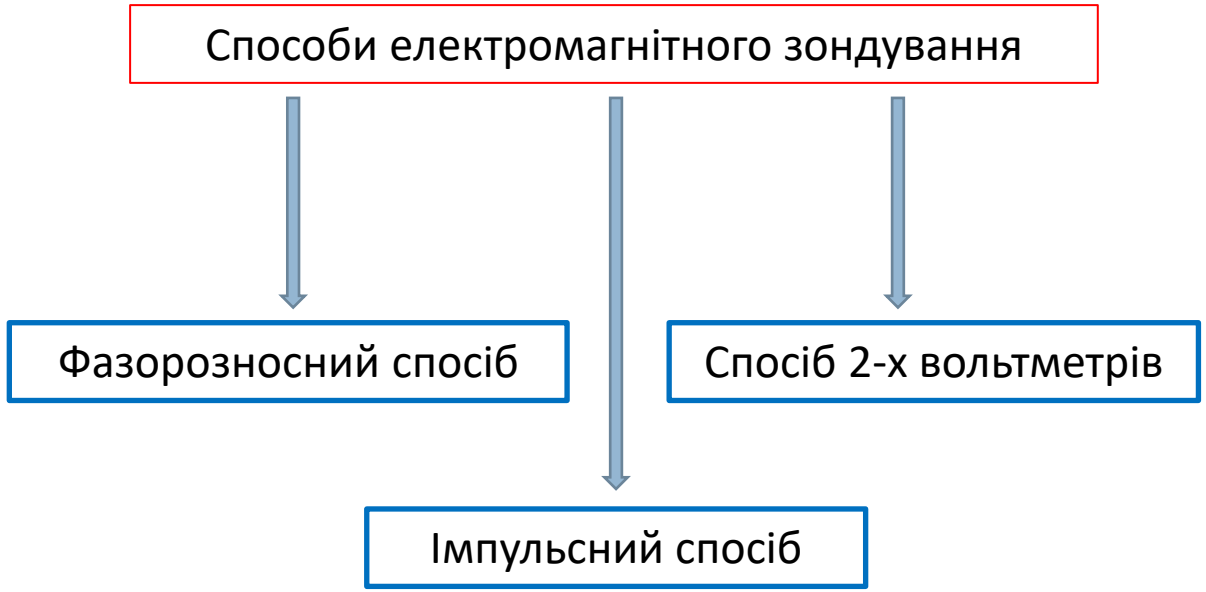
Захист ліній зв'язку$_1$

- Захист лінії зв'язку, що виходять за межі приміщень, що охороняються, або за межі всього об'єкта, є дуже серйозною проблемою, 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 (ТЗ ПІ) має на меті, головним чином, захисту ліній від наведень, створюваних лініями зв'язку в навколишньому просторі. Найбільш економічним способом екранування є групове розміщення інформаційних кабелів в ізольованому коробі, що екранує. Коли такого короба немає, доводиться екранувати окремі лінії зв'язку.

Захист ліній зв'язку$_2$

- Способи зменшення магнітного та електричного зв'язку між проводами дозволяють:
  - зменшити напругу джерела сигналу або струму;
  - зменшити площу петлі;
  - максимально рознести ланцюги;
  - передавати сигнали постійним струмом або на низьких частоти;
  - використовувати провід у магнітному екрані з високою проникністю;
  - увімкнути в ланцюг диференціальний підсилювач.

Захист ліній зв'язку$_3$



Донецький національний технічний університет



Тема 3. Технічні засоби захисту інформації.
Лекція 7. Методи та засоби знищення інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.



Лекційні питання

- Руйнування інформації
- Навмисний силовий вплив
- Комп’ютерні методи руйнування інформації
- Руйнівні програмні засоби

Руйнування інформації

Методи руйнування інформації

Методи руйнування інформації:

- перешкоди;
- апаратні та програмні засоби ПЕОМ - несанкціонований силовий вплив по ланцюгах живлення;
- комп'ютерні віруси та закладки

Перешкодою називається небажана електрична та (або) магнітна дія на систему або її частину, яка може призвести до спотворення збереженої, перетворюваної, переданої або оброблюваної інформації.

Ненавмисні перешкоди природного походження:

космічні та атмосферні перешкоди,
шуми антенних систем,
внутрішні шуми приймачів

Організовані перешкоди

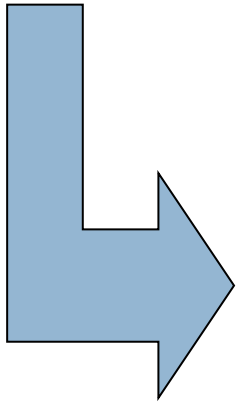
- *Активні* → *що імітують перешкоди*
- *Пасивні* → *маскуючі перешкоди*

Внутрішні перешкоди

- Маскуючі перешкоди створюють шумовий фон, на якому важко виділити корисний сигнал.
- Імітуючі перешкоди є підробкою корисних сигналів.
- За місцем виникнення поділяються на внутрішні та зовнішні.
- Внутрішні перешкоди - шуми, наведення та перешкоди від неузгодження.
  - **Шум** - це флуктуаційний процес, пов'язаний з дискретною природою електричного струму і є послідовністю дуже коротких імпульсів, що з'являються хаотично у великій кількості.
  - **Наведення** — це перешкода, що виникає внаслідок непередбаченої схемою та конструкцією об'єкта, що розглядається, передачі по паразитних зв'язках напруги, струму, заряду або магнітного потоку з джерела перешкоди в розглянуту частину об'єкта.
  - **Перешкоди від неузгодженості** є небажаним перехідним процесом у розглянутому ланцюзі об'єкта, що містить ділянки з розподіленими та зосередженими параметрами, який виникає внаслідок неузгодженості між неоднорідними ділянками.

Зовнішні перешкоди$_1$

Зовнішні перешкоди



- *промислові (індустріальні)*
- *від радіопередавачів*
- *атмосферні*
- *космічні*

Зовнішні перешкоди$_2$

Індустріальні перешкоди

Пристрої, що генерують відносно регулярні електромагнітні коливання, не призначені для випромінювання, такі як медичні високочастотні установки, різного роду промислові агрегати, системи розгортки та ін.

Перешкоди, які випромінюються такими джерелами, як на основній частоті, так і на гармоніках, представляють собою коливання, які наближені до гармонійних.

Пристрої, що не виробляють періодичні електромагнітні коливання.

До них відносяться лінії електропередач, системи запалення двигунів внутрішнього згоряння, високочастотна апаратура для дугового зварювання, газорозрядні пристрої, індукційна і перемикаюча апаратура та ін.

На частотах, що перевищують 30 МГц, які створюються системами пуску зазвичай переважають перешкоди, які створюються іншими системами.

На частотах нижче 30 МГц переважають перешкоди, що породжуються лініями електропередач.

Зовнішні перешкоди$_3$

Індустріальні перешкоди

Провал напруги в мережі живлення змінного струму - це перешкода, протягом дії якої значення амплітуди напруги в мережі в кожному напівперіоді частоти змінного струму стає меншим від регламентованого мінімально допустимого значення.

Перенапруга у мережі живлення змінного струму - це перешкода, протягом дії якої значення амплітуди напруги в мережі в кожному півперіоді частоти змінного струму перевищує регламентоване максимально допустиме значення.

Імпульсні перешкоди

- *Симетричні;*
- *Несиметричні.*

Напруга симетричних перешкод прикладена між фазними проводами мережі живлення.

Напруга несиметричних перешкод між фазним проводом та землею.

Зовнішні перешкоди$_4$

Індустріальні перешкоди

Перешкоди із зовнішніх ліній зв'язку

- *Симетричні імпульсні перешкоди;*
- *несиметричні імпульсні перешкоди;*
- *перешкоди від нееквіпотенційності точок заземлення.*

Напруга симетричної імпульсної перешкоди по лінії зв'язку прикладається між прямим і зворотним проводом лінії зв'язку і називається "поперечною перешкодою"

Напруга несиметричної імпульсної перешкоди по лінії зв'язку прикладається між проводом лінії зв'язку та заземленням і називається "подовжньою перешкодою"

Напруга перешкоди від нееквіпотенційності точок заземлення додається між точками заземлення окремих пристроїв. Якщо зв'язки між пристроями є гальванічними та зворотні дроти зв'язку з'єднані з корпусами пристроїв, то ця напруга виявляється доданою до зворотного дроту зв'язку

Навмисний силовий вплив

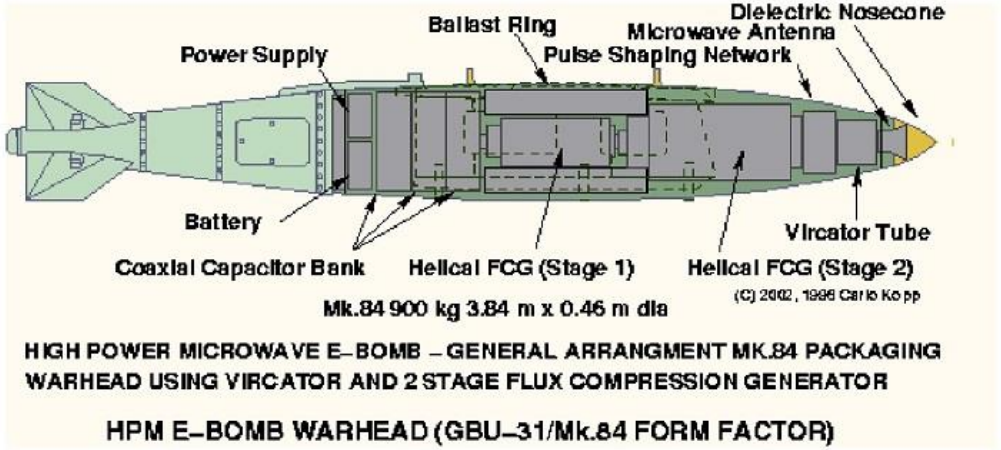
Навмисний силовий вплив

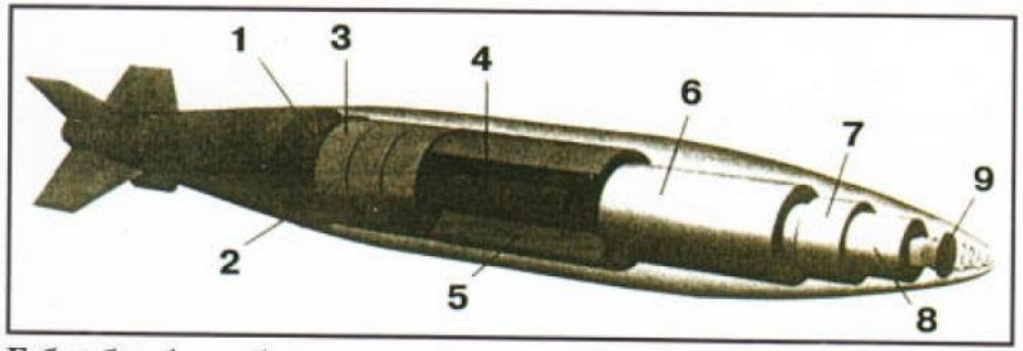
- **Навмисний силовий вплив** – умисне створення різкого сплеску напруги в мережі живлення, по інформаційних провідних лініях або в ефірі з амплітудою, тривалістю та енергією сплеску, які можуть призвести до збоїв у роботі обладнання або до виходу його з ладу.
- **Технічні засоби навмисного силового впливу (ТС НСВ)** є електромагнітною зброєю, яка здатна дистанційно і без зайвого шуму вразити будь-яку систему.
- Істотно підвищує скритність нападу та обставина, що аналіз пошкоджень у знищеному устаткуванні не дозволяє однозначно ідентифікувати причину виникнення пошкодження, оскільки причиною може бути як навмисне (напад), так і ненавмисне (наприклад, індукція від блискавки) силовий вплив. Ця обставина дозволяє зловмиснику успішно використовувати ТЗ НСВ неодноразово.

EMI_1

- **Під зброєю електромагнітного імпульсу (EMI)** розуміють спеціально розроблені й виготовлені неядерні засоби генерування потужного електромагнітного імпульсу або послідовності імпульсів для функціонального ураження озброєння та військової техніки противника, насамперед різноманітних радіоелектронних засобів, що входять до складу його систем управління військами і зброєю.
- На відміну від функціонального подавлення, що здійснюється звичайними засобами та методами радіоелектронної боротьби, при функціональному ураженні елементи РЕЗ противника зазнають необоротних ушкоджень (електричний та (або) тепловий пробій, механічні руйнування тощо), у результаті яких після припинення уражального впливу вони не можуть самостійно повернутися до працездатного стану і потребують ремонту.

EMI_2





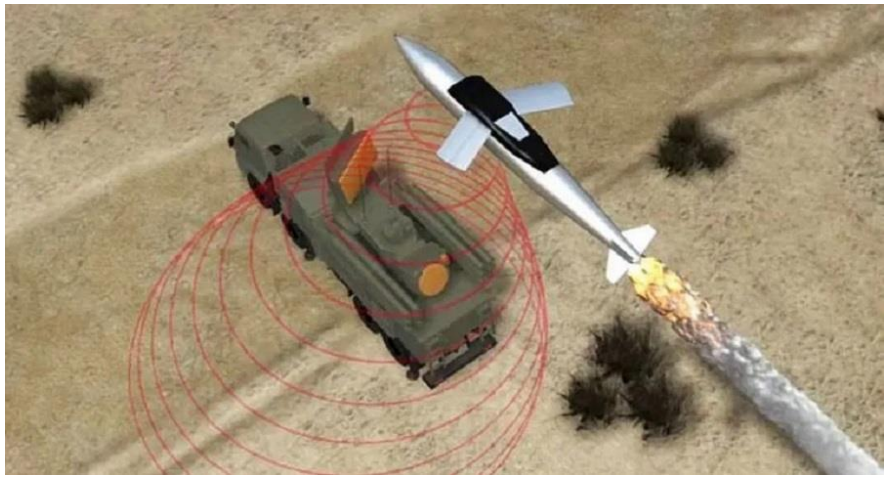
Е-бомба: 1 — блок енергоживлення; 2 — акумулятор; 3 — коаксіальна ємність; 4 — МК-генератор (1 ступінь); 5 — баластний циліндр; 6 — МК-генератор (2 ступінь); 7 — формувач імпульсу напруги; 8 — віркатор; 9 — мікрохвильова антена.



Керована авіабомба з РЧЕМІ.

EMI$_3$

- На думку аналітиків, поряд з традиційними засобами радіоелектронної боротьби, використання зброї EMI для нанесення електронних і комбінованих електронно-вогневих ударів може стати однією з основних форм бойових дій в найближчому майбутньому.
- Більш того, деякі теоретики військової справи вважають, що у перспективі зброя EMI може розглядатися і як силовий, наступальний засіб радіоелектронної та інформаційної боротьби. Основними стратегічними і оперативними завданнями, які можна буде вирішувати за допомогою зброї EMI в такому разі, є такі:
  - стримування агресії;
  - дезорганізація систем управління військами та зброєю противника;
  - зниження ефективності його наступальних повітряних, сухопутних і морських дій;
  - забезпечення панування в повітрі шляхом ураження засобів ППО та РЕБ протиборчої сторони.



EMI_4

- Наприклад у США у 2018 році було прийнято **"Стратегію захисту країни від загроз, пов'язаних з електромагнітними імпульсами та збудженням геомагнітного поля"**. Зазначений документ підготовлено міністерством внутрішньої безпеки (МВБ) США. В стратегії викладаються "чітке бачення і підхід" МВБ "щодо захисту критично важливої інфраструктури" Сполучених Штатів від "потенційно катастрофічних інцидентів з використанням електромагнітного імпульсу", а також принципи реагування на них і відновлення в подібних обставинах.
- Документ розроблений з урахуванням консенсусу, наявного в американських розвідслужбах, щодо тієї небезпеки, яка в зв'язку з застосуванням даного виду озброєнь може виходити від супротивників США.



EMI$_5$

- У 2014 році після початку гібридної агресії РФ проти України Інститут електромагнітних досліджень став ініціатором ідеї по концентрації наявних в Україні сил і можливостей для створення електромагнітного зброї, чим тоді зацікавились і в Міністерстві оборони і в РНБО України. І хоча на сьогодні мало що чутно про постановку на озброєння Збройних сил України конкретних зразків, є всі підстави говорити про те, що наразі Україна, презентована на міжнародному ринку Інститутом електромагнітних досліджень, є потужним світовим постачальником компонентів електромагнітної зброї. Причому, серед десятка країн-замовників електромагнітних «девайсів» розробки та виробництва Інституту більшість відноситься до високорозвинених у технологічному відношенні.

Директор Інституту електромагнітних досліджень (м. Харків) Юрій ТКАЧ з одним з основних серійних продуктів підприємства в руках – портативним вибухомагнітним генератором.

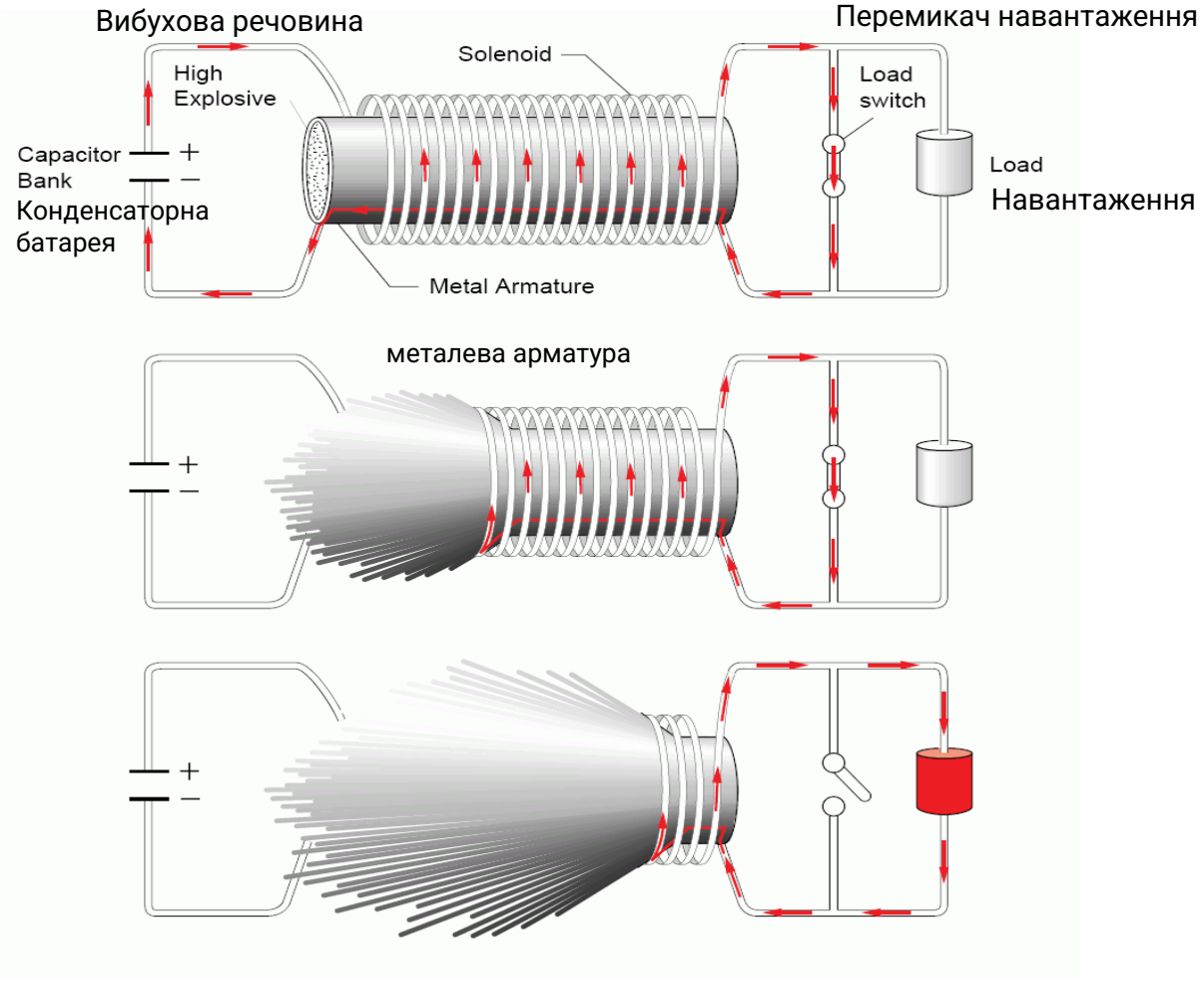


EMI$_6$

- З'явилася інформація, що американські фахівці змогли зробити перші прототипи портативної ручної електромагнітної гранати (Electromagnetic Pulse Grenade або EMP), яка при вибуху генерує потужний імпульс електромагнітного випромінювання і виводить з ладу всі електронні прилади в окрузі. Радіус ураження гранати невідомий. Представники армії США мимохіть згадали EMP, коли говорили про поразку офісної будівлі чи маленького села. Тобто радіус становить від кількох десятків до сотні метрів.



EMI$_7$

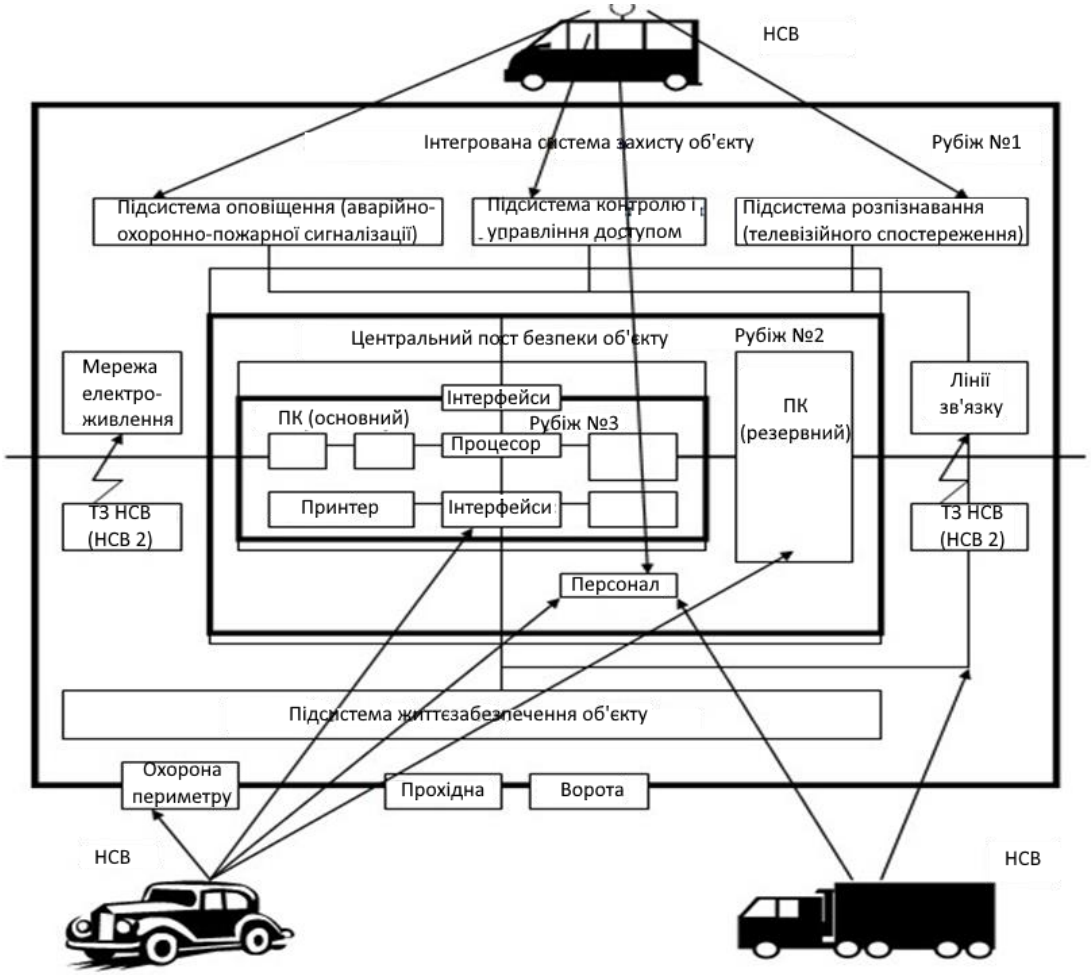


Принцип дії EMI-гранати

Канали навмисного силового впливу$_1$

- Комп'ютер або будь-яке інше електронне обладнання, а також електронні системи безпеки з урахуванням середовища передачі енергії силового впливу можуть отримати навмисний силовий вплив за трьома основними каналами:
  - за мережею електроживлення;
  - за комунікаційними мережами та каналами;
  - за ефіром з використанням потужних коротких електромагнітних імпульсів.

Канали навмисного силового впливу$_2$



Основні канали силового впливу на систему безпеки та рубежі захисту

Навмисна силова дія на мережі живлення

- Під навмисним силовим впливом (НСВ) на мережі живлення розуміється навмисне створення різкого виплеску напруги в мережі живлення з амплітудою, тривалістю та енергією сплеску, які можуть призвести до збоїв у роботі обладнання або до виходу його з ладу.
- Для НСВ використовують спеціальні технічні засоби (ТЗ), які підключаються до мережі безпосередньо за допомогою гальванічного зв'язку через конденсатор або трансформатор.
- НСВ може бути використано для попереднього виведення з ладу сигналізації перед нападом на об'єкт або для провокування помилкових спрацьовувань сигналізації без проникнення на об'єкт.

Технічні засоби для НСВ через мережу живлення



Способи підключення до мережі живлення

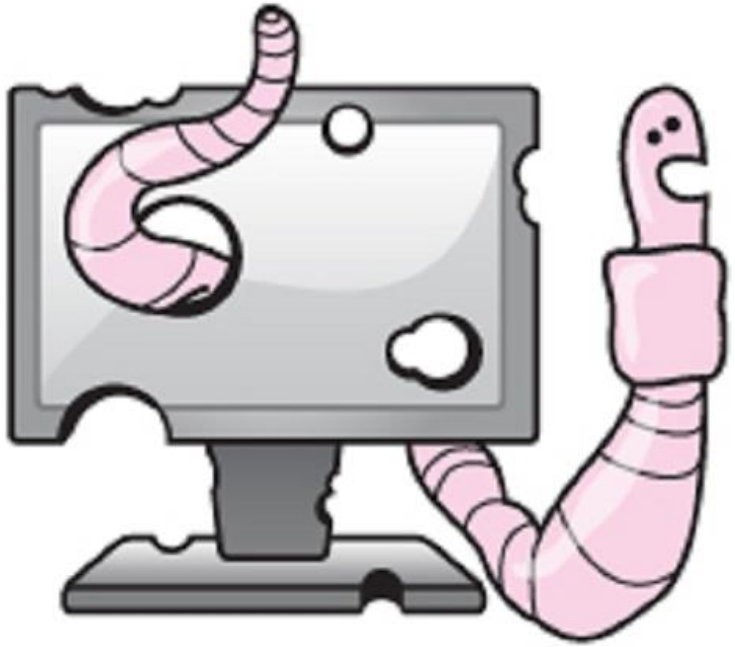
Послідовний (частіше трансформаторний) спосіб вимагає більш серйозного втручання в мережу живлення для підключення обмотки трансформатора в розрив ланцюга. При цьому через другу обмотку трансформатора проходить повний струм споживача, тому ТЗ НСВ має великі розміри і масу, а при більшій потужності, що споживається об'єктом атаки, для підключення ТЗ НСВ необхідні кабелі більшого перетину. Ефективність подібних ТЗ НСВ досягається за рахунок того, що енергія НСВ передається безпосередньо на один об'єкт атаки і не поширюється на всю мережу живлення.

Паралельний спосіб підключення не вимагає втручання в мережу живлення (достатньо вставити стандартну вилку в розетку). Такі ТЗ компактні і не мають демаскуючого кабелю великого перерізу. Але в цьому випадку технічно складніше організувати передачу в мережу живлення довгих імпульсів, найнебезпечніших для ПЕОМ із імпульсним ВДЖ. Крім того, енергія НСВ поширюється на всю мережу електроживлення, а не лише на об'єкт атаки. Ця обставина вимагає накопичувачів енергії ТЗ суттєвого обсягу та знижує дієвість атаки.

Комп’ютерні методи руйнування інформації

Комп’ютерний вірус

Комп'ютерним вірусом називається програма, яка може “заражати” інші програми, включаючи до них свою (можливо, модифіковану) копію. Ця копія, у свою чергу, здатна до подальшого розмноження. Отже, заражаючи програми, віруси здатні поширюватись від однієї програми до іншої. Заражені програми (або їх копії) можуть передаватись через носії інформації або мережі на інші ЕОМ.





Процес зараження

1. Код зараженої програми змінено таким чином, щоб вірус отримував управління першим, до початку роботи програми-носія;
2. При отриманні управління вірус знаходить на диску якусь не заражену програму і вставляє власну копію на початок (або на кінець) цієї програми. Можливі випадки, коли вірус включає себе всередину програми;
3. Якщо вірус дописується над початок програми, він коригує її код (чи навіть знищує програму) про те, щоб отримати управління першим;
4. Після розмноження (або замість нього в окремих випадках) вірус може виробляти різні руйнівні дії;
5. Після цього управління зазвичай передається програмі-носієві (як правило, вона зберігається вірусом) і вона виконує свої функції, роблячи непомітними для користувача дії вірусу.

Троянський кінь

- Для ефективнішого розмноження вірус при першому отриманні управління стає **резидентним**, тобто постійно присутній в оперативній пам'яті під час роботи комп'ютера і розмножує свої копії, як говорилося раніше, при кожному зверненні користувача до програми для її виконання, копіювання, зміни або перегляду.
- Однією з різновидів вірусів є шкідливі програми типу “Троянський кінь”. До них зазвичай відносять спеціально створені програми, які, потрапляючи до обчислювальних систем (зазвичай під виглядом свідомо корисних програм), починають потай виконувати несанкціоновані дії.



Хробаки

- Ще одним типом вірусів є так звані хробаки, які відтворюються, копіюючи себе в пам'яті одного або декількох комп'ютерів (у випадку мережі), незалежно від наявності інших програм.



Програми-носії вірусів$_1$

- Виконані файли, тобто. файли з розширенням COM, EXE, DLL, OVL і т.п. Так як вірус починає роботу при запуску зараженої програми, особливо небезпечне зараження часто використовуваних програм.
- При зараженні програми багатьма із сучасних вірусів, що використовують особливості формату виконуваних файлів для системи Windows, Довжина програми залишається незмінною. Можливе також поширення вірусу в програмах, написаних мовою програмування високого рівня, якщо вони працюють у середовищі інтерпретатора цієї мови, наприклад VBA (Visual Basic for Application), який вбудовується у такі популярні програми, як Microsoft Word,Microsoft Excel, Microsoft Outlook, Microsoft PowerPoint, CorelDraw, AutoCAD та ін.
- Програми операційної системи та драйвери пристроїв (зазвичай мають розширення SYS,BIN,VXD і т.п.).
- Програма-завантажувач операційної системи, що знаходиться у першому секторі диска. Так як програма-завантажувач невелика, вірус зазвичай розміщує себе в додаткових секторах на диску, які позначає як "погані" (bad).

Програми-носії вірусів$_2$

- Як програми-носії вірусів можуть виступати наступні носії:

Об'єктні файли та бібліотеки (розширення OBJ, LIB, TPU і т.п.). Такі файли та бібліотеки, отримані з ненадійного джерела, можуть містити, крім корисного коду, інтегрований вірус. При використанні заражених бібліотек вірус автоматично потраплятиме у всі програми, що створюються на основі таких бібліотек.

Найбільш поширеною руйнівною дією вірусу є ***знищення інформації*** (програм та даних).

Важче виявити не знищення, а ***зміну вмісту*** файлу. Такі дії вірусу особливо небезпечні, тому що файли можуть бути суттєво спотворені, але помітити це вдається занадто пізно.

Програмне придушення обчислювальних систем

Під програмним придушенням обчислювальних систем розуміється комплекс організаційно-технічних заходів, спрямованих на порушення нормального функціонування обчислювальних систем шляхом створення ним умисних програмних перешкод.

Весь процес **програмного придушення обчислювальних систем** розглядається як програма високого рівня, в якій задіяні апаратні та програмні засоби, оператори.

Об'єкти програмного придушення

- Глобальні та локальні обчислювальні мережі
- Обчислювальні центри
- Інформаційно-керуючі системи
- Окремі ЕОМ
- Мікропроцесорні пристрої

Слабкі сторони обчислювальних систем

Слабкі сторони обчислювальних систем:

- відкритість обчислювальних систем як для корисних зовнішніх впливів, так і навмисних програмних перешкод;
- недосконаліть організаційно-технічних та логічних структур обчислювальних систем;
- недосконаліть захисту обчислювальних систем від програмного придушення;
- наявність суттєвих витрат на усунення наслідків впливу програмного придушення на обчислювальних систем;
- можливість тривалого зберігання програмного придушення у пам'яті обчислювальних систем;
- Можливість розмноження програмного придушення в обчислювальних систем та реалізації ними різних деструктивних функцій та ін.

Операції програмного придушення обчислювальних систем

- Основні операції наступні:
  - добування інформації про пригнічувану ОС;
  - обробка отриманої інформації;
  - прийняття рішення на програмне придушення;
  - формування програмних перешкод;
  - отримання доступу до ресурсів ОС для введення до неї програм перешкод;
  - введення програм перешкод до ОС;
  - безпосередній вплив програм перешкод ОС.

Основні методи програмного придушення ОС

- Основними методами є:
  - метод придушення ОС процедурними програмами перешкодами;
  - метод придушення ОС декларативними програмами перешкодами;
  - вплив програм перешкод на програмне забезпечення ОС;
  - вплив програм перешкод на апаратне забезпечення ОС;
  - вплив програм перешкод на операторів ОС.

Руйнівні програмні засоби

Програмні закладки

- **Програмними закладками** називаються програми, що використовують вірусну технологію потайного впровадження, розповсюдження та активізації.
- Програмні закладки призначені для несанкціонованого потайного отримання інформації.

Класифікація програмних закладок$_1$

- Класифікація програмних закладок за методом та місцем їх впровадження та застосування (тобто за способом доставки до системи):
  - закладки, асоційовані з програмно-апаратним середовищем;
  - закладки, асоційовані з первинними програмами завантаження;
  - закладки, асоційовані із завантаженням драйверів, командного інтерпретатора, мережевих драйверів, тобто із завантаженням операційного середовища;
  - закладки, асоційовані з прикладним програмним забезпеченням загального призначення (вбудовані клавіатурні та екранні драйвери, програми тестування ПЕОМ, утиліти та оболонки).

Класифікація програмних закладок$_2$

- використовувані модулі, що містять тільки код закладки (зазвичай, впроваджені у пакетні файли типу BAT);
- модулі-імітатори, що збігаються з деякими програмами, що вимагають введення конфіденційної інформації (за зовнішнім виглядом);
- закладки, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі тощо);
- закладки, що маскуються під програмні засоби ігрового та розважального призначення (як правило, використовуються для первинного впровадження закладок типу “дослідник”).

Типи закладок

Типи закладок

Резидентна - знаходиться в пам'яті постійно з деякого моменту часу до закінчення сеансу роботи ПЕОМ (вимкнення живлення або перевантаження).
Закладка може бути завантажена в пам'ять при початковому завантаженні ПЕОМ, завантаженні операційного середовища або запуску деякої програми (за традицією називається вірусоносієм), а також запущена окремо.

Нерезидентна - починає роботу з аналогічною події, але закінчують її самостійно після закінчення деякого проміжку часу або деякої події, при цьому вивантажуючи себе з пам'яті цілком.

Донецький національний технічний університет



Тема 3. Технічні засоби захисту інформації.
Лекція 8. Програмні методи захисту інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Засоби захисту інформації
- Програми зовнішнього захисту
- Проблеми регулювання використання ресурсів
- Захист програм
- Програмний захист інформації
- Засоби захисту від комп’ютерних вірусів та їх особливості
- Системи захисту інформації

Засоби захисту інформації

Програмні засоби захисту інформації

Програмні засоби захисту інформації (ПЗЗІ) – спеціальні програми, що входять до складу програмного забезпечення автоматизованих систем для вирішення у них (самостійно або в комплекті з іншими засобами) завдань захисту.



Програмні засоби$_1$

1.**Вбудовані засоби захисту інформації**.

2.**Антивірусна програма (антивірус)** – програма для виявлення комп'ютерних вірусів та лікування інфікованих файлів, а також для профілактики – запобігання зараженню файлів або операційної системи шкідливим кодом.

3.**Спеціалізовані програмні засоби захисту інформації** від несанкціонованого доступу мають в цілому кращі можливості та характеристики, ніж вбудовані засоби. Окрім програм шифрування та криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації.

4. **VPN (Віртуальна приватна мережа)** дозволяє передавати секретну інформацію через мережі, в яких можливе прослуховування трафіку сторонніми людьми. Технології, що використовуються: PPTP, PPPoE, IPSec.

Програмні засоби$_2$

5. **Міжмережеві екрани (також звані брандмауерами або файрволами)**. Між локальною і глобальною мережами створюються спеціальні проміжні сервери, які перевіряють і фільтрують весь трафік мережного/транспортного рівнів, що проходить через них. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні до корпоративних мереж, але не усуває цю небезпеку повністю. Більш захищений різновид методу - це спосіб маскараду (masquerading), коли весь трафік, що виходить з локальної мережі, посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

6. **Proxy-servers (proxy - довіреність, довірена особа)**. Весь трафік мережного/транспортного рівнів між локальною та глобальною мережами забороняється повністю – маршрутизація як така відсутня, а звернення з локальної мережі до глобальної відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі до локальної стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях, наприклад, на рівні програми (віруси, код Java та JavaScript).

Засоби програмного захисту$_1$



Засоби програмного захисту$_2$

- Засоби власного захисту (елементи захисту, які притаманні самому програмному забезпеченню або супроводження його продажу та попереджують незаконні дії).
- Засоби захисту у складі обчислювальної системи (засоби захисту апаратури, дисків і штатних пристроїв. При використанні таких засобів операційне середовище, на відміну від штатного режиму, постійно змінюється, так як виконання програм залежить від певних дій, спеціальних заходів попередження та умов, які гарантують захист).
- Засоби захисту з запитуванням інформації (потребують для своєї роботи вводу додаткової інформації з метою ідентифікації повноважень користувачів) .
- Засоби активного захисту (ініціюються при виникненні особливих обставин: ввід невірного паролю; наведення невірної дати або часу при запуску програми; спробах доступу до інформації без дозволу).
- Засоби пасивного захисту (направлені на попередження, контроль, пошук доказів з метою створення обстановки розкриття спроб несанкціонованого доступу) .

Засоби програмного захисту$_3$



Властивості ПЗЗІ

ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

- **УНІВЕРСАЛЬНІСТЬ** → можливість вирішення програмними засобами захисту інформації великої кількості завдань захисту
- **ГНУЧКІСТЬ**
- **ПРОСТОТА РЕАЛІЗАЦІЇ**
- **НАДІЙНІСТЬ** → висока програмна стійкість при великій тривалості безперервної роботи та задоволення високих вимог та достовірності керуючих впливів за наявності різних дестабілізуючих факторів
- **МОЖЛИВІСТЬ МОДИФІКАЦІЇ**
- **РОЗВИТОК**

Недоліки ПЗЗІ

Недоліки ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

- можливість реалізації лише у тих структурних елементах автоматизованих систем, де є процесор
- необхідність використання часу роботи процесора

⇓

- веде до збільшення часу відгуку на запити і, як наслідок, зменшення ефективності її роботи
- зменшення обсягів оперативної пам'яті (ОП) та пам'яті на зовнішніх запам'ятовуючих пристроях (ПЗЗП)
- можливість випадкової чи навмисної зміни

⇓

- внаслідок чого програми можуть не лише втратити здатність виконувати функції захисту, а й стати додатковими джерелами загрози безпеці
- *ОБМЕЖЕНІСТЬ* через жорстку орієнтацію на архітектуру певних типів ЕОМ (навіть у межах одного класу) — залежність програм від особливостей базової системи вводу/виводу, таблиці векторів переривання тощо.

Побудова ПЗЗІ

Організаційна побудова програмних систем захисту інформації

найбільш характерною є тенденція розробки комплексних програм, що виконують цілий ряд ЗАХИСНИХ ФУНКЦІЙ

- розпізнавання користувачів
- розмежування доступу до масивів даних
- заборона доступу до деяких областей обчислювальних систем тощо.

Переваги та недоліки комплексних програм

ПЕРЕВАГИ КОМПЛЕКСНИХ ПРОГРАМ

кожна з них забезпечує вирішення деякої кількості важливих завдань захисту

НЕДОЛІКИ КОМПЛЕКСНИХ ПРОГРАМ

- *стихійність розвитку програм захисту*
  - не дає гарантій повноти наявних засобів
  - не виключає дублювання одних і тих самих завдань захисту
- *жорстка фіксація у кожному з комплексів програм захисних функцій*
- орієнтація переважної більшості наявних програмних засобів на конкретне середовище застосування (тип ЕОМ та операційне середовище)

Вимоги до формування ПЗЗІ$_1$

ВИМОГИ ДО ФОРМУВАННЯ програмних засобів захисту інформації

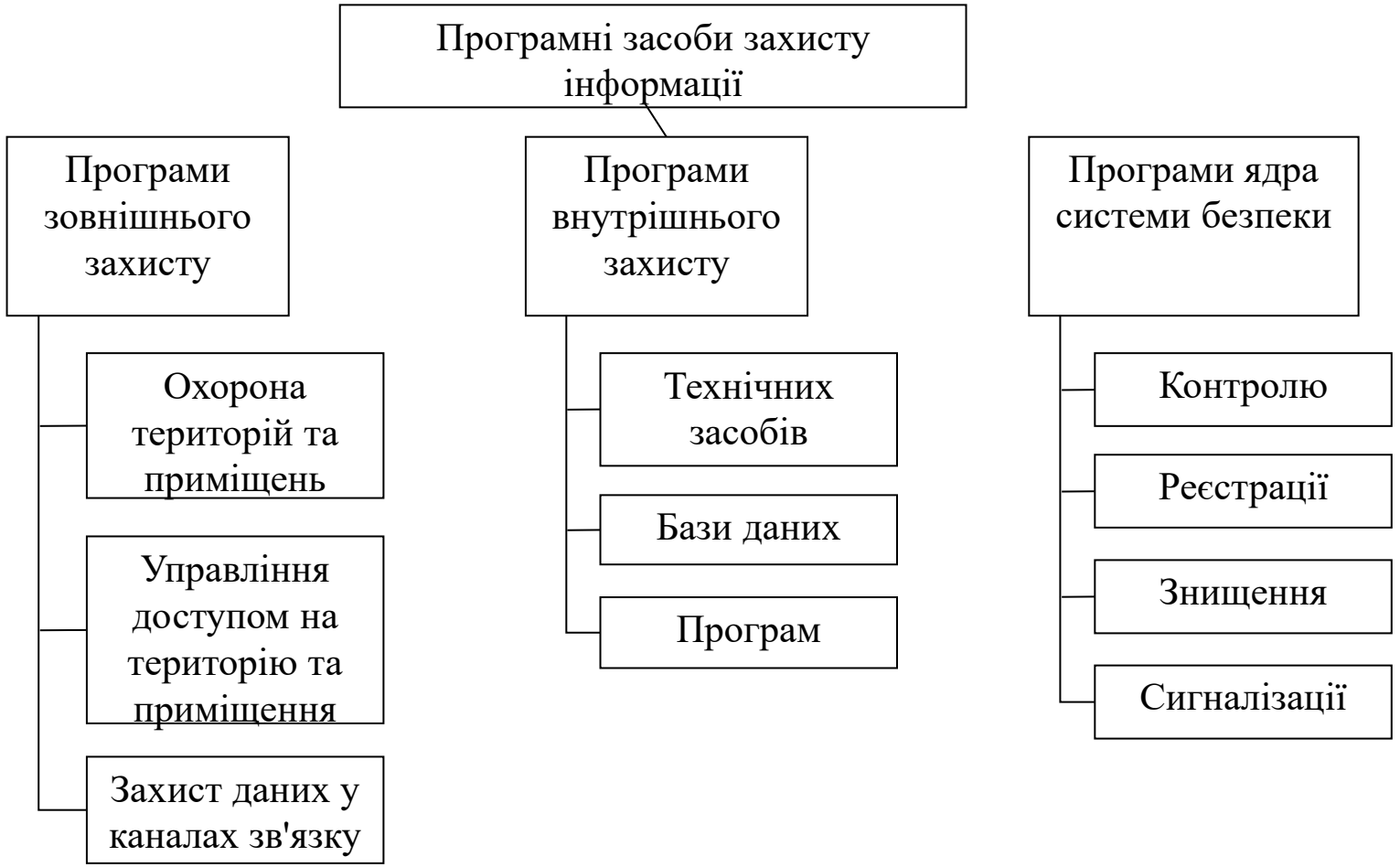
функціональна повнота	гнучкість	уніфікованість використання
повніше охопити всі класи завдань захисту		
	➢ наскрізна модульна побудова; ➢ повна структуризація; ➢ представлення машинно-незалежною мовою	

Вимоги до формування ПЗЗІ$_2$

Принцип *наскрізної модульної побудови* полягає в тому, що кожна з програм будь-якого рівня (об'єму) повинна представлятися у вигляді системи можливих модулів, причому кожен модуль будь-якого рівня повинен бути повністю автономним та мати стандартні вхід та вихід, що забезпечують комплексування з будь-якими іншими модулями. Неважко бачити, що умови можуть бути забезпечені, якщо програмні комплекси розроблятимуться за принципом “згори донизу”, тобто. відповідно до принципу *повної структуризації*.

Подання на машинно-незалежній мові визначає, що представлення програмних модулів має бути таким, щоб їх із мінімальними зусиллями можна було включити до складу програмного забезпечення будь-якої автоматизованої системи. В даний час є алгоритмічні мови високого рівня, що повністю відповідають цим вимогам.

Класифікація ПЗЗІ$_1$



Класифікація ПЗЗІ$_2$

ЗОВНІШНІЙ ЗАХИСТ

сукупність засобів, методів та заходів, спрямованих на захист території, на якій розташовані будівлі обчислювальних центрів, та приміщень, у яких розташовані їх елементи.

ВНУТРІШНІЙ ЗАХИСТ

сукупність засобів, методів та заходів, спрямованих на захист інформації, що обробляється в автоматизованих системах.

ЯДРО СИСТЕМИ БЕЗПЕКИ

програми, що забезпечують захист самої системи захисту інформації

Програми зовнішнього захисту

Програми зовнішнього захисту$_1$

ПРОГРАМИ ЗОВНІШНЬОГО ЗАХИСТУ

- програми захисту території та приміщень;
- програми управління доступом на територію та до приміщень;
- програми захисту даних у каналах зв'язку

ПРОГРАМИ ЗАХИСТУ ДАНИХ У КАНАЛАХ ЗВ'ЯЗКУ

У випадках, коли застосування криптографічних засобів є неможливим або недоцільним, рекомендується використовувати такі програмні методи захисту:

- Впізнання кореспондентів;
- Перевірка рівня таємності каналу зв'язку;
- Контроль за граничними адресами обчислювальних програм;
- Перевірка адреси кореспондента;
- Перевірка зворотного коду

Програми зовнішнього захисту$_2$

РОЗПІЗНАВАННЯ КОРЕСПОНДЕНТІВ

перед видачею даних у канал зв'язку автоматизована система запитує у кореспондента пароль або іншу персональну яка зберігається в таємниці інформацію, порівнює цю інформацію з еталонної, що зберігається в пристрої пам'яті, і видає дані в канал лише у разі збігу пред'явленої та еталонної інформації. Як і будь-яке інше розпізнавання, розпізнавання кореспондентів може бути простим та ускладненим. Вибір способу розпізнавання визначається характером і ступенем секретності пред'явлених даних, а також умовами передачі (протяжність і вид каналу зв'язку, характер території, якою він проходить, і т.п.

ПЕРЕВІРКА РІВНЯ СЕКРЕТНОСТІ КАНАЛУ ЗВ'ЯЗКУ

деякий додатковий засіб захисту і полягає в тому, що кожному каналу зв'язку, використовуваному для передачі інформації, присвоюється певний максимальний рівень секретності, так що передача цього каналу інформації з вищим рівнем секретності не допускається. Перед видачею даних канал автоматизованої системи перевіряє відповідність рівня секретності даних, які підлягають передачі та приймає відповідне рішення. Гриф секретності підготовлених до передачі даних визначається в цьому випадку за максимальним грифом секретності масиву, використаного для формування цих даних.

Програми зовнішнього захисту$_3$

Контроль за граничними адресами обчислювальних програм

для розміщення масиву даних, що передаються в обчислювальній системі виділяється поле, початкова і кінцева адреса якого розміщується в регістрах або в спеціально виділених зонах обчислювальних систем. Перед вибіркою для видачі каналу кожного елемента даних проводиться перевірка адреси вибірки за граничними адресами. Якщо адреса вибірки виходить за межі, видача даних блокується. Цим забезпечується захист від випадкової або навмисної видачі в канал зв'язку даних, що знаходяться на сусідніх полях обчислювальних систем.

ПЕРЕВІРКА ЗВОРОТНОГО КОДУ

є процедурою захисту, що здійснюється в процесі передачі даних. Полягає вона в тому, що у кореспондента періодично запитується ідентифікуюча інформація, яка називається зворотним кодом. Ця інформація порівнюється з еталонною, при розбіжності кодів передача блокується. Перевіркою зворотного коду можна виявити факт зміни (перекомутації) спрямування видачі даних або умисного несанкціонованого використання приймального пристрою зареєстрованого кореспондента.

Програми зовнішнього захисту$_4$

ПЕРЕВІРКА АДРЕСИ КОРЕСПОНДЕНТА

При передачі великого обсягу інформації є принципова можливість випадкової або зловмисної зміни адреси кореспондента, що зберігається в регістрі або спеціально виділеній зоні обчислювальної програми. У цьому випадку дані (після зміни адреси) будуть передаватися на адресу, модифіковану в результаті змін, або задану зловмисником. З метою мінімізації обсягу переданих на хибну адресу даних рекомендується в процесі передачі періодично (через певний інтервал часу та після передачі певного обсягу інформації) перевірити адресу кореспондента. Процедура перевірки є звичайною: адреса кореспондента, що використовується для передачі, порівнюється з еталонним, що зберігається в безпечній зоні програми. При розбіжності порівнюваних адрес передача даних блокується і виробляється відповідний системний сигнал.

Система виявлення вторгнень

Програми внутрішнього захисту здійснюють захист інформації безпосередньо в елементах системи виявлення вторгнень

Регулює використання відповідних ресурсів система виявлення вторгнень (технічних засобів, даних, програм) у суворій відповідності до повноважень, наданих суб'єктам (користувачам) та об'єктам (терміналам, груповим пристроям, програмам). Кожен із видів регулювання зазвичай здійснюється у наступній послідовності.

Спадковість видів регулювання

Спадковість ВИДІВ РЕГУЛЮВАННЯ

НАЙВАЖЛИВІШЕ

1. Встановлення справжності (розпізнавання) суб'єкта чи об'єкта, який звертається до ресурсів системи.

2. Визначення відповідності характеру та змісту запиту повноваженням, пред'явленим запитуючому суб'єкту чи об'єкту.

3. Прийняття та реалізація рішень відповідно до результатів перевірки повноважень

Встановлення справжності

Встановлення справжності

(аутентифікація, ідентифікація, розпізнавання) будь-якого об'єкта або суб'єкта полягає у підтвердженні того, що суб'єкт, що звертався, або пред'явлений об'єкт є саме тим, який повинен брати участь у даному процесі обробки інформації. Основними суб'єктами, справжність яких підлягає встановленню в усіх системах, де обробляється інформація з обмеженим доступом, є користувачі

Контрольне розпізнавання

КОНТРОЛЬНЕ РОЗПІЗНАВАННЯ

розпізнавання видалених терміналів у моменти включення їх у роботу і при зверненні їх до системи під час обробки інформації, що захищається.

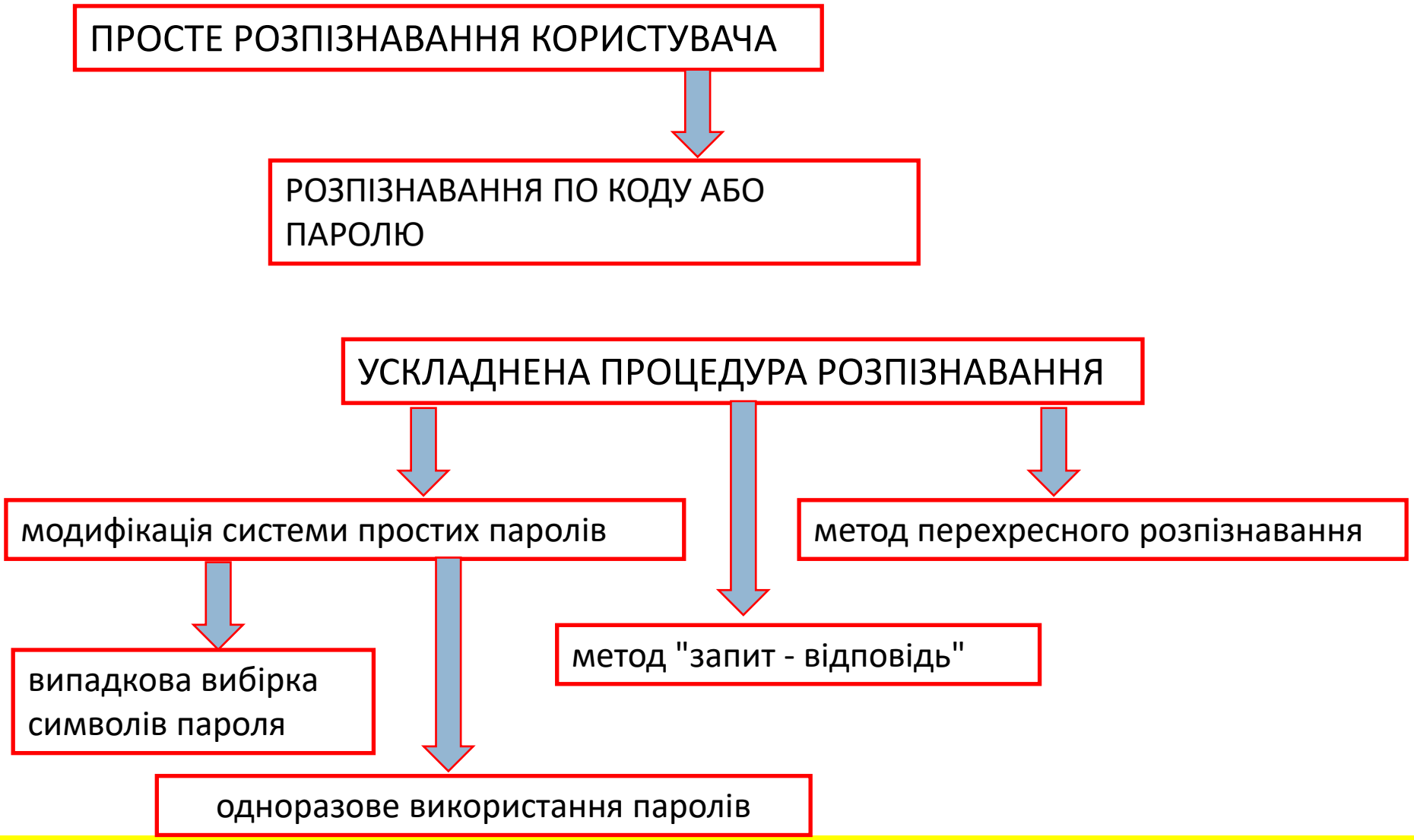
РОЗШИРЕНЕ РОЗПІЗНАВАННЯ

розпізнавання програмістів, віддалених кореспондентів, пристроїв групового управління введенням/виводом, елементів баз даних, що захищаються і т.д.

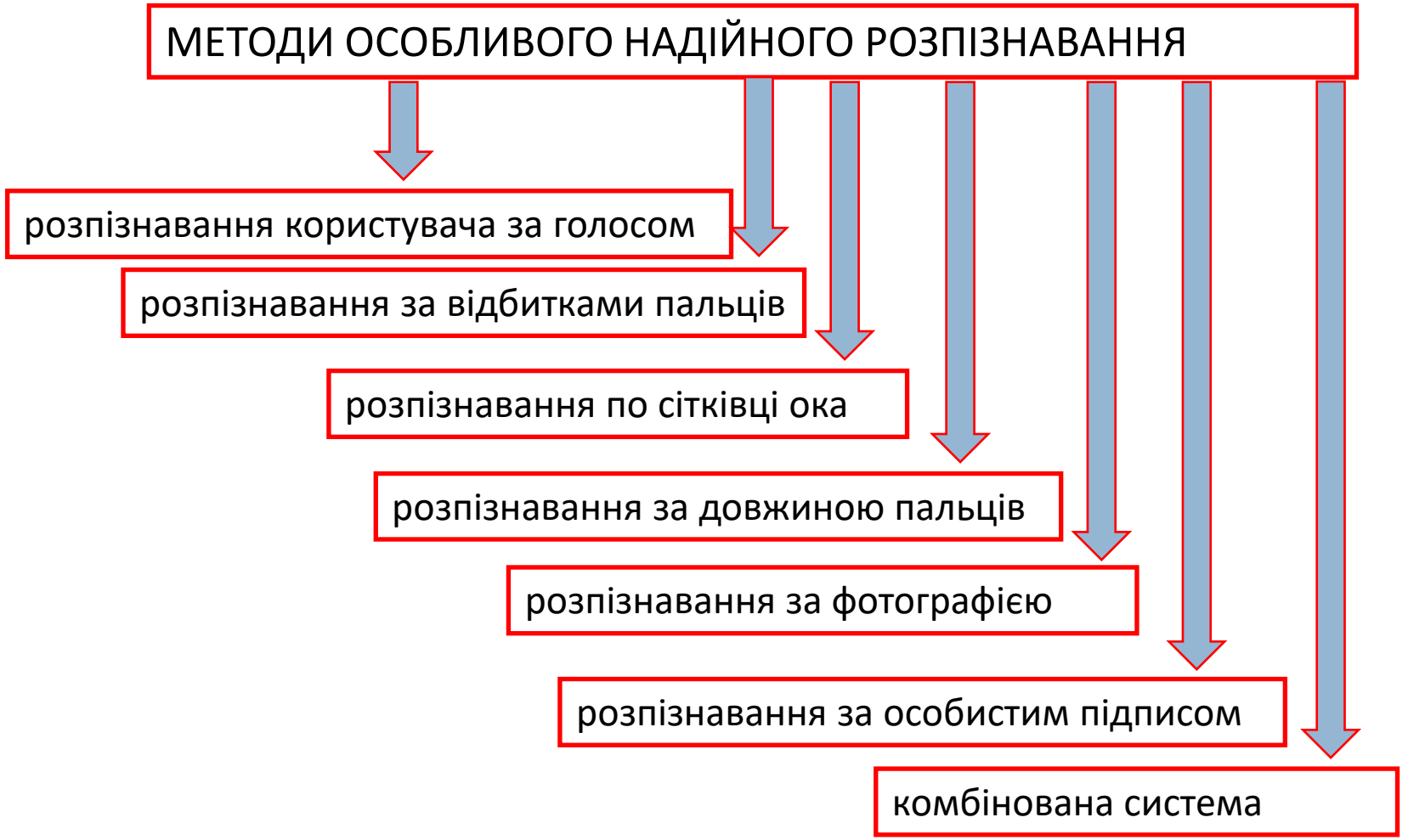
ЗАГАЛЬНЕ РОЗПІЗНАВАННЯ

забезпечується розпізнавання всіх суб'єктів та об'єктів, що мають відношення до обробки інформації, що захищається

Розпізнавання користувача

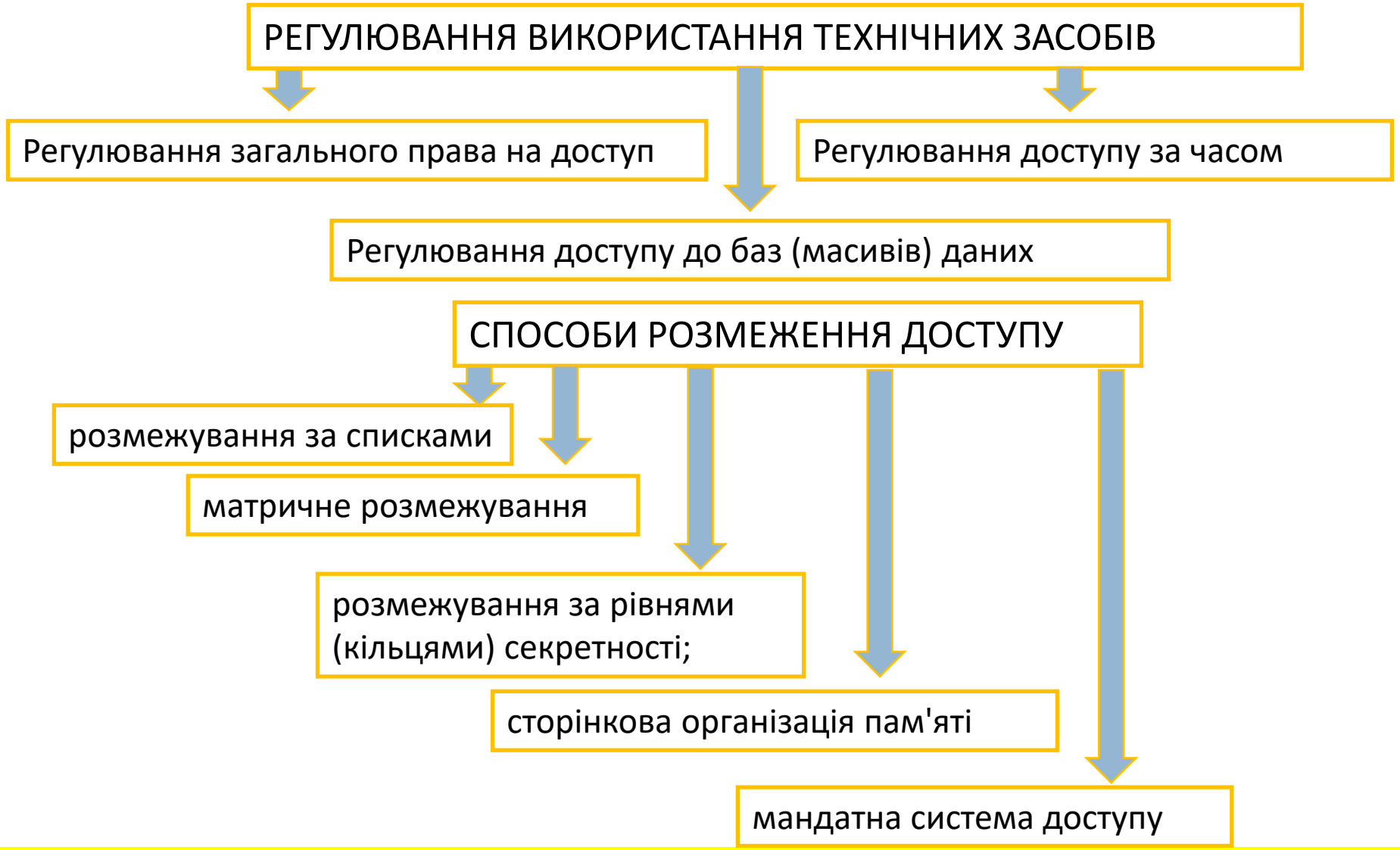


Методи надійного розпізнавання



Проблеми регулювання використання ресурсів

Регулювання використання техзасобів



Розмежування доступу за списками

Розмежування за списками здійснюється у тому випадку, якщо права користувачів на доступ задані у вигляді списків

реалізація послідовності процедури розмежування

- За даними, що містяться в запиті, вибирається відповідний рядок списку: перелік користувачів, допущених до запитуваного елементу або перелік елементів баз даних, до яких користувач, що звернувся із запитом, допущений;
- У вибраному рядку перевіряється наявність імені користувача, який звернувся із запитом, або імені елемента бази даних, до якого звертається користувач;
- За даними перевірки приймається рішення про допуск до даних, що запитуються. Крім того, можуть передбачатися санкції за спробу несанкціонованого доступу, причому як санкції можуть бути вжиті наступні заходи: попередження користувача про те, що їм допущені несанкціоновані дії; відключення користувача від системи повністю або деякий час; подання сигналу контрольним органам про спробу несанкціонованих дій

Матричне розмежування доступу

Матричне розмежування є більш гнучким у порівнянні з розмежуванням за списками, оскільки воно дозволяє не тільки регулювати доступ до даних, а й характер процедур, що виконуються (читання, запис, реконструювання даних і т.д.). Забезпечується це тим, що права користувачів задаються у вигляді матриці, рядками якої представлений список користувачів, а по стовпцях - перелік імен елементів бази даних.

Недоліки методу розмежування за матрицею повноважень

для великих систем з великим обсягом даних матриці повноважень, що захищаються, виявляються громіздкими.

динамічне ведення матриць у процесі функціонування системи є досить складною процедурою

Доступ за рівнями секретності

Розмежування доступу за рівнями (кільцями) секретності полягає в тому, що бази (масиви) даних, що захищаються, діляться на частини відповідно до рівня їх секретності. Повноваження кожного користувача задаються максимальним рівнем секретності даних, доступ до яких дозволено. Відповідно до цього користувачеві дозволяється доступ до всіх даних, рівень секретності яких не вищий за рівень його повноважень

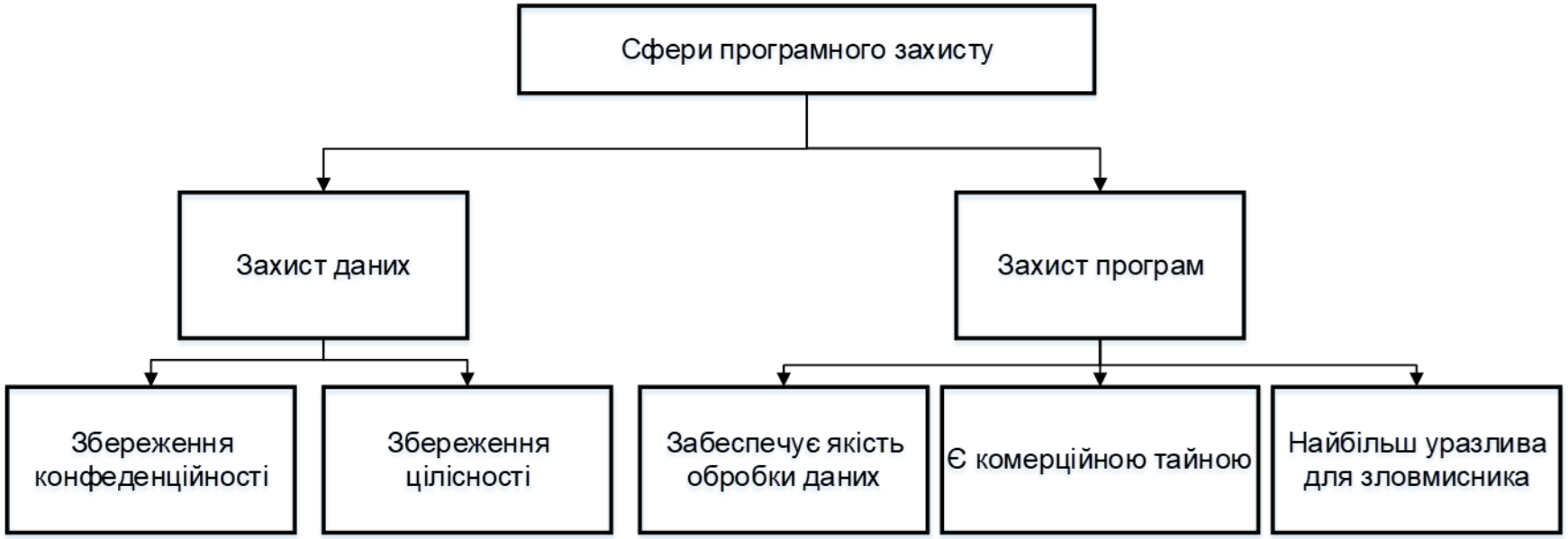
Сторінка організація пам'яті полягає у розділенні обсягу оперативної пам'яті автоматизованої системи на блоки (сторінки) фіксованого розміру. При цьому засобами операційної системи організовується управління використанням сторінок програмами користувача. Будь-яка спроба несанкціонованого входження в поле сторінки викликатиме переривання

Мандатна система доступу

Мандатна система доступу або доступ до пропусків полягає в тому, що користувачеві видається мандат (перепустка) на доступ до відповідних масивів даних або сегментів пам'яті. При кожному зверненні здійснюється перевірка мандата. Сама процедура розмежування є досить простою: мандат, що пред'являється, порівнюється з еталонним і за результатами порівняння приймається рішення про допуск. Однак при цьому виникають ті ж труднощі, що й при роботі з паролями можливі перехоплення, розгадування мандатів тощо

Захист програм

Сфери програмного захисту



Заходи із захисту програм

Необхідність захисту програм обумовлена тим, що вони можуть бути каналом несанкціонованого доступу до інформації. Можливості використання програм для несанкціонованого доступу до інформації можуть бути наслідком як недосконалості програм, так і умисних їх змін

ЗАХОДИ ІЗ ЗАХИСТУ ПРОГРАМ

- точне та однозначне визначення для кожної програми переліку санкціонованих функцій;
- використання засобів та технології програмування, що мінімізують ймовірність наявності додаткових функціональних можливостей, які можуть бути використані для несанкціонованих дій;
- попередження внесення несанкціонованих змін у програмі як у процесі їх розробки, і на етапі експлуатації;
- попередження несанкціонованого використання програм у процесі функціонування системи

Заходи для перекриття каналів

Заходи для перекриття каналів зловмисних процесів над загальносистемними програмними компонентами

1. Періодична перевірка програм за контрольними сумами, причому підвищення надійності перевірок рекомендується проводити як загальне (всього програмного комплексу) контрольне підсумовування, і фрагментарне (окремих блоків, окремих рядків, по заданому маршруту). У цьому спосіб отримання контрольної суми рекомендується зберегти таємно;
2. Перезавантаження, тобто. періодичне оновлення раніше завантажених в оперативну пам’ять програм (або найбільш відповідальних їх компонентів), причому команди на оновлення програм повинні піддаватися керуючої програмою, що особливо захищається;
3. Організація спеціальних точок входу, тобто. декількох нестандартних (збережених у таємниці та періодично змінюваних) адресів звернення до програм та їх окремих блоків;
4. Дублювання програм з обов'язковим порівняння перед виконанням, хоча б двох копій програм, що захищаються;
5. Криптографічне закриття програм, причому зняття шифру має здійснюватися безпосередньо перед використанням

Захист від копіювання$_1$

Система захисту від копіювання або система захисту авторських прав - це комплекс програмних або програмно-апаратних рішень, що забезпечують утруднення або заборону нелегального визначення, використання та (або) зміни програмних продуктів.

Вимоги для підвищення надійності системи захисту від копіювання

Некопіюваність дисків (якщо це необхідно за умовами поширення) автоматичними копіювальниками. Цей пункт гарантує, що для розуміння принципу некопіювання необхідно буде ручне вивчення структури диска.

Неможливість застосування стандартних налагоджувальних засобів щодо ними логіки роботи захищених програм без додаткових маніпуляцій із кодом програми або без плати апаратного налагодження. В даному випадку непрофесіонал або програміст середньої кваліфікації, швидше за все, не зможе "пройти" захищену програму відладчиком.

Захист від копіювання$_2$

- Захист інформації від копіювання реалізується виконанням ряду функцій, які є спільними для всіх систем захисту:
  - ідентифікація середовища, з якого запускатиметься програма;
  - автентифікація середовища, з якого запущено програму;
  - реакція на запуск із несанкціонованого середовища;
  - реєстрація санкціонованого доступу;
  - протидія до вивчення алгоритмів роботи системи.

- Реакція на запуск із несанкціонованого середовища зводиться до видачі повідомлень. Одним із завдань забезпечення безпеки інформації для всіх випадків користування ЕОМ є захист інформації від руйнування, що може статися під час підготовки та здійснення будь-яких відновлювальних заходів.

Програми ядра безпеки системи$_1$

ЯДРО СИСТЕМИ БЕЗПЕКИ

↓

ОРГАНІЗАЦІЯ УПРАВЛІННЯ

↓

засоби, методи, заходи, що використовуються в автоматизованих системах для захисту інформації

Програми ядра безпеки системи$_2$

ФУНКЦІЇ КОМПЛЕКСУ ЯДРА СИСТЕМИ БЕЗПЕКИ

- завантаження програм захисту;
- встановлення та контроль встановлення регістрів межі зон пам'яті;
- контроль своєчасності та надійності, знищення залишкової інформації, тобто. даних, що містяться на полях пристроїв пам'яті після виконання завдання;
- перевірка умов дозволу;
- перевірка розподілу та використання паролів та кодів;
- включення терміналів користувачів до працюючих і виключення їх із цього числа після завершення роботи або після виявлення несанкціонованої діяльності;
- створення та ведення масивів даних та повноважень користувачів;
- поточний контроль використання даних про повноваження користувачів

Програми контролю

Призначення програми контролю полягає в контролі стану основних компонентів механізму захисту, дотримання правил використання даних, що захищаються, і дотримання правил використання механізму захисту

Контроль стану компонентів механізму захисту полягає у перевірці їх справності та здатності виконувати свої функції

Реєстрація-сукупність засобів і методів, що використовуються для регулярного збору, фіксації, обробки видачі відомостей про всі запити, що містять звернення до даних, що захищаються

Аварійне знищення інформації – таке її знищення, яке здійснюється за спеціальними командами у тих випадках, коли виявляється невідворотна небезпека несанкціонованого доступу. Здійснюється воно програмними засобами шляхом надсилання у відповідні області пам'яті комбінацій нулів та одиниць

Програми сигналізації призначені, з одного боку, для попередження користувачів про необхідність дотримуватись обережності при роботі з секретними даними, а, з іншого, — для своєчасного попередження фахівців служби безпеки, адміністрації та користувачів автоматизованих систем про несанкціоновані дії

Метод визначення факту інформаційного втручання

Система виявлення вторгнень - програмний або апаратний засіб, призначений для виявлення фактів неавторизованого доступу до комп'ютерної системи або мережі або несанкціонованого управління ними в основному через Інтернет. Відповідний англійський термін – Intrusion Detection System (IDS). Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем

Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активної діяльності, що може порушити безпеку комп'ютерної системи

Типи шкідливої активності

ТИПИ ШКІДЛИВОЙ АКТИВНОСТІ

- мережеві атаки проти вразливих сервісів;
- атаки, спрямовані на підвищення привілеїв; неавторизований доступ до важливих файлів;
- дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів та хробаків)

Системи виявлення втручань

ПАСИВНА СИСТЕМА ЗНАХОДЖЕННЯ ВТРУЧАНЬ

при виявленні порушення безпеки інформація про порушення записується в лог-додатки (програми), а також сигнали небезпеки відправляються на консоль та/або адміністратору системи по певному каналу зв'язку

АКТИВНА СИСТЕМА ЗНАХОДЖЕННЯ ВТРУЧАНЬ (Система запобігання вторгненням (ips - intrusion prevention system)

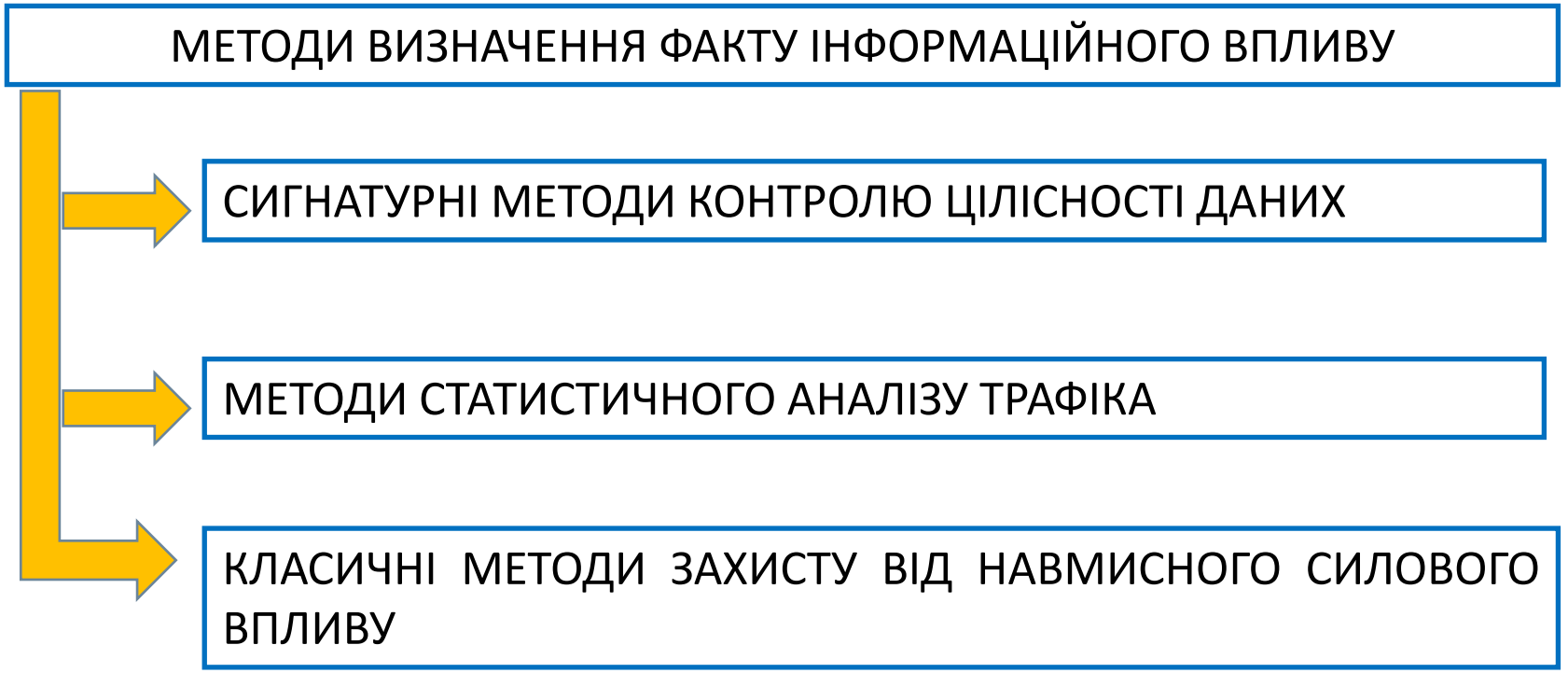
веде дії у відповідь на порушення, скидаючи з'єднання або переналаштовуючи міжмережевий екран для блокування трафіку від зловмисника. Події у відповідь можуть проводитися автоматично або за командою оператора

Архітектура системи виявлення вторгнень

АРХІТЕКТУРА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

- сенсорна підсистема, призначена для збору подій, пов'язаних з безпекою системи, що захищається
- підсистема аналізу, призначену для виявлення атак та підозрілих дій на основі даних сенсорів
- сховище, що забезпечує накопичення первинних подій та результатів аналізу
- консоль управління, що дозволяє конфігурувати система виявлення вторгнень, спостерігати за станом системи, що захищається, та система виявлення вторгнень, переглядати виявлені підсистемою аналізу інциденти

Методи визначення факту інформаційного впливу



Базові принципи методу

БАЗОВІ ПРИНЦИПИ МЕТОДУ

- Кожна копія алгоритму детектування є унікальною. Для захисту множини різних рядків необхідно кілька різних алгоритмів. Ідея полягає в тому, щоб забезпечувати контроль за кожним рядком за допомогою унікальної множини детекторів
- Процес виявлення змін носить імовірнісний характер. Умова використання кількох різних наборів детекторів обумовлюється та імовірнісним характером методу. Так як поодинокі зміни в ланцюжках (рядках) можуть бути ефективно виявлені тільки з використанням безлічі детекторів
- Стійка система повинна забезпечувати із заданою часткою ймовірності будь-яку несанкціоновану активність щодо зміни інформаційних ланцюжків

Програмний захист інформації

Програмні засоби ЗІ

Програмні засоби захисту інформації

- контроль доступу;
- анти-кейлогери;
- анти-шпигуни (anti-spyware);
- анти-експлуататори (anti-subversion);
- анти-модифікатори (anti-tampering);
- антивіруси;
- шифрування;
- брандмауери (firewall);
- системи виявлення вторгнень;
- системи запобігання вторгненням;
- пісочниця

Захист інформації від НСД$_1$

- Для захисту від чужого вторгнення обов'язково передбачаються певні заходи безпеки.
- Особливі функції, які мають здійснюватися програмними засобами, це:
  - ідентифікація об'єктів та суб'єктів;
  - розмежування (іноді повна ізоляція) доступу до обчислювальної техніки;
  - контроль та реєстрація дій з інформацією та програмами.

- У процедурах ідентифікації використовуються різні методи:
  - прості, складні та одноразові паролі;
  - обмін питаннями та відповідями з адміністратором;
  - засоби аналізу індивідуальних характеристик;
  - ключі, магнітні карти, значки і т.п.
  - спеціальні ідентифікатори чи контрольні суми для апаратури.

Захист інформації від НСД$_2$

- Після ідентифікації захист здійснюється на 3 рівнях:
  - апаратури;
  - програмного забезпечення;
  - даних.

- Захист на рівні апаратури та програмного забезпечення передбачає керування доступом до обчислювальних ресурсів.
- Захист на рівні даних спрямований на захист інформації при зверненні до неї в процесі роботи та на захист інформації при її передачі каналами зв'язку. Засоби реєстрації, як і засоби контролю доступу, належать до ефективних методів захисту від НДД. Однак, якщо засоби контролю доступу призначені для запобігання таким діям, завдання реєстрації – виявити вже скоєні дії.

Захист інформації від НСД$_3$

- Для запобігання несанкціонованому доступу можна зберігати всю конфіденційну інформацію на знімних носіях – магнітних стрічках, магнітооптичних дисках та дискетах.
- Але такий спосіб зберігання має істотні недоліки:
  - знімні носії мають обмежений об'єм, і для зберігання на них великого обсягу секретної інформації потрібно заводити картотеки таких носіїв - що і де записано;
  - необхідність надійного фізичного зберігання таких накопичувачів, наприклад, сейфах;
  - необхідність контролю доступу до цих носіїв – призначення адміністратора, який видаватиме їх під розпис співробітникам, ведення спеціальних журналів обліку тощо;
  - людський фактор – за необхідності частого доступу до такої інформації ці правила зберігання можуть просто порушуватися: диски із секретними даними можуть бути засунуті в ящик робочого столу, а секретна інформація може бути скопійована на жорсткий диск.

Захист інформації від НСД$_4$

- Простішою і надійнішою альтернативою є захист конфіденційної інформації за допомогою шифрування. Існують різні методи забезпечення конфіденційності за допомогою шифрування:
  - архівація з паролем;
  - використання прикладних шифруючих застосунків;
  - криптографічні файлові системи.
- Незручністю їх застосування можна назвати необхідність ручних операцій під час створення архівів.
- Втім, сучасні архіватори позбавлені цього недоліку - з їх допомогою можна легко захистити архів паролем прямо з меню програми. Але основною і більш значущою причиною, через яку не можна розглядати архівування з паролем як серйозний метод, невисокий ступінь захисту даних, що надається.

Захист інформації від НСД$_5$

- Набагато надійніше для шифрування окремих файлів користуватися спеціальними програмами – шифрувальними машинками. Для вилучення файлу з архіву потрібно всього лише пароль, який можна підібрати з допомогою спеціальних утиліт. Для доступу до зашифрованих файлів потрібен як пароль, а й шифр, без володіння якими зловмисник не зможе відкрити ці файли.
- Шифрування файлів дає практично стовідсоткову гарантію їхнього захисту за умови, що користувач не розкидає свої паролі та шифри, а зберігає їх у захищеному місці. Програми шифрування окремих файлів вимагають від користувача особливої уваги.
- Важливо не забувати після роботи з розшифрованим файлом знову його зашифрувати. Інакше, зрозуміло, він буде доступний для перегляду всім, хто отримає фізичний доступ до диска. Але найголовнішим недоліком описаного методу є те, що він не захищає від такої загрози, як можливість простого видалення самого зашифрованного файлу.

Захист інформації від НСД$_6$

- Зазначених вище недоліків позбавлені засоби шифрування інформації, які використовують принцип роботи - програми шифрування "на льоту".
- Такі програми встроюються як проміжна ланка в процес обміну інформацією між жорстким диском та процесором. Програми контролюють цей процес, зашифровуючи або розшифровуючи дані при їх читанні та запису. Перетворення даних відбувається в автоматичному режимі, що дозволяє користувачеві працювати у звичному для нього порядку, не звертаючи увагу на втручання програми.
- НЕДОЛІК
  - Неможливо передбачити точний обсяг конфіденційної інформації, яку потрібно буде шифрувати, тому, як правило, під зашифровані диски відводилось мало місця. Якщо ці секретні дані переставали поміщатися на дисках, приходилось створювати нові логічні диски.

Прозоре шифрування$_1$

- «ПРОЗОРОМУ" шифруванню піддаються не сектори жорстких дисків, а об'єкти, розміщені цих дисках.
- Розрізняють ШИФРУВАННЯ ТОМІВ, ШИФРУВАННЯ ФАЙЛОВИХ СИСТЕМ і ШИФРУВАННЯ ФАЙЛІВ. Закрита інформація зберігається в так званих криптозонах, доступ до яких можна отримати тільки за допомогою самої програми шифрування, природно, знаючи паролі.
- Решта, незашифрована інформація зберігається на тих же дисках як завжди - у відкритому вигляді. Такий підхід до шифрування дозволяє відмовитися від резервування місця на диску під зберігання секретної інформації.

Прозоре шифрування$_2$

- ШИФРУВАННЯ ТОМІВ уможливлює кодування всіх логічних розділів і виявляється зручним та інтуїтивно зрозумілим для застосування кінцевим користувачем, хоча і не надає надійний контроль за доступом до окремих директорій або файлів.
- ШИФРУВАННЯ ФАЙЛІВ оперує рівнем додатків і забезпечує надійне неперервне кодування файлів. Для надання якоїсь прозорості кінцевому файлу користувача програми зазвичай трохи переписуються для підтримки шифру. Цей метод виправданий лише для невеликої кількості файлів, але не зовсім придатний для систем збереження.
- Метод ШИФРУВАННЯ ФАЙЛОВИХ СИСТЕМ позбавлений цього недоліку і надає прозоре шифрування файлів на підставі прав доступу як до файлу, так і до каталогу, використовуючи єдиний ключ.

Прозоре шифрування$_3$

- Наведені вище методи застосовуються, якщо необхідно забезпечення конфіденційності локальної інформації, яка використовується і зберігається на одному ПК, і не застосовні у разі, коли потрібен захист інформації, що передається локальною або глобальною мережею між окремими вузлами, так і між сегментами мережі.
- В цьому у разі застосовна технологія віртуальних приватних мереж (Virtual private network). Можна виділити два можливі способи приховування даних:
  - шифрування інформації, що передається по мережі (технологія IPSec;
  - розподіл трафіку в каналі передачі.
- Другий спосіб залежить від застосування його у локальній чи глобальній мережі. У першому разі це всім відома технологія віртуальних локальних мереж (VLAN), яка використовується для структуризації сучасних локальних мереж.

VPN$_1$

- ЧОТИРИ ОСНОВНІ ВАРІАНТИ ПОБУДОВИ МЕРЕЖІ VPN:
  - **Intranet VPN** – дозволяє об'єднати в єдину захищену мережу декілька розподілених філіалів однієї організації, що взаємодіють відкритими каналами зв'язку.

VPN_2

- **Remote Access VPN** – дозволяє реалізувати захищену взаємодію між сегментом корпоративної мережі (центральним офісом або філією) та одиночним користувачем, який підключається до корпоративних ресурсів з дому (домашній користувач) або через notebook (мобільний користувач).
- Даний варіант відрізняється від першого тим, що віддалений користувач, як правило, не має статичної адреси, і він підключається до ресурсу не через виділений пристрій VPN, а прямо зі свого власного комп'ютера, на якому і встановлюється програмне забезпечення, що реалізує функції VPN.
- Компонент VPN для віддаленого користувача може бути виконаний як у програмному, так і у програмно-апаратному вигляді.
  - В першому випадку програмне забезпечення може бути як вбудованим в операційну систему.
  - У другому випадку для реалізації VPN застосовуються невеликі пристрої класу SOHO (Small Office\Home Office), котрі не вимагають серйозного налаштування і можуть бути використані навіть некваліфікованим персоналом;

VPN_3

- **Client/Server VPN –** забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі.
  - Особливість цього варіанта в тому, що VPN будується між вузлами, що знаходяться, як правило, в одному сегменті мережі, наприклад, між робочою станцією та сервером. Така необхідність дуже часто виникає в тих випадках, як у однієї фізичної мережі необхідно створити кілька логічних мереж.
  - Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, які звертаються до серверів, що у одному фізичному сегменті.

VPN$_4$

- **Extranet VPN –** призначений для тих мереж, до яких підключаються користувачі "з боку" (партнери, замовники, клієнти і т.д.), рівень довіри до яким набагато нижчі, ніж до своїх співробітників. Хоча за статистикою найчастіше саме співробітники є причиною комп'ютерних злочинів та зловживань.

VPN$_5$

- ЗАСОБИ ПОБУДОВИ VPN :
  - у вигляді спеціалізованого програмно-апаратного забезпечення, яке призначене для вирішення завдань VPN.
    - ПЕРЕВАГА таких пристроїв – їх висока продуктивність і вища, проти іншими рішеннями, захищеність.
    - Такі пристрої можуть застосовуватися в тих випадках, коли необхідно забезпечити захищенний доступ великої кількості абонентів.
    - НЕДОЛІК таких рішень у тому, що управляються вони окремо від інших рішень щодо безпеки, що ускладнює завдання адміністрування інфраструктури безпеки. На перше місце ця проблема виходить при побудові великої та територіально-розподіленої мережі, що налічує десятки пристроїв побудови VPN;

VPN$_6$

- у вигляді програмного рішення, що встановлюється на звичайний комп'ютер, функціонуючим, як правило, під керуванням операційної системи Unix.
  - Для прискорення обробки трафіку можуть бути використані спеціальні апаратні прискорювачі, які замінюють функції програмного шифрування.
  - Також у вигляді програмного рішення реалізуються абонентські пункти, призначені для підключення до захищеної мережі мобільних користувачів;

VPN$_7$

- інтегровані рішення, в яких функції побудови VPN реалізуються поряд з функцією фільтрації мережевого трафіку, забезпечення якості обслуговування або розподілу смуги пропускання.
  - ОСНОВНА ПЕРЕВАГА такого рішення – централізоване керування всіма компонентами з єдиної консолі.
  - ДРУГА ПЕРЕВАГА – нижча вартість у розрахунку на кожен компонент порівняно з ситуацією, коли такі компоненти купуються окремо.

Засоби захисту від комп’ютерних вірусів та їх особливості

Технології сканування

- В ДАНИЙ ЧАС ІСНУЄ І АКТИВНО ВИКОРИСТОВУЄТЬСЯ ТРИ ТЕХНОЛОГІЇ СКАНУВАННЯ :
  - **сигнатурний аналіз** – пропонує швидкий спосіб ідентифікації вірусів, але його користь зменшується або стає марною при виявленні нового вірусу;
  - **евристичний аналіз** – полягає у пошуку ознак коду, який може виконувати зловмисні функції. У свою чергу за методом аналізу поділяється на статичний та динамічний евристичний аналіз;
  - **аналіз поведінки програмного забезпечення** – аналізатор інтегрується з операційною системою хоста і спостерігає поведінку різних програм у реальному часі на предмет спроб скоєння підозрілих дій.
- Існуючі системи блокування поведінки можна розділити на дві категорії: системи блокування на основі політики та на основі експертизи.

Детектори

- Для захисту від різноманітних вірусів існує декілька видів антивірусів, які за своїм призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини.

- **Детектори (сканери)** – перевіряють оперативну або зовнішню пам’ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм. Якщо детектор – резидентний, то програма перевіряється і тільки в разі відсутності вірусів вона активується. Детекторами є, наприклад, програма MS AntiVirus.

Фаги, поліфаги

- **Фаги (поліфаги)** – виявляють та знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть проводити евристичний аналіз файлу, досліджуючи його на наявність коду, характерного для вірусу (додання частини однієї програми в іншу, шифрування коду тощо).
- Фагами є, наприклад, програми Aidstest, DrWeb.
- Дуже часто функції детектора та фага суміщені в одній програмі, а вибір режиму роботи здійснюється завданням відповідних параметрів (опцій, ключів). На початку вірусної ери кожний новий вірус визначався та лікувався окремою програмою. При цьому для деяких з вірусів (наприклад, VIENNA) цих програм було не менше десятка. Згодом окремі програми почали виявляти та лікувати декілька типів вірусів, тому їх стали звати полідетекторами та поліфагами відповідно.
- Сучасні антивірусні програми знаходять і знешкоджують багато тисяч різновидів вірусів і заради простоти їх звуть коротко детекторами та фагами. Серед детекторів та фагів найбільш відомими та популярними є програми Aidstest, DrWeb (фірма «ДиалогНаука», Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США).

Ревізори

- **Ревізори** – програми, що контролюють можливі засоби зараження комп’ютера, тобто вони можуть виявити вірус, невідомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів. При створенні будь-яких змін користувачеві видається повідомлення (навіть у разі відсутності вірусів, але наявності змін).
- При першому запуску ревізор утворює таблиці, куди заносить інформацію про вільну пам’ять, Partition Table, Boot-сектор, директорії, файли, що містяться у них, погані кластери тощо. При повторному запуску ревізор сканує пам’ять та диски і видає повідомлення про всі зміни, що відбулися у них з часу останнього сеансу ревізії. Нескладний аналіз цих змін дозволяє надійно визначити факт зараження комп’ютера вірусами.
- Свого часу, коли не було надійних засобів боротьби з вірусами, широкого поширення набули так звані фільтри. Ці антивірусні програми блокують операцію записування на диск і виконують її тільки при вашому дозволі. При цьому легко визначити, чи то ви санкціонували команду на запис, чи то вірус намагається щось заразити. До числа широко відомих свого часу фільтрів можна віднести програми VirBlk, FluShot та ін.

Сторожі, вакцини

- **Сторожі** – резидентні програми, які постійно зберігаються у пам’яті комп’ютера й у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP.

- **Вакцини** – це програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів.

Три рубежі захисту

ІСНУЮТЬ ТРИ РУБЕЖІ ЗАХИСТУ ВІД КОМП’ЮТЕРНИХ ВІРУСІВ:

- Запобігання надходженню вірусів.
- Запобігання вірусній атаці, якщо вірус усе-таки потрапив у комп’ютер.
- Запобігання руйнівним наслідкам, якщо атака відбулася.

Методи реалізації рубіжної оборони

ТРИ МЕТОДИ РЕАЛІЗАЦІЇ РУБІЖНОЇ ОБОРОНИ:

- «Програмні методи захисту».
- Апаратні методи захисту.
- Організаційні методи захисту.

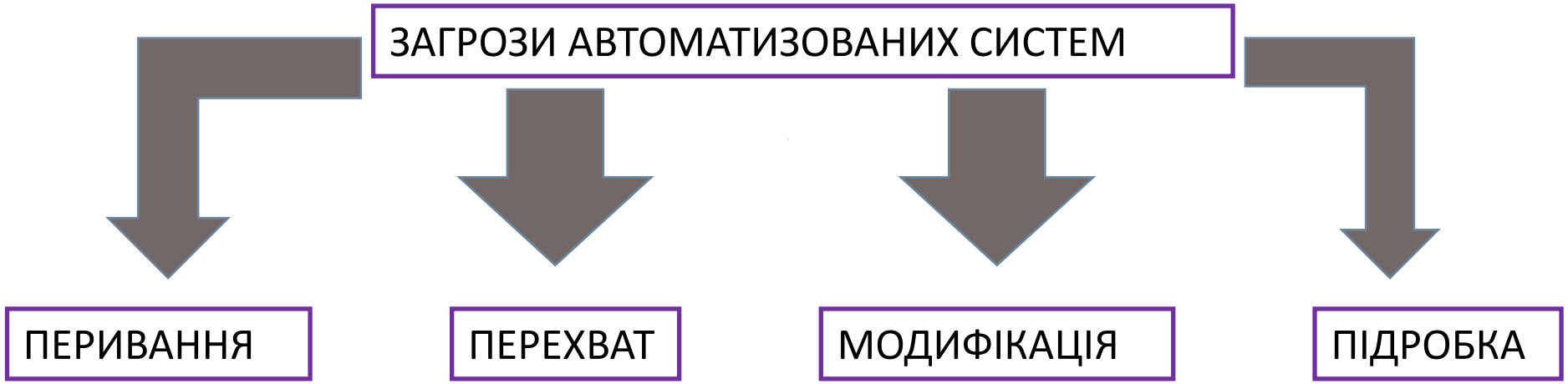
Резервне копіювання

- **Основним засобом захисту інформації є резервне копіювання** найцінніших даних. У разі втрати інформації внаслідок будь-якої з названих вище причин, жорсткий диск треба відформатувати й підготувати до нової експлуатації. На «чистий» диск установлюють операційну систему з дистрибутивного компакт-диска, потім під її керуванням треба встановити все необхідне програмне забезпечення, яке теж беруть з дистрибутивних носіїв. Відновлення комп’ютера завершують відновленням даних, які беруть з резервних носіїв.
- Створюючи план заходів з резервного копіювання інформації, необхідно враховувати, що резервні копії повинні зберігатися окремо від комп’ютера. Тобто, наприклад, резервне копіювання інформації на окремому жорсткому дискові того самого комп'ютера лише створює ілюзію безпеки. Відносно новим і досить надійним методом зберігання даних є зберігання їх на віддалених серверах в Інтернеті. Є служби, які безплатно надають простір для зберігання даних користувача.

Системи захисту інформації

Безпека автоматизованих систем





Види втручань$_1$

При перериванні

- компонент системи втрачається (наприклад, внаслідок викрадення);
- компонент системи стає недоступним (наприклад, внаслідок блокування – фізичного чи логічного);
- компонент системи втрачає працездатність

ПЕРЕХВАТ

- незаконне копіювання програм та даних;
- несанкціоноване читання даних із лінії зв'язку комп'ютерної мережі тощо.

Види втручань$_2$

МОДИФІКАЦІЯ

- отримує доступ до компонента;
- маніпулює компонентом

МОДЕРНІЗАЦІЯ

- додавання фальшивого процесу до системи;
- додавання підробленого запису до файлів системи або інших користувачів

Принципи побудови СЗІ$_1$

ПРОСТОТА МЕХАНІЗМУ ЗАХИСТУ

Цей принцип загальновідомий, але завжди глибоко усвідомлюється. Справді, деякі помилки, які не виявлені при проектуванні та експлуатації, дозволяють виявити невраховані шляхи доступу. Необхідне ретельне тестування програмного забезпечення або апаратних засобів захисту, проте на практиці така перевірка можлива лише для простих та компактних схем.

У НОРМАЛЬНИХ УМОВАХ ДОСТУП ДО МЕХАНІЗМУ ЗАХИСТУ ПОВИНЕН БУТИ ВІДСУТНІМ

Для роботи системи необхідно, щоб виконувались певні умови, за яких доступ до механізму захисту стає неможливим. Помилка визначення повноважень користувача в системі захисту, заснованої на використанні дозволів, призводить до розширення сфери заборон. Цю помилку найлегше виявити і вона не зруйнує загального статусу захисту.

Принципи побудови СЗІ$_2$

ВСІ МОЖЛИВІ КАНАЛИ ВИТОКУ ПОВИННІ БУТИ ПЕРЕКРИТІ

Цей принцип передбачає перевірку повноважень будь-якого звернення до будь-якого об'єкта та є основою системи захисту. При цьому слід враховувати такі режими роботи як: запуск, відновлення після збоїв, вимкнення та профілактичне обслуговування. Необхідно забезпечити надійне визначення джерела будь-якого звернення до даних.

МЕХАНІЗМ ЗАХИСТУ МОЖНА НЕ ЗАСЕКРЕЧУВАТИ

Немає сенсу засекречувати деталі реалізації систем захисту, призначеної для широкого використання. Ефективність захисту не повинна залежати від того, наскільки досвідчені потенційні порушники. Відкритість механізму захисту дозволяє за необхідності зробити його предметом обговорення серед фахівців, не торкаючись інтересів користувачів.

Принципи побудови СЗІ$_3$

Дозвіл повноважень

Цей принцип полягає у застосуванні кількох ключів захисту. Наявність декількох ключів захисту в автоматизованих системах зручна в умовах, коли право на доступ визначається виконанням низки умов.

Мінімальні повноваження

Для будь-якої програми та будь-якого користувача має бути визначено мінімальне коло повноважень, необхідних для виконання дорученої роботи. Внаслідок цього значною мірою зменшується збиток, який завдається при збоях та випадкових порушеннях.

Максимальна обґрунтованість механізму захисту

З метою виключення обміну інформацією між користувачами рекомендується при проектуванні схем захисту мінімізувати кількість загальних для декількох користувачів параметрів і характеристик механізму захисту.

Принципи побудови СЗІ$_4$

Психологічна привабливість

Система захисту має бути простою в експлуатації. Звичайно, чим точніше збігається уявлення користувача про систему захисту з її фактичними можливостями, тим менше помилок виникає у процесі застосування.

При побудові систем виникають серйозні труднощі, пов'язані з великими витратами їх реалізацію. Тому важливим фактором при реалізації систем захисту є їх економічна ефективність. Тому надмірне обтяження системи дорогими засобами захисту може зробити її неконкурентоспроможною

Донецький національний технічний університет



Тема 4. Технічні канали витоку інформації. Лекція 9. Технічні канали витоку інформації. Загальні поняття. Потенційні канали витоку інформації.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Технічні канали просочування інформації. Загальні положення
- Передумови утворення ТКПІ
- Потенційні канали витоку інформації

Технічні канали просочування інформації. Загальні положення

Просочування інформації

- Фізичні явища, що лежать в основі появи випромінювань, мають різний характер, проте, в загальному вигляді просочування інформації за рахунок побічних випромінювань може розглядатися як ненавмисна передача конфіденційної інформації по деякій “побічній системі зв'язку”, що складається:
  - з передавача (джерела випромінювань),
  - середовища, в якому ці випромінювання поширюються,
  - приймаючої сторони.



Технічний канал просочування інформації

- В традиційних систем зв'язку, в яких передаюча і приймаюча сторони, переслідують одну мету, — передати інформацію з найбільшою достовірністю
- При захисті сторона, що “передає” , зацікавлена в можливо більшому погіршенні передачі інформації, оскільки це сприяє її захисту.
- Описану “систему зв'язку” прийнято називати ***технічним каналом просочування інформації***.

Перешкоди

- У реальних умовах в навколишньому просторі присутні багаточисельні перешкоди як природного, так і штучного походження, які істотним чином впливають на можливості прийому.
- Технічні канали просочування інформації найчастіше розглядають в сукупності з джерелами перешкод.
- Для традиційних систем зв'язку такі перешкоди є негативним явищем, що в значній мірі викликають труднощі прийому,
- Для захисту технічних засобів від просочування інформації по побічних каналах ці перешкоди виявляються корисними і нерідко створюються спеціально.

Джерела випромінювань в технічних каналах

- **Джерелами випромінювань в технічних каналах є різноманітні технічні засоби, в яких циркулює інформація з обмеженим доступом.**
- **Такими засобами можуть бути:**
  - **мережі електроживлення і лінії заземлення;**
  - **автоматичні мережі телефонного зв'язку;**
  - **системи телеграфного, телекодового і факсимільного зв'язку;**
  - **засоби гучномовного зв'язку;**
  - **засоби звуко- і відеозапису;**
  - **системи звукопідсилення мови;**
  - **електронно-обчислювальна техніка;**
  - **електронні засоби оргтехніки.**

Типи технічних каналів просочування інформації

- Технічні канали просочування інформації прийнято ділити на типи:
  - **радіоканали** (електромагнітні випромінювання радіодіапазона);
  - **акустичні канали** (поширення звукових коливань в будь-якому звукопровідному матеріалі);
  - **електричні канали** (небезпечна напруга і струми в різних струмопровідних комунікаціях);
  - **оптичні канали** (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектра);
  - **матеріально-речові канали** (папір, фото, магнітні носії, відходи і так далі).

Причини утворення технічних каналів витоку інформації



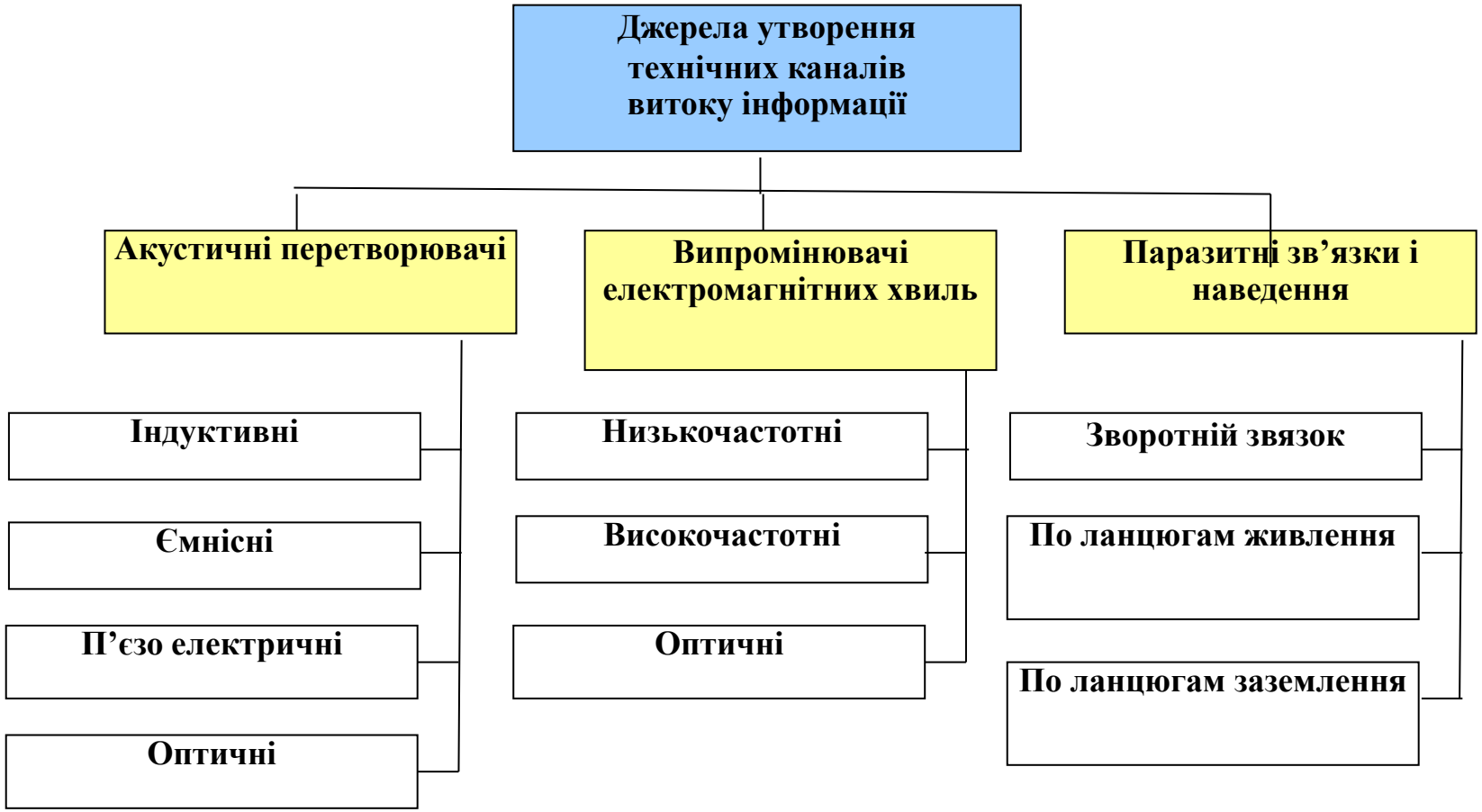
Джерела утворення ТКПІ$_1$

- **Основними *джерелами* утворення технічних каналів просочування інформації**
  - **перетворювачі фізичних величин;**
  - **випромінювачі електромагнітних коливань;**
  - **паразитні зв'язки і наведення на дроти і елементи електронних пристроїв.**

- **За принципами перетворення акустичні перетворювачі підрозділяються на**
  - **індуктивні,**
  - **ємкісні,**
  - **п'єзоелектричні**
  - **оптичні.**

- **За виглядом перетворення вони можуть бути і акустичними, і електромагнітними.**

Джерела утворення ТКПІ$_2$



Передумови утворення ТКПІ

Передумови утворення каналів просочування інформації$_1$

- **Робота систем інформатизації і зв'язку, а також ведення переговорів по закритих питаннях супроводжуються виникненням акустичних і електромагнітних полів, і (або) електричних сигналів, що поширюються в різному середовищі (в повітрі, в струмопровідних конструкціях і так далі).**
- **Тому існують певні передумови для утворення каналів просочування інформації (або технічних каналів просочування інформації) при роботі різних технічних засобів і систем.**

Передумови утворення каналів просочування інформації$_2$

- **Необхідною умовою утворення каналів є наявність небезпечного сигналу (тобто сигналу, що містить закриту інформацію) в електричних полях і інших сигналах, які утворюються роботою технічних засобів.**
- **Виявлення, прийом і аналіз носіїв небезпечного сигналу технічними засобами розвідки дозволяє несанкціоновано отримати закриту інформацію, що обробляється технічними засобами систем інформатизації і зв'язку.**
- ***У загальному випадку під технічним каналом просочування інформації будемо розуміти сукупність джерела небезпечного сигналу, середу поширення носія небезпечного сигналу і засобу розвідки.***

Передумови утворення каналів просочування інформації$_3$

- **Можливість утворення технічних каналів просочування інформації в системах і засобах інформатизації і зв'язку обумовлена наступними причинами:**
  - **наявністю інформаційних радио-, оптичних і електричних сигналів в різних технічних засобах передачі і обробки інформації;**
  - **наявністю небажаних електромагнітних випромінювань систем і засобів інформатизації і зв'язку;**
  - **утворенням наведень електромагнітних випромінювань на різні струмоведучі ланцюги и і конструкції;**
  - **вживанням спеціальних дій на елементи технічних засобів;**
  - **вживанням різних заставних пристроїв;**
  - **виникненням і поширенням в навколишньому середовищі акустичних коливань при обговоренні питань, що містять секретні відомості;**
  - **наявністю випадкових електроакустичних перетворювачів в окремих елементах технічних засобів.**

Паразитні зв'язки і наведення

- Паразитні зв'язки і наведення виявляються у вигляді зворотнього зв'язку (найбільш характерний позитивний зворотній зв'язок), витоку по ланцюгах живлення і заземлення.
- Технічні засоби і системи можуть не лише безпосередньо випромінювати в простір сигнали, що містять оброблювану ними інформацію, але і уловлювати за рахунок своїх мікрофонних або антенних властивостей
- Такі технічні засоби можуть перетворювати прийняті випромінювання в електричні сигнали і передавати їх по своїх лініях зв'язку, як правило, безконтрольним, за територією об'єкту на значні відстані, що в ще більшій мірі підвищує небезпеку просочування інформації.

Можливість утворення ТКПІ

- Можливістю утворювати радіотехнічні канали витоку володіють деякі телефонні апарати, датчики охоронної і пожежної сигналізації, їх лінії, а також мережа електроживлення.
  - Непоодинокі випадки, коли технічні пристрої мають в своєму складі, окрім подібних “мікрофонів” і “антен”, високочастотні або імпульсні генератори.
  - Коливання, що генеруються, в таких пристроях можуть бути промодульовані електричними сигналами, що виявилися, внаслідок чого ці технічні пристрої перетворюються на радіопередавачі і представляють серйозну небезпеку, оскільки здатні випромінювати інформацію в навколишній простір.

Небезпечний сигнал$_1$

- Як в будь-якій системі зв'язку, в каналах просочування інформації небезпечний сигнал (сигнал, що несе секретну інформацію) характеризується тривалістю Т динамічним діапазоном Д і шириною спектра F добутком яких є його об'єм
  - V = T F Д.
- Щоб прийняти такий об'єм інформації, на приймаючій стороні має бути апаратура, що володіє відповідними характеристиками, тобто що має необхідну чутливість при певному перевищенні сигналу над рівнем власних перешкод, і що забезпечує необхідну ширину смуги сигналів, що приймаються, при відповідній тривалості їх передачі.

Небезпечний сигнал$_2$

- По каналу може проходити без спотворення лише такий сигнал, який задовольняє умовам (Тк Fк і Дк — це тривалість прийому інформації каналом, ширина спектру сигналу, що приймається, і динамічний діапазон каналу, відповідно):

$$T \leq Тк;\ F \leq Fк;\ Д \leq Дк$$

Небезпечний сигнал$_3$

- Ширина смуги пропускання (частотний спектр) каналу F міняється від 3100 Гц для телефонного до 8 Мгц для телебачення і до сотень мегагерц для оптичних ліній зв'язку.
- Перевищення сигналу над перешкодою в каналі (динамічний діапазон) Д, співвідношення, що визначається потужностей сигналу і перешкоди в каналі, — здатність каналу передавати різні рівні сигналу.
  - Цей параметр пов'язаний з розрахунковим рівнем перешкод, можливостями модуляції. Динамічний діапазон Д обмежує дальність передачі, а також впливає на можливість виділення сигналу на тлі перешкод.

Кількість переданої інформації

- Дальність визначається виразом:
  - Д = log (Рс/ Рп),
    - де Рс і Рп — середні потужності, відповідно, сигналу і перешкоди в каналі на вході приймача.
- Кожен канал також характеризується кількістю інформації, яка може бути передана по ньому.
- Граничне значення кількості інформації, яка може бути передана по каналу зв'язку, що володіє смугою пропускання F визначається формулою Шеннона:
  - C = F log (1 + Рс/ Рш) [дв. од./с],
    - де Рс — середня потужність сигналу, Р — потужність шумів з рівномірним частотним спектром.

Потенційні канали витоку інформації

Промислове шпигунство

- **Поняття промислове шпигунство** виникло разом з появою промисловості і є невід'ємною часткою стосунків в країнах, де на ряду з державною існують і інші форми власності.
- **Суть промислового шпигунства** – це прагнення до опанування секретів конкурентів з метою отримання максимальної комерційної вигоди.

Потенційні канали витоку інформації$_1$

1. Розмова декількох осіб	Акустичний сигнал	Підслуховування, у тому числі випадкове. Диктофони. Заставні пристрої з передачею інформації по: наявним коммунікаціям (трубам, ланцюгам сигналізації, мережам 220 В, телефонним лініям...), спеціально прокладеним дротам, радіо- або ІЧ-каналам. Направлений мікрофон.
	Віброакустичний сигнал	Стетоскоп - вібродатчик з передачею інформації по: радіоканалу, дротам, комунікаціям, ІЧ-каналу. Оптичний лазерний мікрофон
	Гідроакустичний сигнал	Гідроакустичний датчик.
	Акустоелектричний сигнал	Радіоприймач спецпризначення.
	Рух губ	Візуально, у тому числі оптичними приладами. Камера, у тому числі з передачею по дротах і радіоканалі.

Потенційні канали витоку інформації$_2$

2. Розмова по телефону	**Акустичний сигнал**	**Аналогічно п. 1**
	Електричний сигнал в лінії	**Паралельний телефон, пряме підключення, підключення через електромагнітний датчик, телефонна радіозакладка**
	Побічні електромагнітні випромінювання (ПЕМВ) і наведення	**Спеціальні радіотехнічні пристрої**

Потенційні канали витоку інформації$_3$

3. Розмова по радіотелефону	**Акустичний сигнал Електромагнітні хвилі**	**Апаратура п. 1 Спеціальні радіоприймальні пристрої**
4. Документ на паперовому носієві	**Наявність**	**Візуально, у тому числі за допомогою оптичних засобів. Фотографування, у тому числі з дистанційною передачею знімка. Копіювання**

Потенційні канали витоку інформації$_4$

5. Розмноження документа на паперовому носієві	**Сліди на нижньому листі, копіювальному папері або фарбувальній стрічці**	**Крадіжка, візуально.**
	Шуми принтера	**Спецапаратура акустичного контролю.**
	ПЕМВ від ПЕОМ	**Спеціальні радіотехнічні пристрої.**

Потенційні канали витоку інформації$_5$

6. Поштові відправлення	**Наявність**	**Прочитання: з розтином, без розтину**
7. Документ на непаперовому носієві	**Носій**	**Копіювання, розтин, несанкціоноване використання ПЕОМ.**

Потенційні канали витоку інформації$_6$

8. Виготовлення документа на непаперовому носієві	**Зображення на дисплеї**	**Візуально, у тому числі за допомогою оптичних засобів.** **Фотографування.** **Відео або телевізійні заставні пристрої.**
	ПЕМВ	**Спеціальні радіотехнічні пристрої**
	Електричні сигнали в мережах	**Апаратні закладки**

Потенційні канали витоку інформації$_7$

9. Передача документів на непаперовому носієві.	**Електричні сигнали**	**Несанкціоноване підключення до інформаційної системи, імітація користувача**

Донецький національний технічний університет



Тема 4. Технічні канали витоку інформації.
Лекція 10. Просочування інформації технічними каналами.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Просочування інформації по ланцюгах заземлення
- Просочування інформації по ланцюгах живлення
- Віброакустичний канал
- Електроакустичний канал
- Просочування інформації у волоконно-оптичних лініях зв'язку

Просочування інформації по ланцюгах заземлення

Заземлення

- **Заземленням** називається навмисне з'єднання об'єкту із заземляючим пристроєм. Заземлення здійснюється шляхом створення системи провідних поверхонь і електричних з'єднань, призначених для виконання різних функцій.
- **Захисне заземлення** призначене для виключення поразки обслуговуючого персоналу електричним струмом. Захисне заземлення повинне підтримувати елементи конструкції при одному і тому ж потенціалі, рівному або близькому до потенціалу «землі», і забезпечувати низькоомне навантаження для великих струмів, що виникають в системах при аварійних ситуаціях.
- Як правило, захисні заземлення повинні мати хороший низькоомний контакт з «землею», тому їх часто називають зовнішніми заземлювачами

Види заземлень

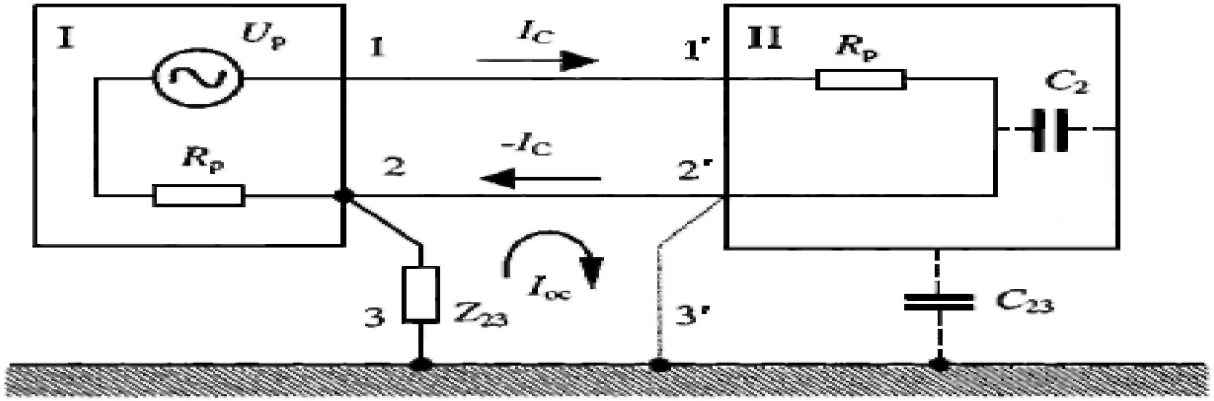
- Зовнішні заземлювачі здійснюють заземлення силових систем, радіочастотних антен, громовідводів, зтікачів статичної електрики і так далі.
- Робочі заземлення включають заземлення силового устаткування.
- Сигнальне або схемне заземлення забезпечує формування опорного потенціалу, необхідного для роботи електронних схем.
- Заземлення екрануючих поверхонь сприяє ослабленню небажаних зв'язків і є складовою частиною системи екранування.
  - Провідні поверхні і електричні з'єднання системи заземлення екранів призначені для протікання зворотних струмів в сигнальних ланцюгах і ланцюгах електроживлення.

Виникнення небезпечного сигналу в контурах заземлення$_1$

- Однією з причин попадання небезпечного сигналу в систему заземлення є наявність електромагнітного поля – носія небезпечного сигналу в місцях розташування елементів системи заземлення.
  - Це електромагнітне поле наводить в розташованій поблизу системі заземлення струм небезпечного сигналу.
- Проникнення небезпечного сигналу в ланцюг заземлення може бути пов'язане з утворенням, так званих контурів заземлення.

Виникнення небезпечного сигналу в контурах заземлення$_2$

- Розглянемо два пристрої, сполучені парою провідників, один з яких є сигнальним, а інший служить для протікання зворотних струмів

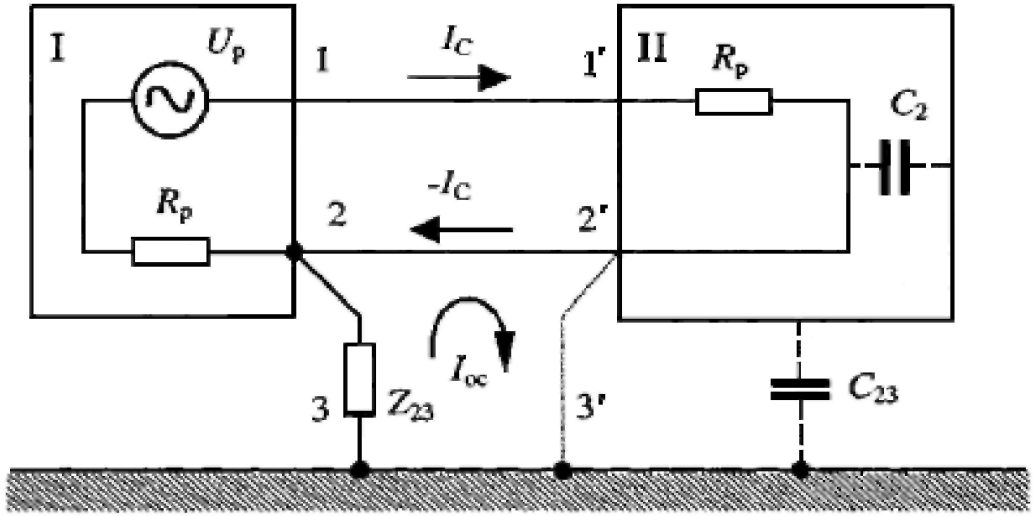


- Зворотній провідник сполучении з корпусом першого (I) пристрою, а корпус – із землею. Якщо цей провідник сполучений з корпусом другого (II) пристрою, що також має електричний контакт із землею (з'єднання 2'–3'), то утворюється замкнутий провідний контур 2–2'–3'–3–2. Зовнішнє електромагнітне поле джерела небезпечного сигналу наводить в цьому контурі ЕДС, викликаючи протікання струму IOC який, у свою чергу, створює на ділянці 2–3 падіння напруги UOC рівне:

$$U_{OC} = I_{OC} Z_{23},$$

Виникнення небезпечного сигналу в контурах заземлення$_3$

- Якщо відсутній провідник 2'–3' або з'єднання провідника 2–2' з корпусом другого пристрою, то можливість утворення контуру заземлення повністю не виключається. У цих випадках контур може складатися з провідників 2–2', 3–3', земляної шини і паразитних ємностей між сигнальним ланцюгом і корпусом другого пристрою С2 а також між корпусом другого пристрою і землею С23.



Виникнення небезпечного сигналу в контурах заземлення$_4$

- Ще одна причина появи небезпечного сигналу в ланцюзі заземлення пов'язана з кінцевим значенням величини опору заземляючих провідників.
- По заземляючому провідникові протікає зворотний електричний струм небезпечного сигналу

Із-за кінцевого опору R_3 земляної шини на цьому опорі створюється падіння напруги:

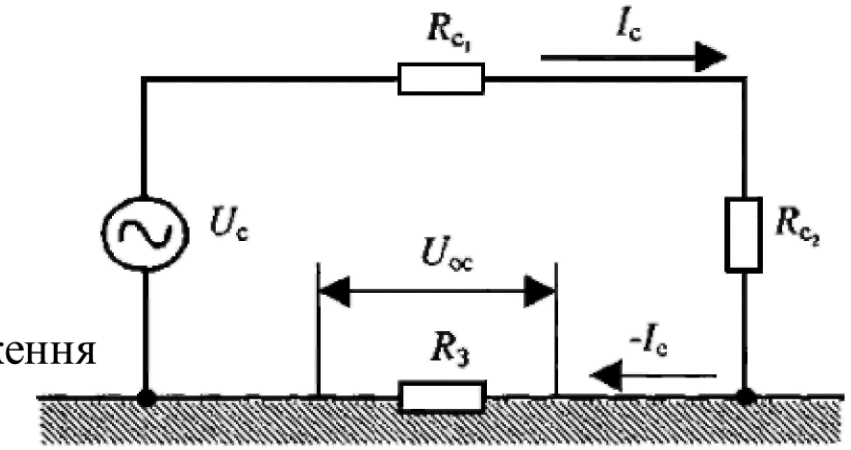
$$U_{OC} = \frac{U_C R_3}{R_{C_1} + R_{C_2} + R_3},$$

де U_{OC} – напруга джерела сигналу;

R_{C_1}, R_{C_2} – внутрішній опір джерела сигналу і опір навантаження відповідно.

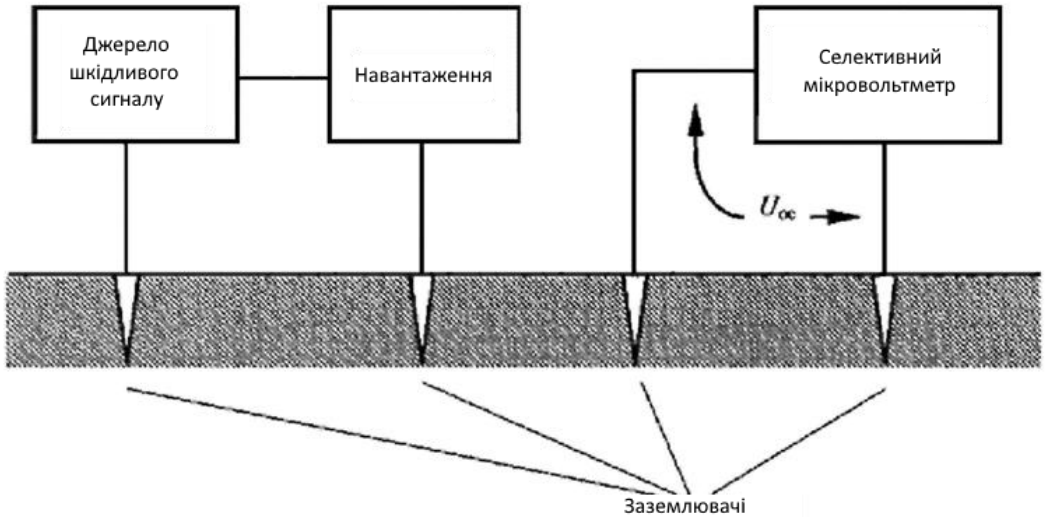
При $R_{C_1} + R_{C_2} >> R_3$

$$U_{OC} \approx \frac{U_C R_3}{R_{C_1} + R_{C_2}},$$



Перехоплення електромагнітного поля небезпечного сигналу в ґрунті навколо заземлювача

- Можливість просочування інформації, пов'язана з ланцюгами заземлення, обумовлена також наявністю електромагнітного поля небезпечного сигналу в ґрунті навколо заземлювача.
- Із-за великого загасання, що вноситься ґрунтом, магнітне поле в землю практично не проникає. Електричне поле в землі визначається величиною потенціалу заземлювача і параметрами ґрунту
- За допомогою додаткових спеціально встановлених заземлювачів можна здійснити перехоплення небезпечного сигналу

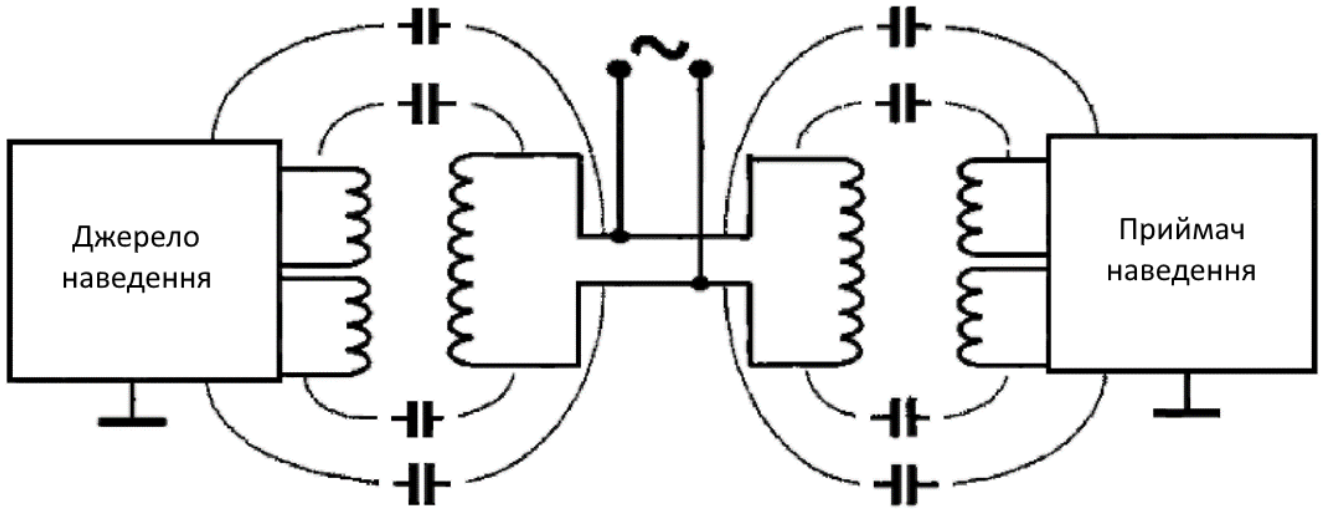


Просочування інформації по ланцюгах живлення

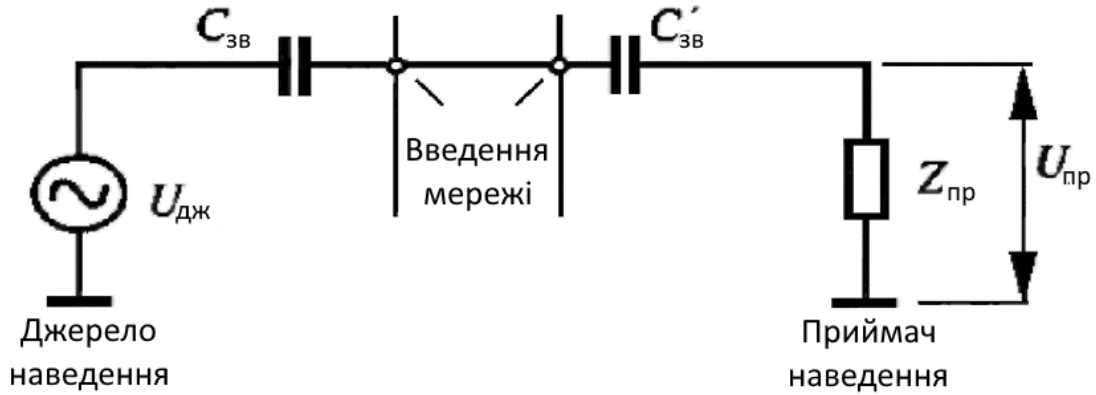
Асиметричне наведення$_1$

- Просочування інформації по ланцюгах живлення обумовлене різними причинами.
- Як правило, дроти загальної мережі живлення розподіляються по різних приміщеннях, де розташовані технічні системи, і сполучені з різними пристроями.
- Внаслідок цього утворюється небажаний зв'язок між окремими технічними засобами. Крім того, дроти мережі живлення є лінійними антенами, здатними випромінювати або сприймати електромагнітні поля.
- У разі асиметричного наведення, коли дроти мережі живлення прокладаються разом і мають однакові ємкості щодо джерел і приймачів наведення, в них наводиться напруга, однакова по величині і по фазі щодо землі і корпусу приладів.

Асиметричне наведення$_2$



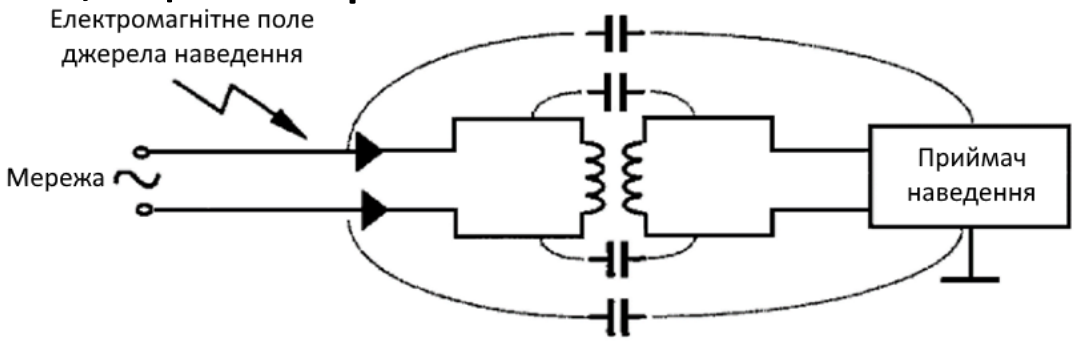
Дійсна схема небажаного асиметричного зв'язку



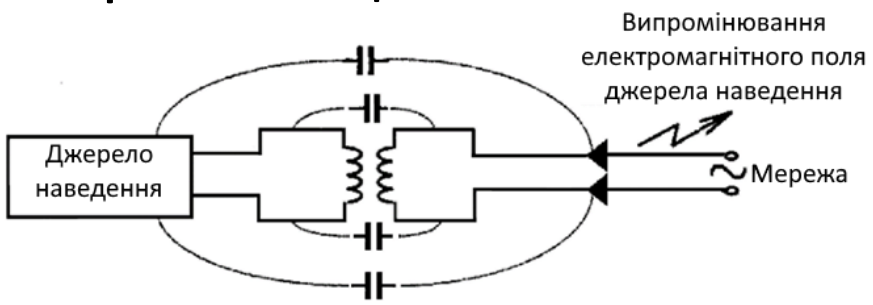
Еквівалентна схема небажаного асиметричного зв'язку

Асиметричне наведення$_3$

- Здійснення прийому небезпечного сигналу через мережу живлення, в якій наводиться напруга за рахунок електромагнітного поля, що випромінюється технічними засобами.



- Випромінювання небезпечного сигналу через ланцюги живлення джерела наведення.



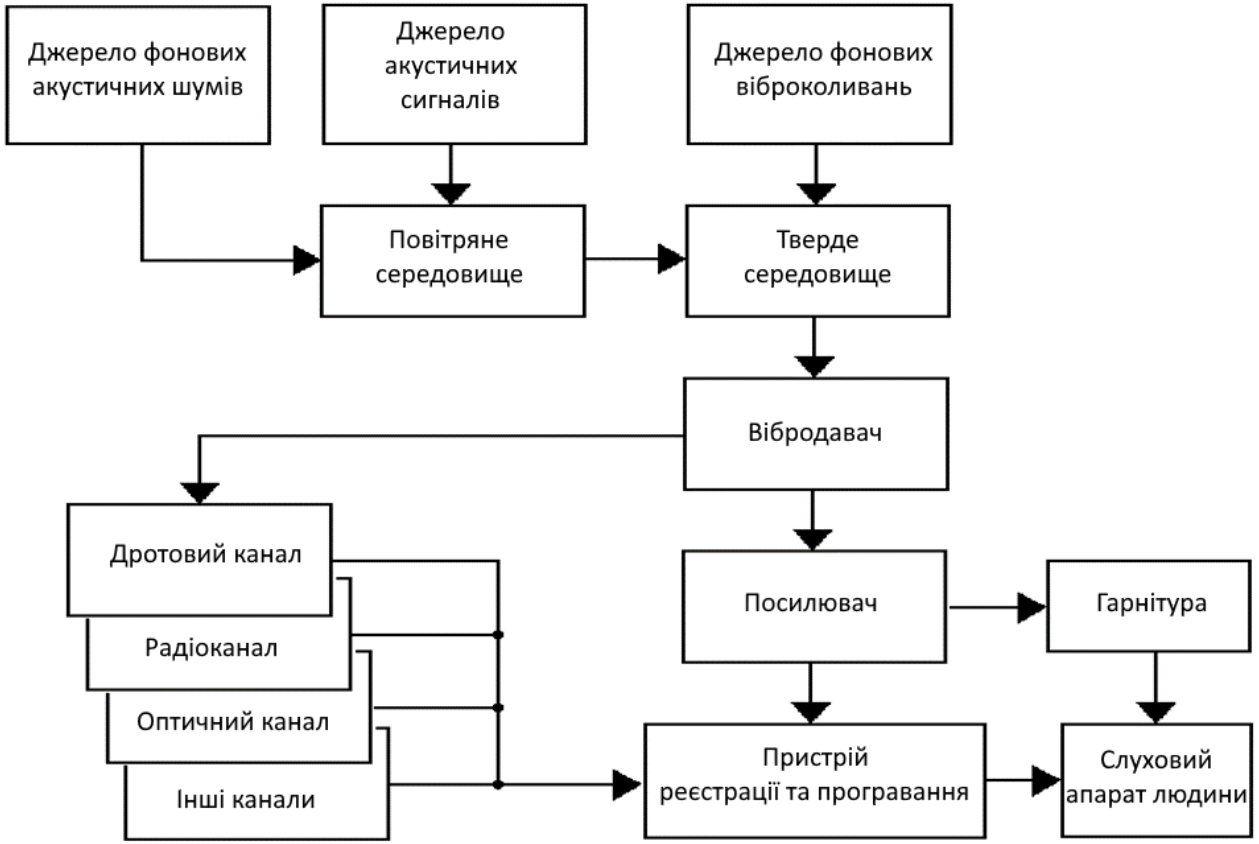
Віброакустичний канал

Віброакустичне перетворення

- Дія акустичних хвиль на поверхню твердого тіла приводить до виникнення в нім вібраційних коливань в результаті віброакустичного перетворення.
- Ці коливання, що розповсюджуються в твердому середовищі, можуть бути перехоплені спеціальними засобами розвідки, а мовна інформація, що міститься в акустичному полі, за певних умов може бути відновлена. З цією метою використовують спеціальні пристрої, що перетворюють вібраційні коливання в електричні сигнали, відповідні звуковим частотам. Такі пристрої називаються вібродатчиками.
- Сигнал, що знімається з виходу вібродатчика, після посилення може прослуховувати, бути зареєстрований на магнітному або іншому носієві або переданий в пункт прийому, що знаходиться на видаленні від місця прослуховування, по дротяному, радіо- або іншому каналу передачі інформації.

Віброакустичний канал просочування інформації

- Структурна схема віброакустичного каналу просочування інформації



Звукопроводи

- Як звукопровода можна використовувати труби водопостачання, каналізації, батареї опалювання і так далі
- Кріплення вібродатчиків до елементів конструкції, по якій розповсюджуються вібрації, може здійснюватися за допомогою спеціальних мастик, клейових складів, магнітів і так далі
- На якість прийому вібросигналів окрім властивостей вібродатчика і матеріалу твердого середовища впливають її товщина, а також рівні фонових акустичних шумів в приміщенні і вібрацій в твердому середовищі.

Електроакустичний канал

Електроакустичний канал просочування інформації

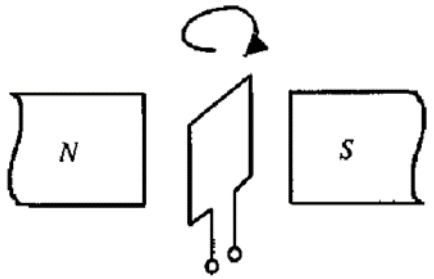
- Утворення електроакустичного каналу просочування інформації пов'язане з наявністю в ТЗОІ випадкових електроакустичних перетворювачів, що називаються **випадковими мікрофонами**.
- Ці елементи володіють здатністю перетворювати акустичні коливання в електричні сигнали, хоча і не призначені для цієї мети. Елементи технічних засобів обробки інформації, що володіють властивостями випадкових електроакустичних перетворювачів, можуть піддаватися дії акустичних полів з достатніми інтенсивністю і звуковим тиском.
- В результаті на виходах випадкових електроакустичних перетворювачів можуть виникнути електричні заряди, струми або ЕДС, або відбутися зміни параметрів струмів і напруги, що формуються в ланцюгах технічних засобів при їх функціонуванні, обумовлені небезпечними сигналами (наприклад, небажана модуляція).

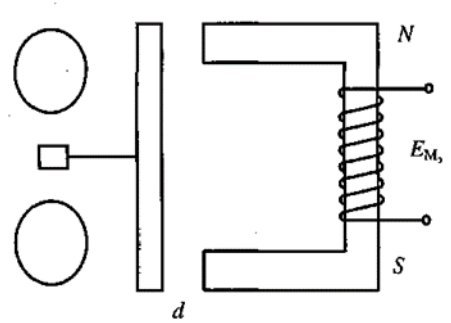
Електроакустичні перетворювачі$_1$

- Мікрофонні властивості випадкових електроакустичних перетворювачів виявляються в результаті різних фізичних явищ, що приводять до появи струму або ЕДС при переміщенні елементу або його деформації під дією акустичного поля.
- Велику групу випадкових електроакустичних перетворювачів складають індукційні (індуктивні) перетворювачі. Наприклад, якщо помістити рамку (котушку індуктивності) в магнітне поле, що створюється постійним магнітом і змінювати її орієнтацію щодо напряму вектора магнітній індукції поля, то на виході рамки з'явиться ЕДС індукції.

Електроакустичні перетворювачі$_2$

- До індуктивних випадкових електроакустичних перетворювачів відносять електричні дзвінки, гучномовці, електромеханічні реле, трансформатори і так далі.





Викличний дзвінок $ТА_1$

- До складу телефонного апарату входить викличний дзвінок, який при покладеній мікротелефонній трубці підключений до лінії через конденсатор. Цей дзвінок є електромагнітною системою в якій під впливом акустичного поля відбувається переміщення якоря, що викликає появу ЕДС небезпечного сигнала в обмотці дзвінка і в лінії, підключеній до телефонного апарату.

Викличний дзвінок $ТА_2$

Акустична чутливість викличного дзвінка може бути розрахована по формулі (мВ/Па)

$$\eta = \frac{VS\mu\omega S_м}{d^2 Z_м},$$

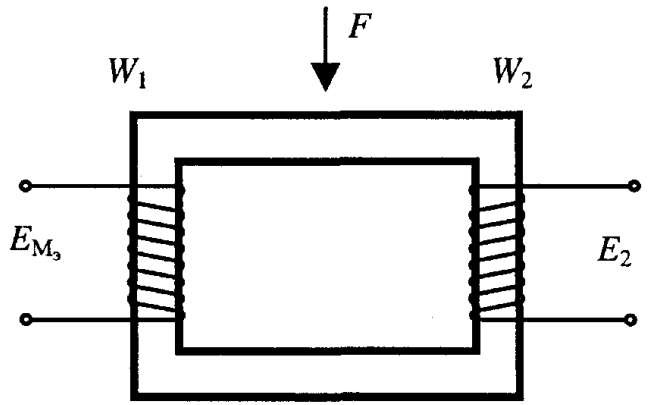
де V – магніторушійна сила постійного магніту;
S – площа якоря;
μ – магнітна проникність сердечника;
ω– число витків котушки дзвінка;
$S_М$– площа полюсного наконечника магніту;
d – величина зазору в магнітному ланцюзі якоря;
$Z_М$– механічний опір акустикомеханічної системи дзвінка.

Електродинамічні гучномовці

- Достатньо високу чутливість до акустичної дії мають електродинамічні гучномовці, використовувані в системах звуковідтворення або в радіотрансляційній мережі (2-3 мВ/Па), а також виконавчі пристрої вторинного електричного годинника, що працює від системи єдиного часу (100-500 мкВ/Па).

Трансформатори

- Різні трансформатори (вхідні, вихідні, в мережі живлення і так далі) також можуть виконувати роль електроакустичних перетворювачів. Трансформатор складається із замкнутого сердечника, зробленого з м'якої сталі або фериту, на якому є, як мінімум, дві ізольовані один від одного обмотки з різним числом витків W1 і W2



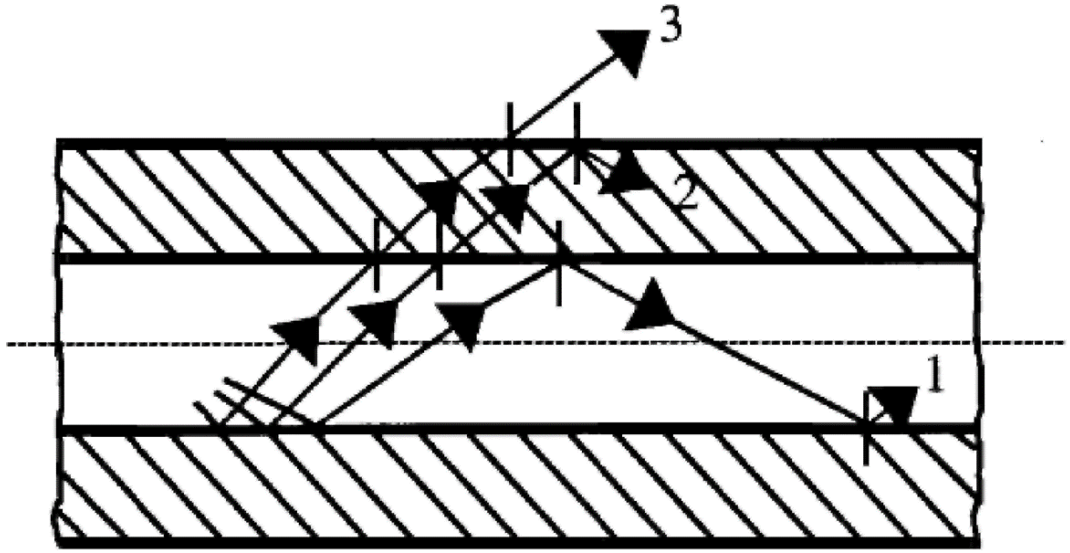
Просочування інформації у волоконно-оптичних лініях зв'язку

Просочування інформації в ВОЛЗ

- Основні причини просочування інформації у волоконно-оптичних лініях пов'язані з випромінюванням світлової енергії в навколишній простір.
- Причини цього випромінювання обумовлені процесами, що відбуваються при введенні (виводі) випромінювання в оптичний хвилевід і розповсюдженні хвиль в діелектричному хвилеводі.
- Просочування інформації за рахунок оптичного випромінювання може мати місце із-за наявності постійних і роз'ємних з'єднань оптичних волокон, а також вигинів і пошкоджень цих волокон

Прямолінійні світловоди

- У прямолінійних світлопроводах випромінювання в навколишнє середовище невелике. Проте в місцях вигинів хвилеводів інтенсивність випромінювання в оболонку або повітря збільшується, і тим більше, чим сильніше ці вигини. Інтенсивність випромінювання в навколишній простір збільшується і при пошкодженні оболонки світлопровода.

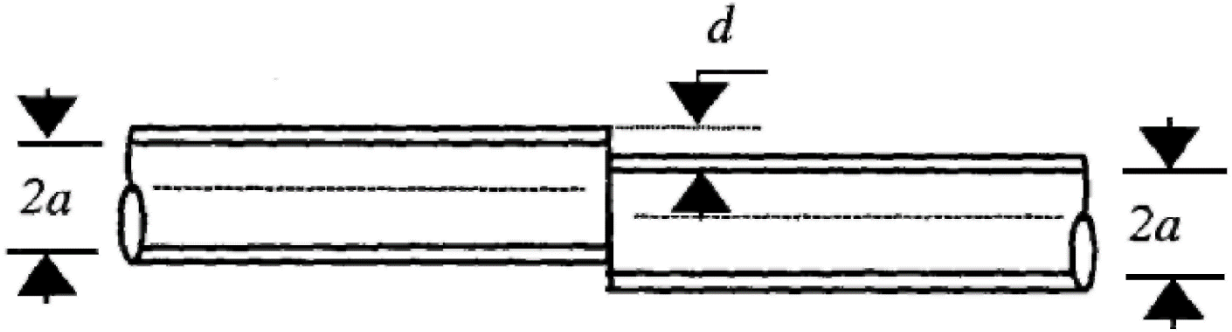


Неузгодженість оптичних волокон$_1$

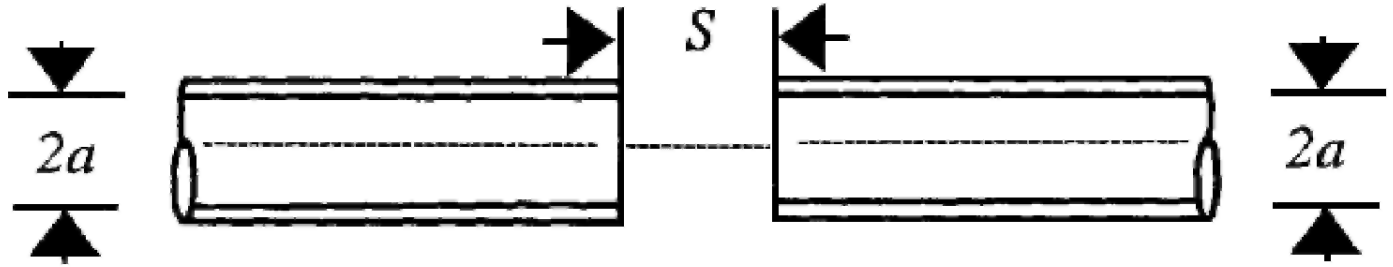
- Постійні з'єднання відрізів оптичних волокон між собою здійснюють зварюванням, сплавом або склеюванням в котирувальному пристрої. Оптичні роз'єми (з'єднувачі) повинні допускати багатократні з'єднання – роз'єднання оптичних волокон.
- Неузгодженість волокон виникає із-за наявних відмінностей в числовій апертурі, профілі показника заломлення, діаметрі серцевини або із-за погрішностей у взаємній орієнтації волокон при їх з'єднанні.

Неузгодженість оптичних волокон$_2$

- Зсув (осьове несуміщення d) з’єднуємих волокон

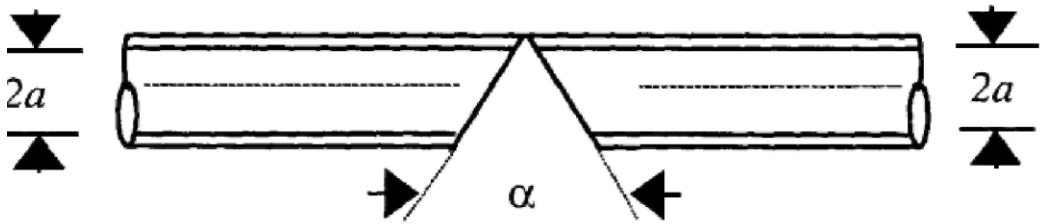


Наявність зазору шириною S між торцями з’єднуємих волокон



Неузгодженість оптичних волокон$_3$

Непаралельність $\alpha > 0$ торцевих поверхонь з'єднуємих волокон



Кутова неузгодженість осей з'єднуємих волокон

Донецький національний технічний університет



Тема 4. Технічні канали витоку інформації.
Лекція 11. Канали витоку інформації при експлуатації ЕОМ.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Канали витоку інформації ЕОМ
- Перехоплення ПЕМВ
- Способи перехоплення інформації, що обробляється технічними засобами
- Способи і засоби захисту інформації
- Оцінка рівня ПЕМВ

Канали витоку інформації ЕОМ

Ділянки, які підлягають захисту

- Як відомо, сучасні ПЕОМ можуть працювати як незалежно один від одного, так і взаємодіючи з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, але й глобальними.
- Ділянки, в яких можуть знаходитися дані, які підлягають захисту:
  - безпосередньо в оперативній або постійній пам'яті ПЕОМ;
  - на знімних магнітних, магнітооптичних, лазерних і інших носіях;
  - на зовнішніх пристроях зберігання інформації колективного доступу (RAID - масиви,файлові сервери і т.ін.);
  - на екранах пристроїв відображення (дисплеї, монітори, консолі);
  - у пам'яті пристроїв введення-виведення (принтери, графічні пристрої, сканери);
  - у пам'яті керуючих пристроїв, лініях зв'язку, каналів узгодження комп'ютерних мереж.



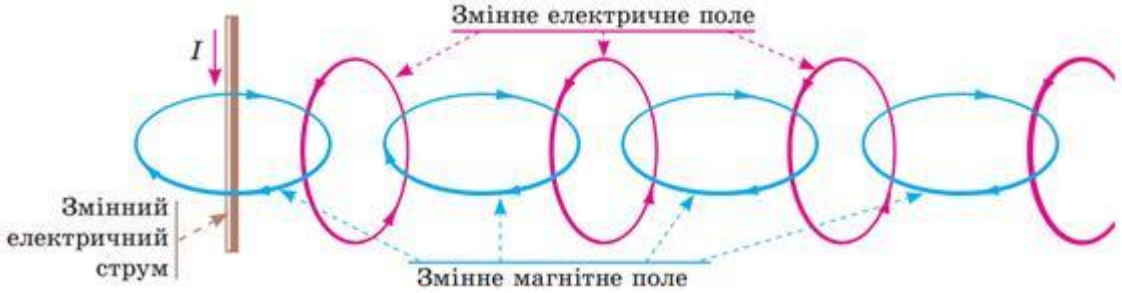




Джерела каналів витоку інформації

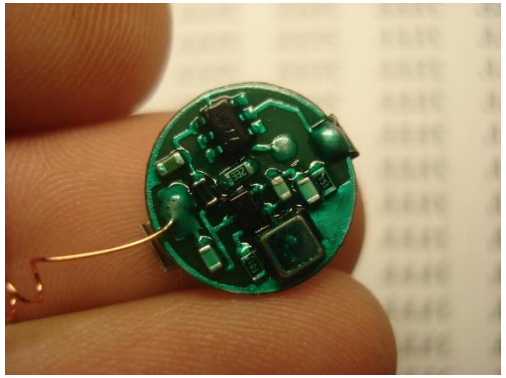
- Канали витоку інформації утворюються як при безпосередній роботі ЕОМ, так і в режимі очікування.
- Джерелами таких каналів є:
  - електромагнітні поля;
  - струми, що наводяться, і напруги в провідних системах (живлення, заземлення й з’єднання);
  - перевипромінювання оброблюваної інформації на частотах паразитної генерації елементів і пристроїв технічних засобів ЕОМ;
  - перевипромінювання оброблюваної інформації на частотах контрольно-вимірювальної апаратури (КВА).





Навмисні канали витоку інформації

- Крім цих каналів, зумовлених природою процесів, що протікають в ПЕОМ і їх технічними особливостями, в ПЕОМ, що поставляються на ринок, можуть навмисно створюватися додаткові канали витоку інформації.
- Для утворення таких каналів може використовуватися:
  - розміщення в ПЕОМ закладок на мову або оброблювану інформацію (замасковані під якісь електронні блоки);
  - встановлення в ПЕОМ радіомаячків;
  - навмисне застосування таких конструктивно-схемних рішень, які приводять до збільшення електромагнітних випромінювань у певній частині спектра;
  - встановлення закладок, що забезпечують знищення ПЕОМ ззовні (схемні рішення);
  - встановлення елементної бази, що виходить із ладу.





Типи обробки інформації

- Крім того, класифікацію можливих каналів витоку інформації в першому наближенні можна здійснити на основі принципів, відповідно до яких обробляється інформація, що отримується по можливому каналу витоку.
- Передбачається три типи обробки:
  - людиною
  - апаратурою
  - програмою.







Обробка людиною

- Відповідно до кожного типу обробки довільні канали витоку також поділяються на три групи.
- Відносно ПЕОМ групу каналів, в яких основним видом обробки є обробка людиною, виділяються наступні можливі канали витоку:
  - розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);



  - читання інформації з екрана сторонньою особою;



  - читання інформації із залишених без нагляду паперових роздруківок.



Обробка апаратурою

- У групі каналів, в яких основним видом обробки є обробка апаратурою, можна виділити наступні можливі канали витоку:
  - під’єднання до ПЕОМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;





  - використання спеціальних технічних засобів для перехоплення
  - електромагнітних випромінювань технічних засобів ПЕОМ.

Програмна обробка

- У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі канали витоку:
  - несанкціонований доступ програми до інформації;
  - розшифровка програмою зашифрованої інформації;
  - копіювання програмою інформації з носіїв;
  - блокування або вимкнення програмних засобів захисту.





Основні технічні засоби та системи

- **Основні технічні засоби та системи (ОТЗС)** - технічні засоби та системи, а також їх комунікації, що використовуються для обробки, зберігання та передачі конфіденційної інформації.
- До ОТЗС відносяться:
  - технічні засоби АС управління, електронно-обчислювальні машини та їх окремі елементи;
  - засоби виготовлення та розмноження документів;
  - апаратура звукопідсилення, звукозапису, звуковідтворення та синхронного перекладу;
  - системи внутрішнього телебачення;
  - системи відеозапису та відеовідтворення;
  - системи оперативно-командного зв'язку;
  - системи внутрішнього автоматичного телефонного зв'язку, включаючи і з'єднувальні лінії перерахованого вище обладнання та ін.

Допоміжні технічні засоби та системи

- **Допоміжні технічні засоби та системи (ДТЗС)** - технічні засоби та системи, не призначені для передачі, обробки та зберігання конфіденційної інформації, що встановлюються спільно з основними технічними засобами та системами або в приміщеннях, що захищаються.
- До ДТЗС відносяться:
  - різного роду телефонні засоби та системи;
  - засоби передачі даних у системі радіозв'язку;
  - системи охоронної та пожежної сигналізації;
  - засоби оповіщення та сигналізації;
  - контрольно-вимірювальна апаратура;
  - системи кондиціювання;
  - системи провідної радіотрансляційної мережі та прийому програм радіомовлення та телебачення (абонентські гучномовці, системи радіомовлення, телевізори та радіоприймачі тощо);
  - засоби електронної оргтехніки;
  - засоби та системи електрочасифікації;
  - інші технічні засоби та системи.

Побічні електромагнітні випромінювання та наведення

- **Побічні електромагнітні випромінювання та наведення (ПЕМВН)** – це паразитні та побічні електромагнітні випромінювання радіоелектронного обладнання та засобів обчислювальної техніки.
- Залежно від середовища розповсюдження розрізняють:
  - електромагнітні канали витоку інформації, однорідне середовище поширення – ефір;
  - електричні канали витоку інформації, неоднорідне середовище поширення – ефір та лінії допоміжних технічних засобів та системи, у тому числі і проникнення їх від основних технічних засобів та систем у лінії, що відходять.
- У електромагнітних каналах витоку інформації носієм інформації є електромагнітні випромінювання (ЕМВ), що виникають під час обробки інформації технічними засобами.
- Побічні електромагнітні випромінювання (ПЕМВ) - небажані (паразитні) електромагнітні випромінювання, що виникають при функціонуванні технічних засобів обробки інформації, і призводять до витоку інформації, що обробляється

Інформативні та неінформативні ПЕМВ

- **Інформативними ПЕМВ** називаються сигнали, що мають ВЧ несучу, модульовану інформацією оброблюваної на засобах обчислювальної техніки (наприклад, зображенням, що виводиться на екран монітора, даними, оброблюваними на пристроях введення-виведення тощо).
- **Неінформативними ПЕМВ** називаються сигнали, аналіз яких може дати уявлення лише про режим роботи засобах обчислювальної техніки і не розкриває характер інформації, оброблюваної на засобах обчислювальної техніки.
- Основними причинами виникнення електромагнітних каналів витоку інформації у технічних засобах обробки інформації (ТЗОІ) є:
  - побічні електромагнітні випромінювання, що виникають внаслідок протікання інформативних сигналів щодо елементів ТЗОІ;
  - модуляція інформативним сигналом побічних електромагнітних випромінювань високочастотних генераторів ТЗОІ (гетеродини, генератори підмагнічування та стирання, що задають генератори);
  - модуляція інформативним сигналом паразитного електромагнітного випромінювання ТЗОІ (наприклад, що виникає внаслідок самозбудження підсилювачів низької частоти).

Джерела ПЕМВ в ЕОМ$_1$

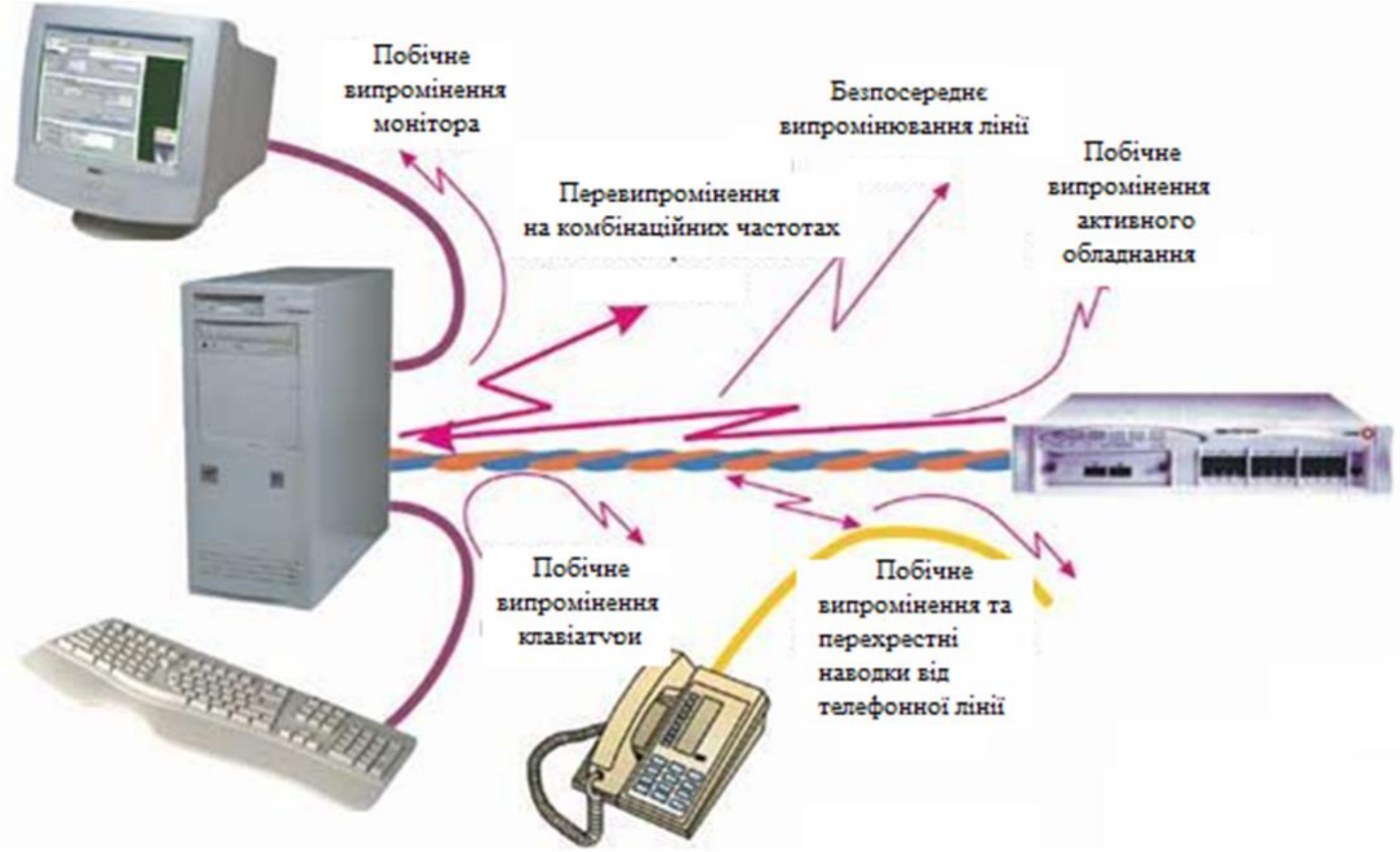
- Майже всі компоненти засобів обчислювальної техніки під час роботи є джерелами виникнення ПЕМВ:
  - процесор, шина даних процесора та ланцюга живлення;
  - контролери та міст чіпсету;
  - модулі пам'яті та шина даних;
  - інвертори живлення перелічених вище пристроїв;
  - HDD та шини IDE (ATA) та SATA;
  - CD та шина IDE (ATA);
  - відеокарта та шина AGP або E-PCI;
  - COM порт та зовнішні підключення по ньому;
  - LTP порт та зовнішні підключення по ньому;
  - USB порт;
  - VGA та інші види портів, призначені для підключення моніторів;
  - бездротові мережеві адаптери IEEE 802 для локальних мереж.







Джерела ПЕМВ в ЕОМ$_2$

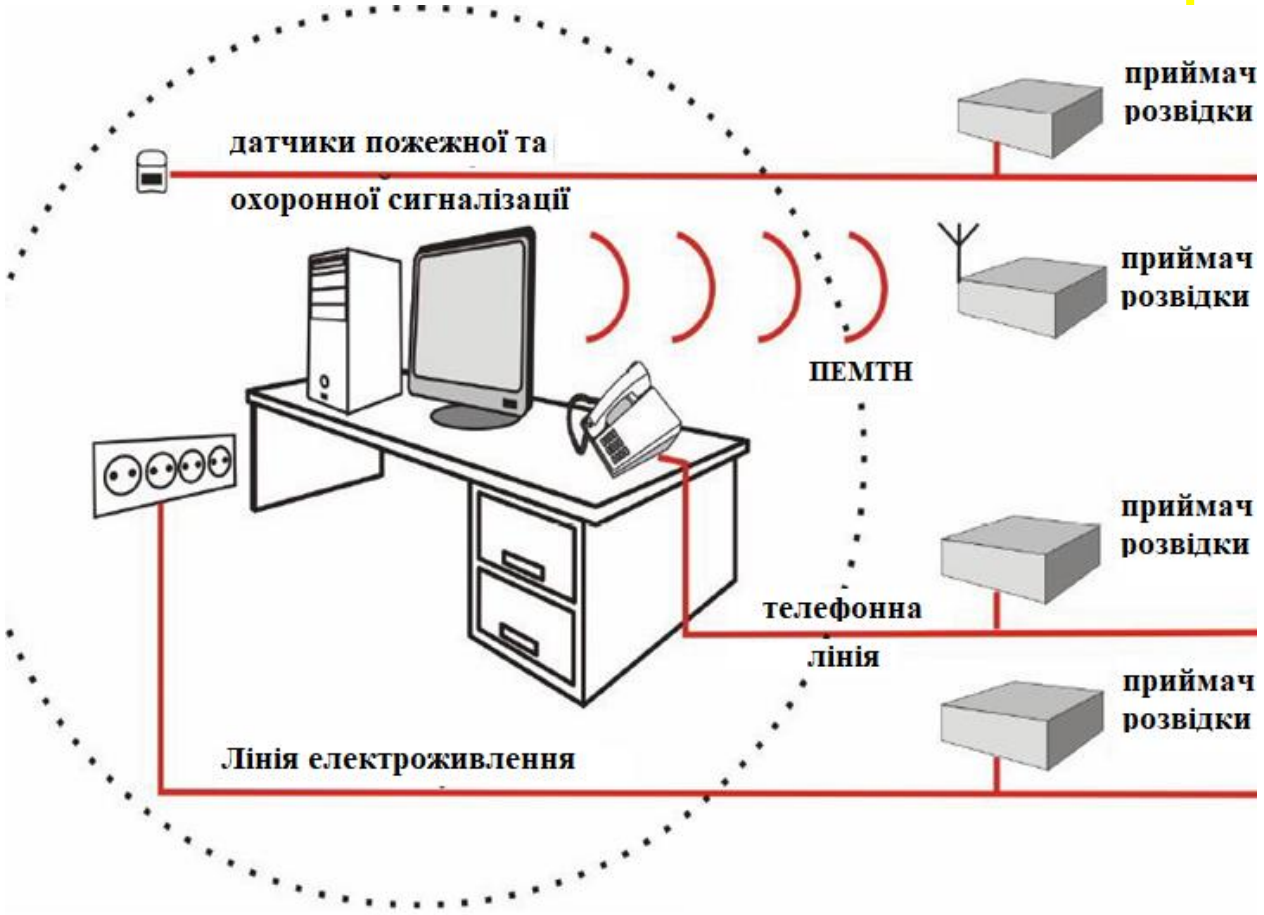


Фізичні причини ПЕМВ

- ЗАЛЕЖНО ВІД ФІЗИЧНИХ ПРИЧИН ВИНИКНЕННЯ НАВЕДЕННЯ ІНФОРМАТИВНИХ СИГНАЛІВ МОЖНА ПОДІЛИТИ НА:
  - наведення інформативних сигналів в електричних ланцюгах ТЗОІ, викликані інформативними побічними електромагнітними випромінюваннями ТЗОІ (ПЕМВ - струм у провіднику);
  - наведення інформативних сигналів у сполучних лініях допоміжних технічних засобах та системах та сторонніх провідників, викликані інформативними побічними електромагнітними випромінюваннями ТЗОІ;
  - наведення інформативних сигналів в електричних ланцюгах ТЗОІ, викликані внутрішніми ємнісними та індуктивними зв'язками (“просочування” інформативних сигналів у ланцюзі електроживлення через блоки живлення ТЗОІ, струм – струм);
  - наведення інформативних сигналів у ланцюгах заземлення ТЗОІ, викликані інформативними побічними електромагнітними випромінюваннями ТЗОІ, а також гальванічним зв'язком схемної (робочої) землі та блоків ТЗОІ (ПЕМІ - струм у провіднику, струм - струм).

Контрольована зона

- Рівень наведень залежить від відстані між джерелом випромінювання та випадковою антеною, типу випадкової антени (зосереджена або розподілена), довжиною паралельного пробігу та величиною перехідного згасання ліній, напруги інформативного сигналу в лінії та рівня шумів (перешкод) та інших факторів.
- Крім природних технічних каналів витоку інформації існують і спеціально створені технічні канали витоку (ТКВІ), наприклад, технічні канали витоку інформації, що створюються шляхом «високочастотного опромінення» ЗОТ або створювані шляхом впровадження в ЗОТ електронних пристроїв перехоплення інформації («заставних пристроїв»).



КОНТРОЛЬОВАНА ЗОНА

Режими обробки інформації

- Інформація в процесі обробки засобами обчислювальної техніки проходить через низку режимів її перетворення, передачі та відображення.
- НАЙБІЛЬШ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИМИ Є:
  - виведення інформації на екран монітора;
  - введення даних із клавіатури;
  - запис інформації на магнітні носії інформації (МНІ);
  - читання інформації з МНІ;
  - передача даних канали зв'язку;
  - виведення даних на пристрої друку;
  - запису даних від сканера на МНІ.

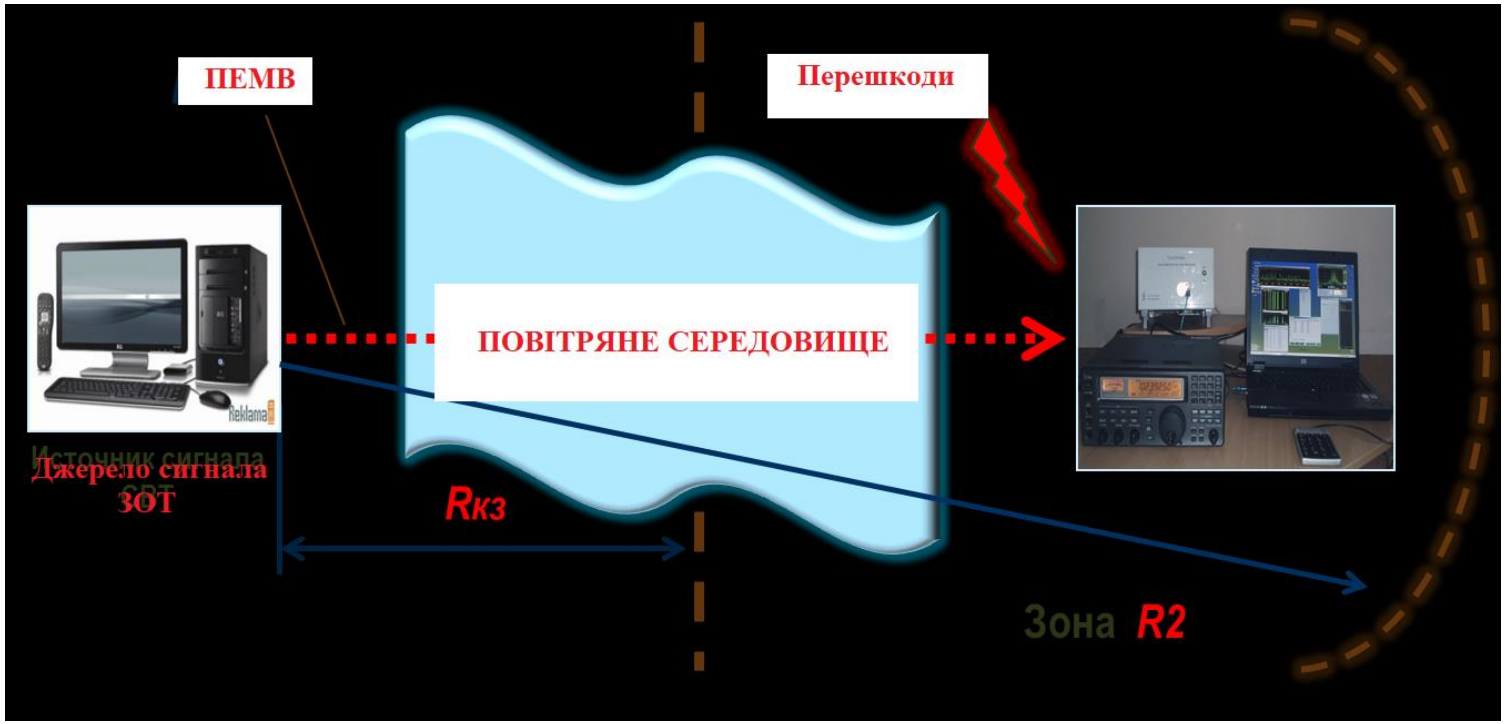
Дистанції перехоплення інформації

- Можливості перехоплення інформації засобами перехоплення побічного електромагнітного випромінювання та наведення залежить від виду технічного засобу та становить:
  - монітори з електронно-променевою трубкою – десятки, сотні метрів;
  - рідкокристалічні монітори – одиниці, десятки метрів;
  - жорсткі магнітні диски – одиниці метрів;
  - принтери, сканери, МФУ – десятки метрів;
  - клавіатура – десятки, сотні метрів;
  - Flash-накопичувачі, зовнішні HDD – без подовжувача – одиниці, з подовжувачем – десятки метрів.
- Зазначені відстані є зразковими і для конкретного об'єкта можуть відрізнятися як у меншу, так і більшу сторону.

Перехоплення ПЕМВ

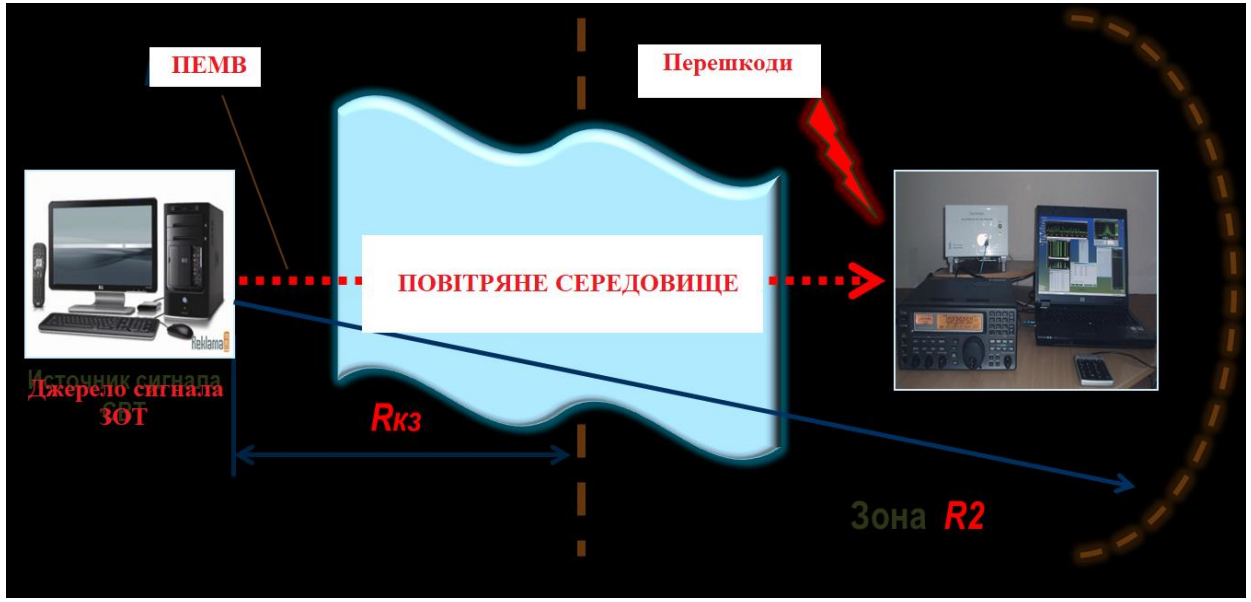
Схема технічного каналу витоку інформації

- У загальному вигляді схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки, виглядає так:



Зони поширення сигналу

- Повітряне середовище – це середовище поширення сигналу.
- Крім повітряного, середовищем поширення сигналу можуть бути:
  - лінії електроживлення та заземлення;
  - сторонні провідники (токопровідні інженерні комунікації, що виходять за межі КЗ);
  - сполучні лінії допоміжних технічних засобів та системи , що виходять за межі КЗ.
- Простір навколо основних технічних засобів та систем, на межі та за межами якого напруженість електромагнітного поля не перевищує допустимого (нормованого) значення, називається зоною 2 (R2).



Знімання наведень ПЕМВ$_1$

- ВИПАДКОВІ АНТЕНИ - різні допоміжні технічні засоби, їх з'єднувальні лінії, а також лінії електроживлення, сторонні провідники та ланцюги заземлення, при безпосередньому підключенні до яких засобів розвідки побічного електромагнітного випромінювання та наводок можливе перехоплення інформаційних сигналів.
- ВИПАДКОВІ АНТЕНИ можуть бути зосередженими та розподіленими.
  - **Зосереджені** - телефонний апарат, гучномовець радіотрансляційної мережі, датчик пожежної сигналізації і т. п., підключені до лінії, що виходить за межі КЗ.
  - **Розподілені** - кабелі, дроти, металеві труби та інші струмопровідні комунікації, що виходять за межі КЗ.

Знімання наведень ПЕМВ$_2$

- Простір навколо основних технічних засобів та систем (ОТЗС), на межі та за межами якого рівень наведеного від ОТЗС інформативного сигналу в зосереджених антенах не перевищує допустимого (нормованого) значення, називається зоною 1 (r1), а в розподілених антенах - зоною 1', (r1').
- Значення показника захищеності залежатиме не лише від рівня ПЕМВ ОТЗС, а й від довжини випадкової антени (від приміщення, в якому встановлено ОТЗС, до місця можливого підключення до неї засобу розвідки = Кл).
- Схема технічного каналу витоку інформації, що виникає за рахунок наведення ПЕМВ ЗОТ у випадкових антенах (схема електричного каналу витоку інформації):

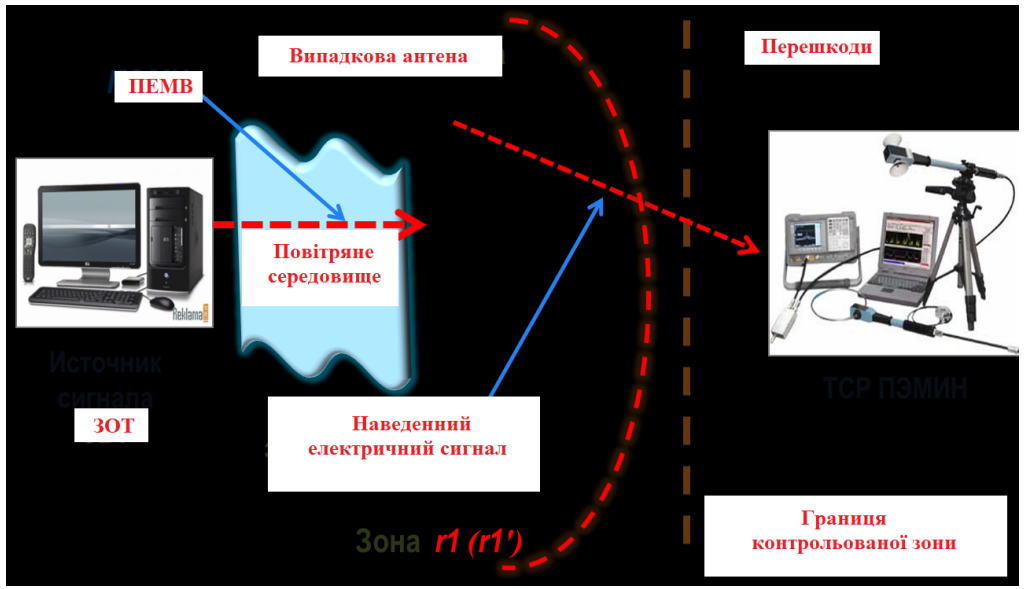
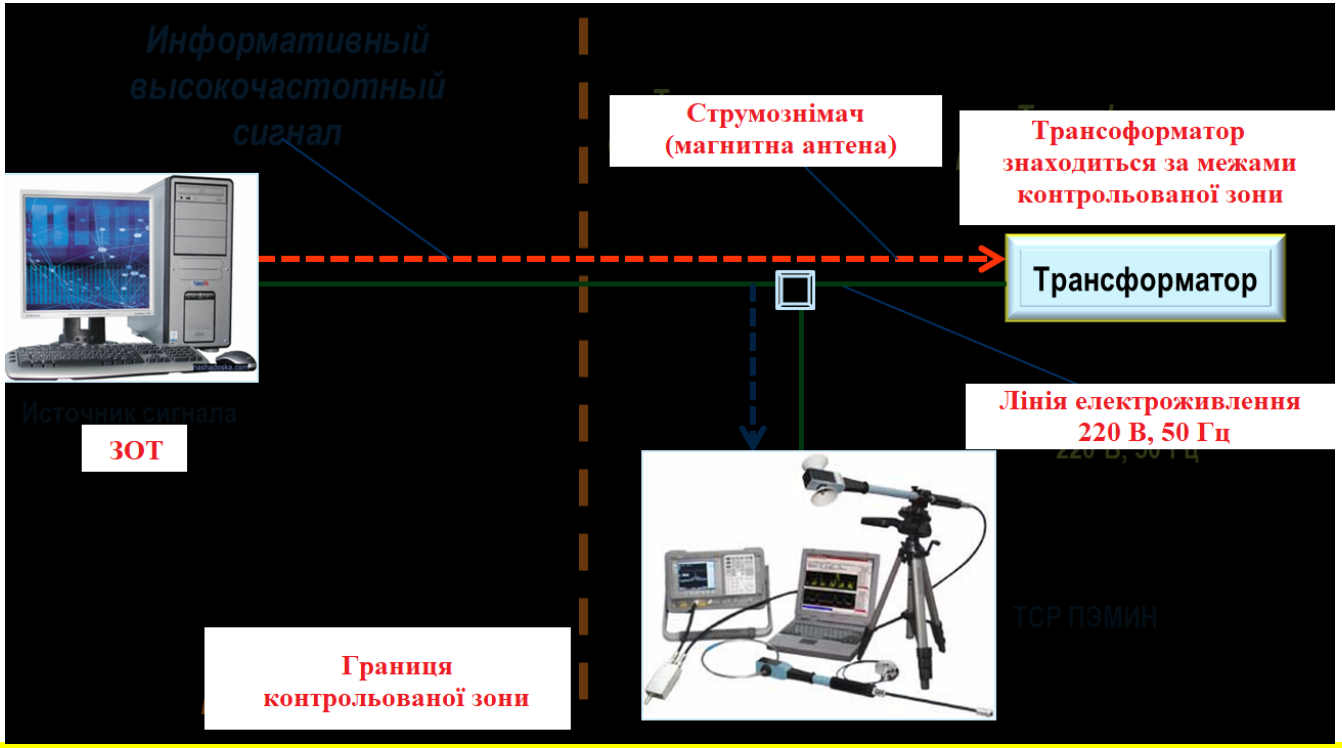


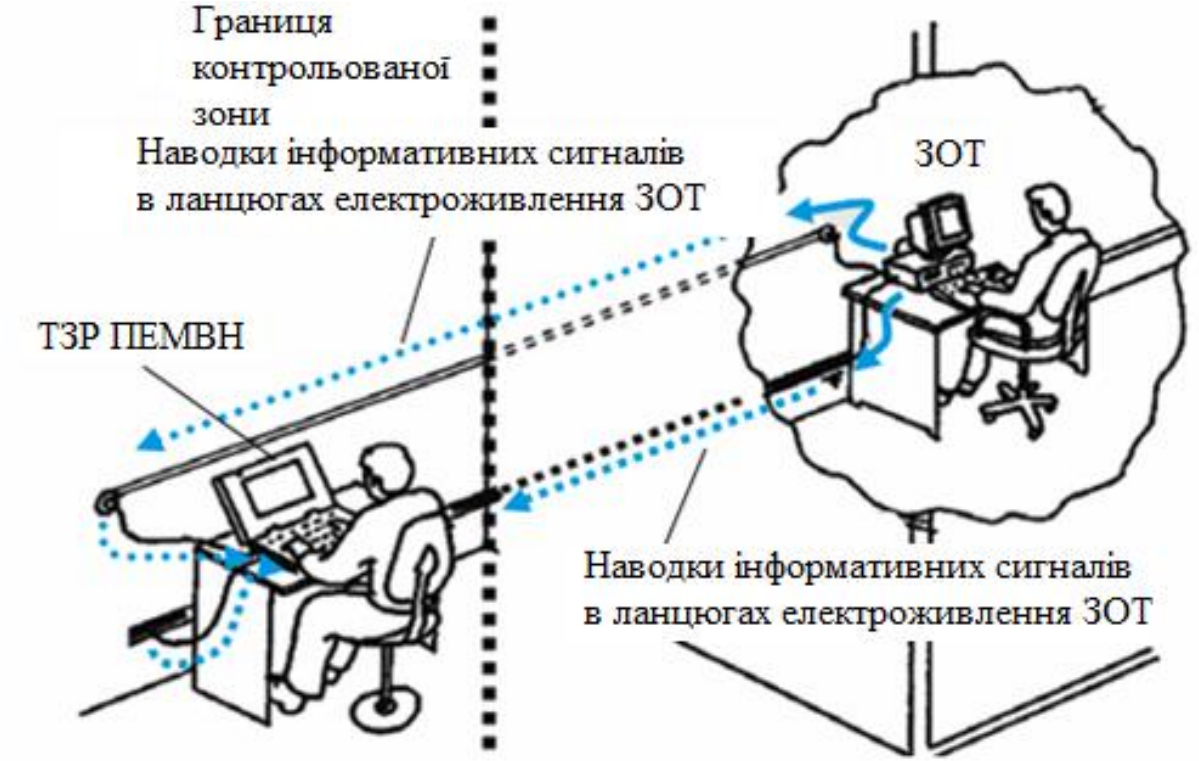
Схема ТКВІ

- Схема технічного каналу витоку інформації, що виникає за рахунок наведення інформативних сигналів у лініях електроживлення та заземлення ЗОТ:



Перехоплення ПЕМВН з ліній електроживлення та заземлення

- Перехоплення інформативних сигналів при підключенні ТЗР ПЕМВН до ліній електроживлення та заземлення ЗОТ:



Технічними засобами перехоплення ПЕМВІН є комплекси перехоплення побічних електромагнітних випромінювань ЗОТ, що складаються зі спеціальних прийомних пристроїв з дальністю перехоплення ПЕМВ від 10 до 50 метрів і спрямованої широкосмугової антени з діапазоном частот від 80МГц до 1,3 ГГц, коефіцієнтом посиленого.

Способи перехоплення інформації, що обробляється технічними засобами

Перехоплення побічних електромагнітних випромінювань

1.Перехоплення побічних електромагнітних випромінювань (магнітні та електричні антени):

- перехоплення ПЕМВ, що виникають внаслідок протікання по ТЗОІ змінного електричного струму;
- перехоплення ПЕМІ, що виникають внаслідок роботи ВЧ генераторів, що входять до складу ТЗОІ;
- перехоплення ПЕМВ, що виникають внаслідок паразитної генерації;

2.Перехоплення наведень інформативних сигналів (широкосмугові струмознімачі та пробники):

- перехоплення наведень інформаційних сигналів у сполучних лініях допоміжних технічних засобах та системах та сторонніх провідників;
- перехоплення наведень інформаційних сигналів з ліній електроживлення ТЗОІ;
- перехоплення наведень інформаційних сигналів із ланцюгів заземлення ТЗОІ.

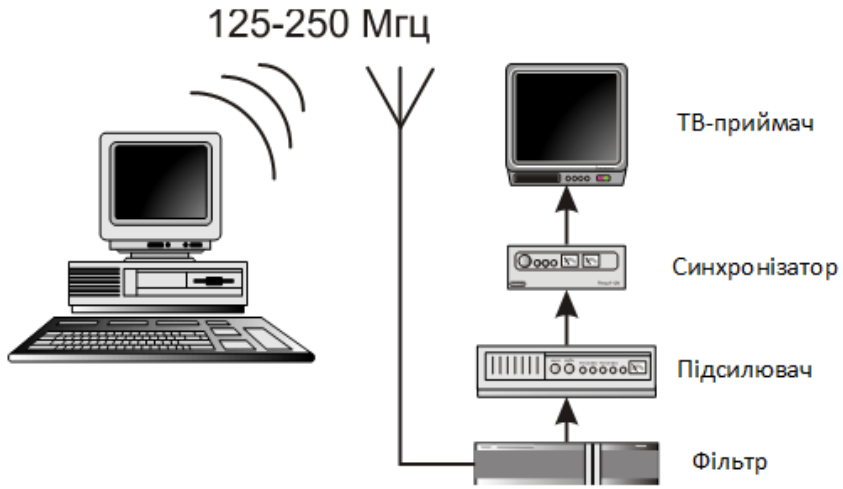
3.Перехоплення шляхом «високочастотного опромінення» ТЗОІ (спеціальна апаратура).

4.Перехоплення від впроваджених у ТЗОІ електронних пристроїв негласного знімання інформації.

Схема перехоплення інформації з ПЕОМ

Технічний контроль потенційних каналів витоку інформації

- побічні електромагнітні випромінювання в діапазоні частот від 10 Гц до 100МГц;
- наведення сигналів у ланцюгах електроживлення, заземлення та в лініях зв'язку;
- небезпечні сигнали, що утворюються за рахунок електроакустичних перетворень, які можуть відбуватися у спеціальній апаратурі контролю інформації. Ці сигнали повинні контролюватись у діапазоні частот від 300 Гц до 3,4кГц;
- Канали витоку інформації, що утворюються внаслідок впливу високочастотних електромагнітних полів на різні дроти, які знаходяться в приміщенні і можуть, таким чином, стати приймальною антеною. І тут перевірка проводиться у діапазоні частот від 20 кГц до 100 МГц.



Способи і засоби захисту інформації

Засоби і методи ЗІ

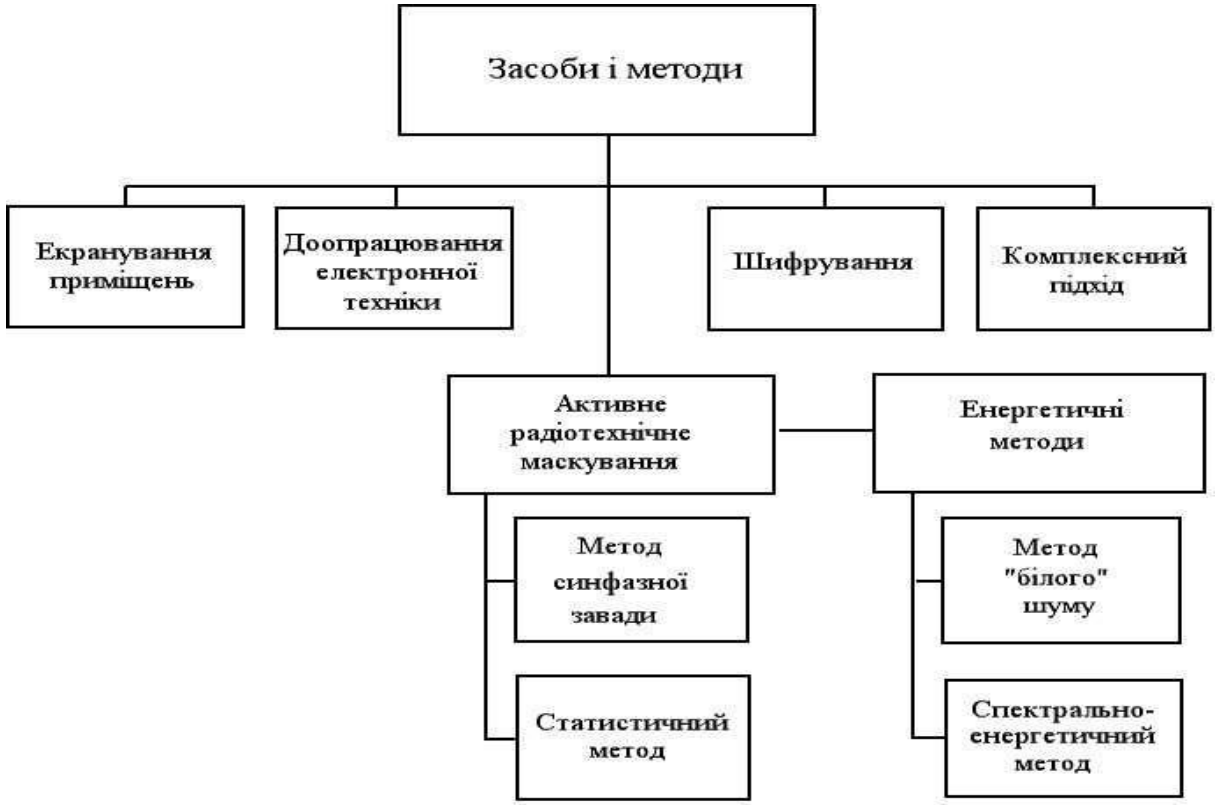


Рис. 1. Способи і методи ЗІ, що обробляється засобами електронної техніки, від витоку по радіотехнічному каналу

Екранування

- Розрізняють такі способи екранування: електростатичне, магнітостатичне та електромагнітне.
- Електростатичне та магнітостатичне екранування засновані на замиканні екраном (що володіє в першому випадку високою електропровідністю, а в другому магнітопровідністю) відповідно електричного та магнітного полів.
- Електростатичне екранування по суті зводиться до замикання електростатичного поля на поверхню металевого екрану та відведення електричних зарядів на землю (на корпус приладу).
- Заземлення електростатичного екрану є необхідним елементом для реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля. При використанні діелектричних екранів, щільно прилеглих до елемента, що екранується, можна послабити поле джерела наведення в ε раз, де ε - відносна діелектрична проникність матеріалу екрану.

Вимоги до електричних екранів

- Основні вимоги до електричних екранів можна сформулювати наступним чином:
  - конструкція екрана повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрана, не виходячи за межі;
  - в області низьких частот при глибині проникнення (δ) більше товщини (d), тобто при δ > d ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрану з корпусом пристрою і мало залежить від матеріалу екрану і його товщини;
  - в області високих частот при δ > d ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідністю та магнітною проникністю.

Магнітостатичне екранування

- Магнітостатичне екранування використовується при необхідності придушити наведення на низьких частотах від 0 до 3-10 кГц.
- Основні вимоги до магнітостатичних екранів можна звести до наступних:
  - магнітна проникність μα матеріалу екрана має бути можливо вищою. Для виготовлення екранів бажано застосовувати магнітом'які матеріали з високою магнітною проникністю (наприклад, пермалою);
  - збільшення товщини стінок екрану призводить до підвищення ефективності екранування, проте при цьому слід брати до уваги можливі конструктивні обмеження за масою та габаритами екрану;
  - стики, розрізи та шви в екрані повинні розміщуватись паралельно лініям магнітної індукції магнітного поля, їх число має бути мінімальним;
  - заземлення екрану не впливає на ефективність магнітостатичного екранування.

Вибір матеріалу екрану$_1$

- Вибір матеріалу екрана проводиться виходячи із забезпечення необхідної ефективності екранування заданому діапазоні частот при певних обмеженнях. Ці обмеження пов'язані з масогабаритними характеристиками екрану, його впливом на об'єкт, що екранується, з механічною міцністю і стійкістю екрану проти корозії, з технологічністю його конструкції і т.д.
- Таблиця 1. Коефіцієнти екранування електромагнітного поля деяких матеріалів

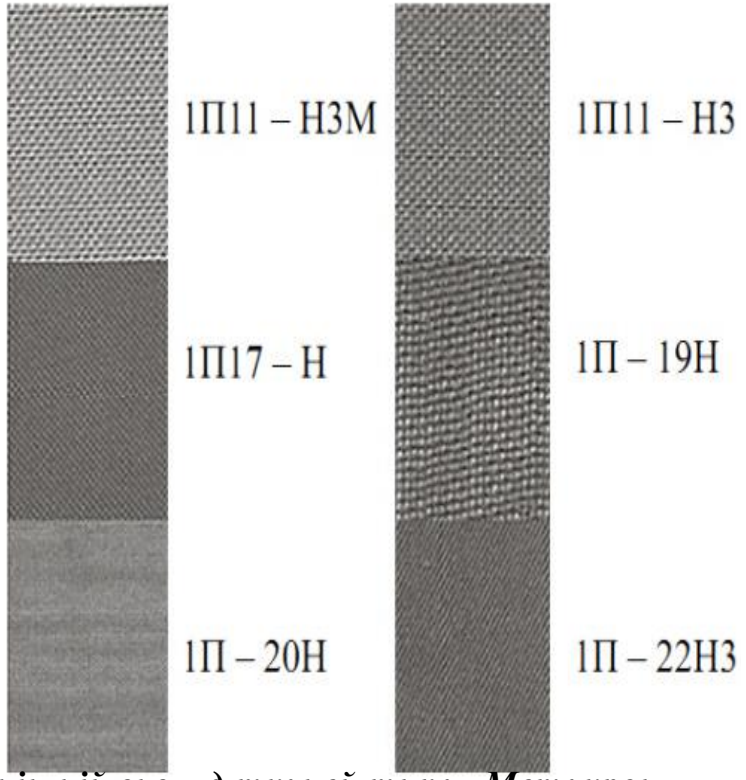
Вибір матеріалу екрану$_2$

Таблиця 1. Коефіцієнти екранування електромагнітного поля деяких матеріалів

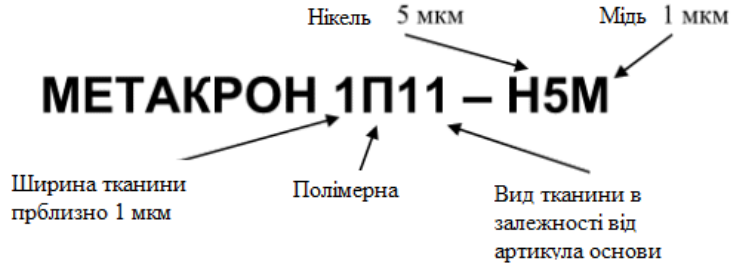
Найменування матеріалу	Товщина, мм	Діапазон частот, МГц	Коефіцієнт екранування, дБ
Листова сталь СТ-3, ГОСТ 19903-74	1,40	30-40000	100
Фольга алюмінієва, ГОСТ 618-73	0,08	30-40000	80
Фольга мідна, ГОСТ 5638-75	0,08	30-40000	80
Сітка стальна тканина, ГОСТ 5336-73	0,3-1,3	30-30000	30
Радіозахисне скло з одно- чи з двостороннім полупровідниковим покриттям, ТУ 21-54-41-73	6,0	30-30000	20-40
Тканина хлопчатобумажна з наноструктурним ферромагнитним мікропроводом		30-1000	15-40
Тканина трикотажна (поліамід + проволока), ТУ 6-06-С202-90		0,3-30000	15-40
Тканина метализована «Восход»	Товщина напилення 4-6 мкм	0,1-12000	60-80
Тканина металлизована «Метакрон», ТУ 8388-008-17310584-04	Товщина напилення 1-12 мкм	0,1-12000	50-80

Тканина «Метакрон»

- Тканини «Метакрон» мають високу відбивну здатність (понад 99,99%) у діапазоні електромагнітних випромінювань, що не іонізують. Для тканини з Ni покриттям товщиною 10 мкм ослаблення електромагнітного поля в діапазоні частот 1 МГц 10 ГГц становить від 80 до 100 дБ, з товщиною покриття 5 мкм - від 50 до 80 дБ. Ослаблення магнітного поля діапазоні частот 0,1 30 МГц становить від 5 до 60 дБ.



Зовнішній вигляд тканей типа «Метакрон»



Розшифровка марок ткинини «Метакрон»

Доопрацювання засобів $ЕТ_1$

- Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ здійснюється організаціями, що мають відповідні ліцензії. Використовуючи різні радіопоглинаючі матеріали і схемотехнічні рішення, за рахунок доопрацювання вдається суттєво знизити рівень випромінювань. Вартість такого доопрацювання залежить від радіуса необхідної зони безпеки і складає від 20 %до 70 % від вартості ПЕОМ.



ПЕОМ в спеціальному захищенному виконанні

Доопрацювання засобів ET_2

- Ланцюг, показаний на рис. 5(а), має велику площу петлі, утвореної «прямим» проводом та «землею». Цей ланцюг схильний насамперед до магнітного впливу. Екран заземлений на одному кінці та не захищає від магнітного впливу. Перехідне згасання для цієї схеми приймемо рівним 0 дБ для порівняння із загасанням схем на рис. 5 (б - і).

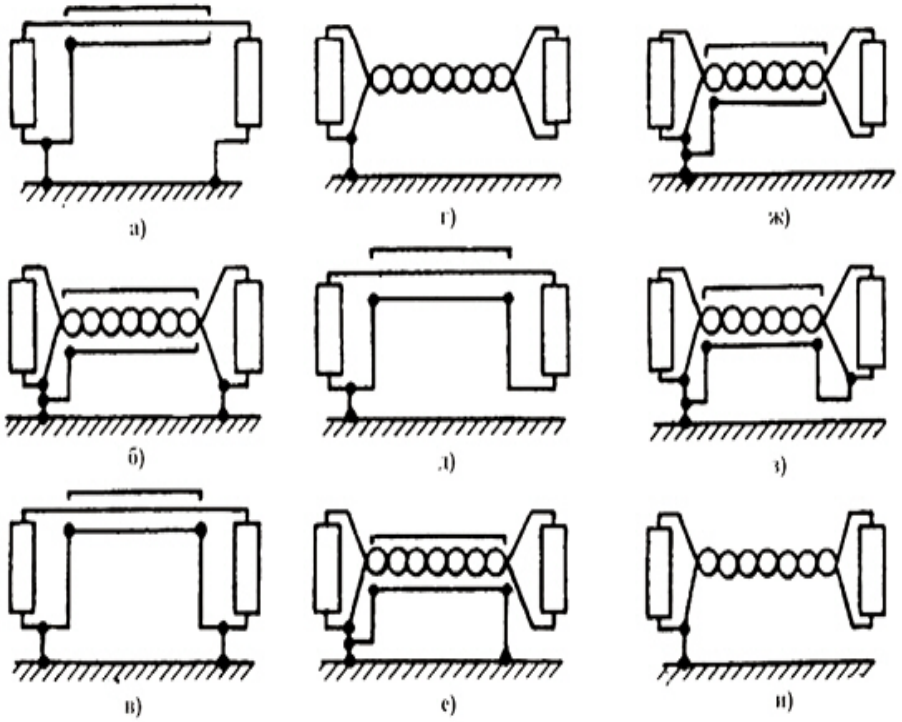


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів $ЕТ_3$

- Схема на рис. 5(б) практично не зменшує магнітний зв'язок, так як зворотний провід заземлений з обох кінців, і в цьому сенсі вона аналогічна схемою на рис. 5(а). Ступінь поліпшення можна порівняти з похибкою розрахунку (вимірювання).

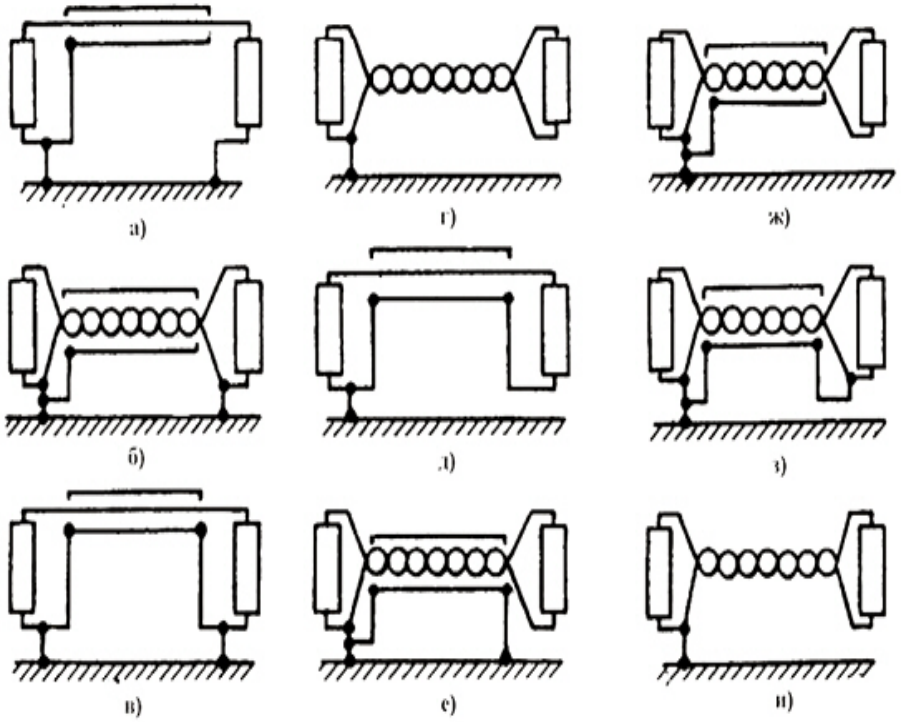


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів $ЕТ_4$

- Схема на рис. 5(в) відрізняється від схеми на рис. 5 (а) наявністю зворотного дроту -коаксіального екрану, проте екранування магнітного поля погіршено, оскільки ланцюг заземлений на обох кінцях, в результаті чого з землею утворюється петля великої площі.

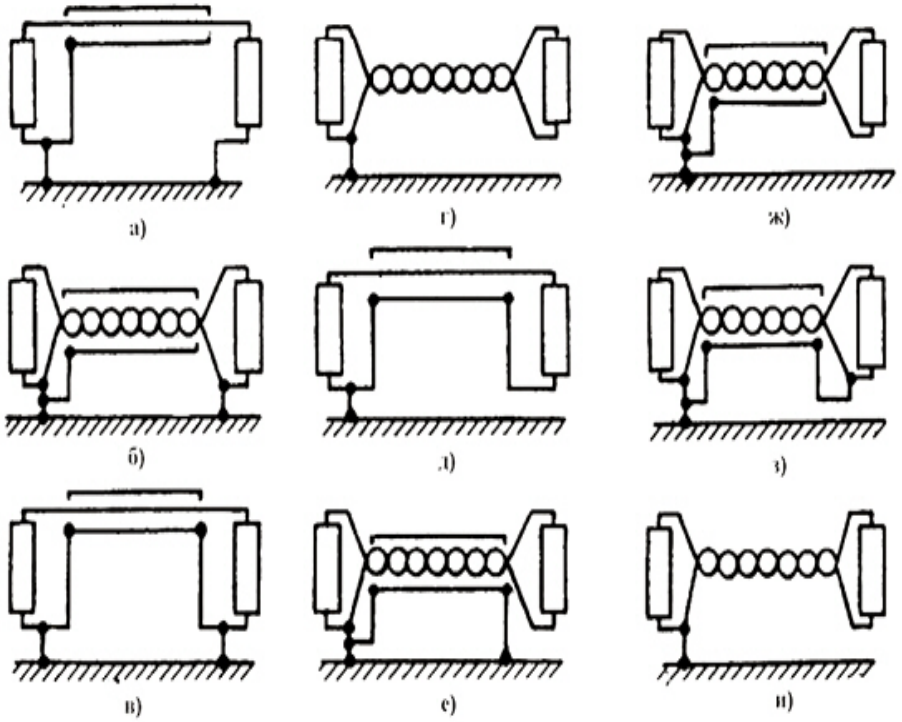


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів $ЕТ_5$

- Схема на рис. 5 (г) дозволяє суттєво підвищити захищеність ланцюга завдяки скрутці дротів. В цьому випадку (порівняно зі схемою на рис. 5 (б)) петлі немає, оскільки правий кінець ланцюга не заземлений.

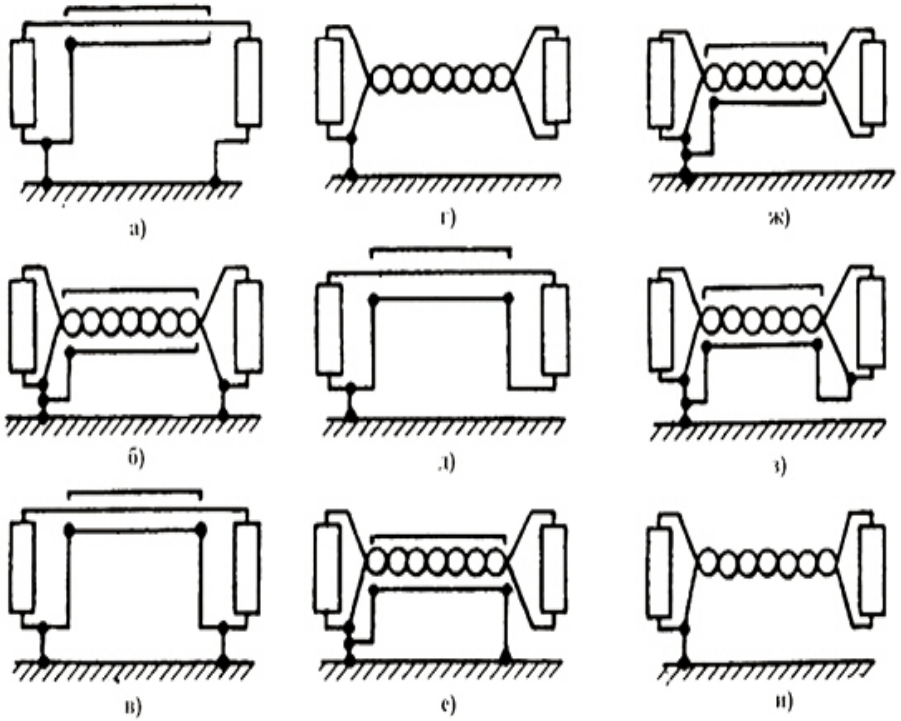


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів ЕТ$_6$

- Подальше підвищення захищеності ланцюга досягається застосуванням схеми на рис. 5 (с), коаксіальний ланцюг якого забезпечує краще магнітне екранування, ніж скручена пара на рис. 5 (г).

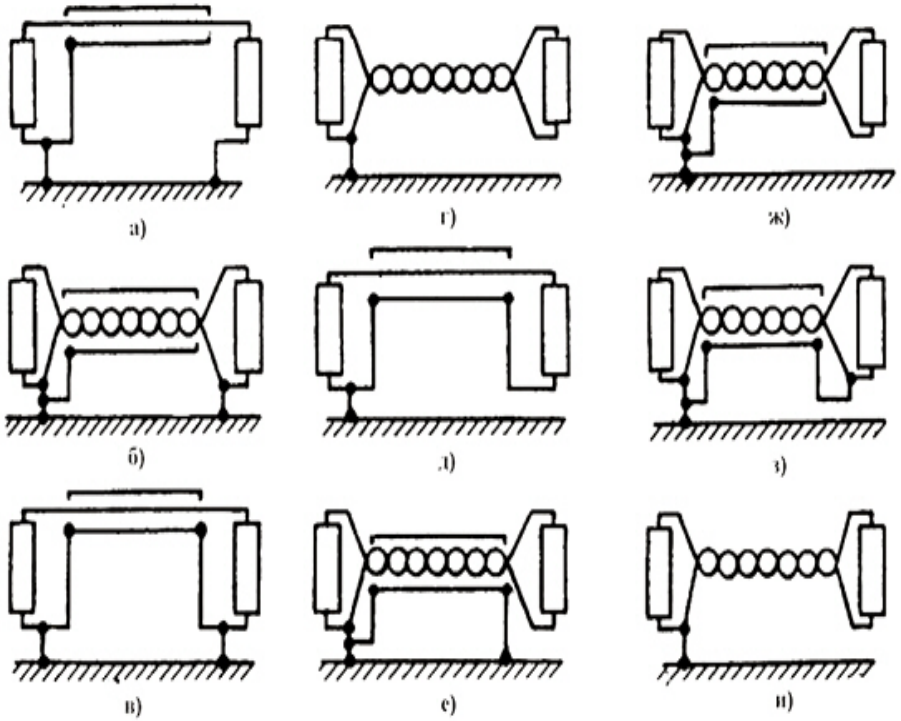


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів ET_7

- Площа петлі у схемі на рис. 5(д) не більше, ніж у схемі на рис. 5 (г), так як поздовжня вісь коаксіального екрану кабелю збігається з його центральним проводом.

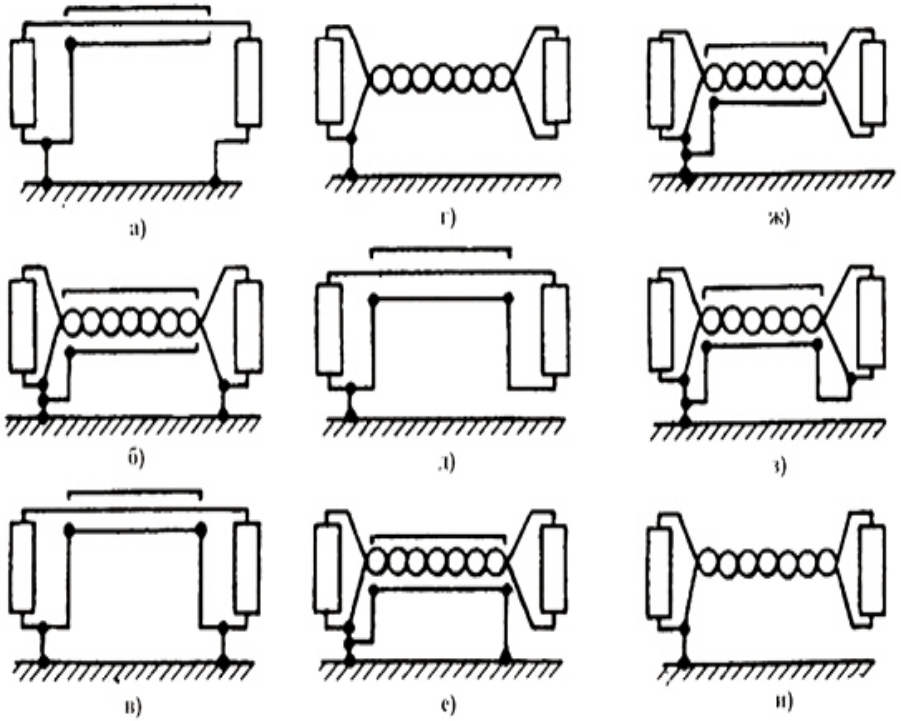


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів ЕТ$_8$

- Схема на рис. 5 (е) дозволяє підвищити захищеність ланцюга завдяки тому, що скручена пара заземлена лише на одному кінці. Крім того, у цій схемі використовується незалежний екран.

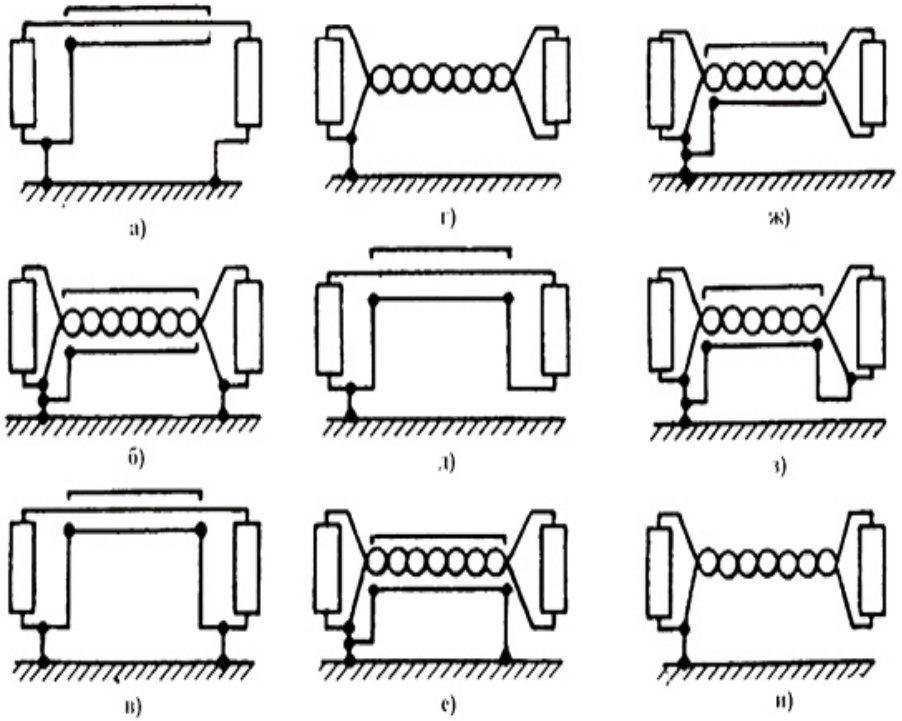


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів $ЕТ_9$

- Схема на рис. 5(ж) має ту ж захищеність, що і схема на рис. 5 (е): ефект той самий, що і при заземленні на обох кінцях, оскільки довжина ланцюга та екрана істотно менша від робочої довжини хвилі.

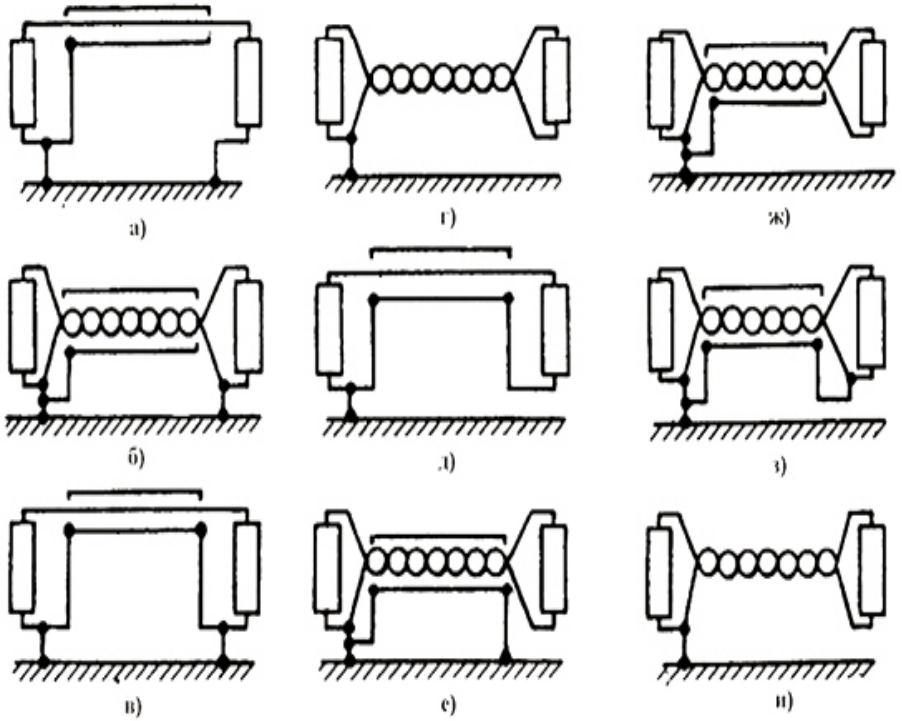


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Доопрацювання засобів ET_{10}

- Більш щільне скручування проводів (схема рис. 5 (і)) дозволяє додатково зменшити магнітний зв'язок. Крім того, при цьому зменшується електричний зв'язок (в обох проводах струми наводяться однаково).

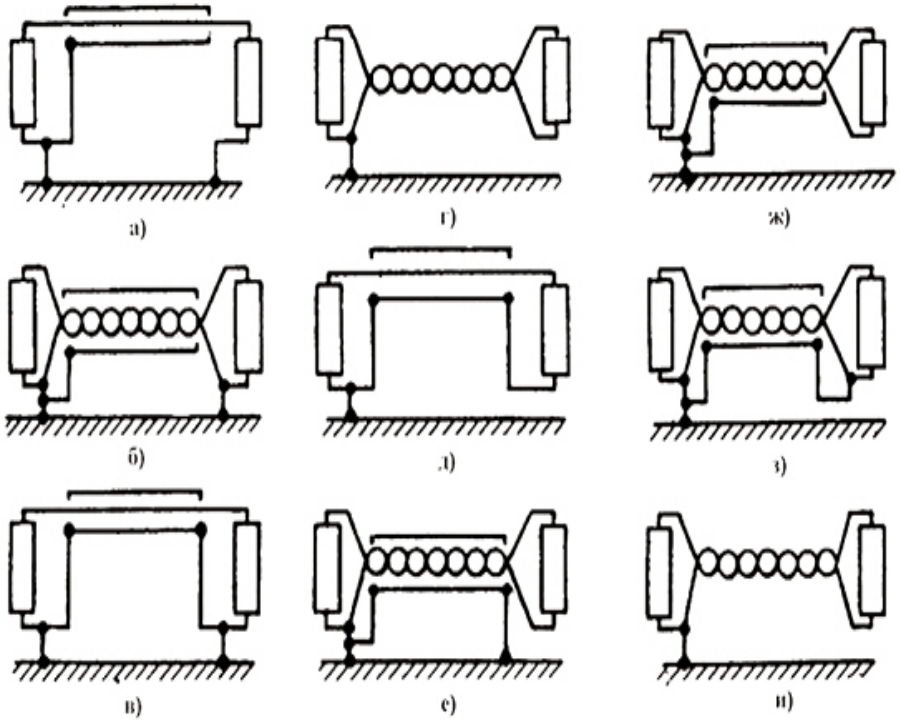


Рис. 5. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних та електричних полів:
а) 0 дБ; б) 2 дБ; в) 5 дБ;
г) 49 дБ, вита пара, 18 витків на метр;
д) 57 дБ; е) 64 дБ, схема переважна на високих частотах;
ж) 64 дБ; з) 71 дБ; і) 79 дБ, скручена пара (54 витка на метр)

Екрановані приміщення, споруди та камери

- У звичайних (неекранованих) приміщеннях основний екрануючий ефект забезпечують залізобетонні стіни будинків (табл. 2).
- Як правило, ступінь екранування звичайних приміщень невисока внаслідок наявності в них вікон, дверей та вентиляційних отворів, тому їхньому екрануванню необхідно приділяти першорядну увагу.

Таблиця 2. Ступінь екрануючої дії різних типів будівель

Тип будівлі	Ступінь екранування, дБ		
	100 МГц	500 МГц	1000 МГц
Віконний проріз 30% від площі стіни			
Цегляна будівля з товщиною стін 1,5 цегли	13-15	15-17	16-19
Залізобетонна будівля з осередком арматури 15х15 см та товщиною стін 160 мм	20-25	18-19	15-17
Віконний проріз 30 % від площі стіни, закритий металевими гратами з коміркою 5х5 см			
Цегляна будівля з товщиною стін 1,5 цегли	17-19	20-22	22-25
Залізобетонна будівля з осередком арматури 15х15 см та товщиною стін 160 мм	28-32	23-27	20-25

Екранування приміщень

- Ступінь екранування приміщення залежить від використовуваних засобів екранування і може становити від 40 до 60 дБ за наявності вікон у приміщенні та до 100 дБ за їх відсутності (табл. 3).

Таблиця 3. Гранично досяжні величини ослаблення електромагнітних випромінювань для різних типів приміщень, що екранують.

Тип конструкції екранованого приміщення	Ступінь екранування, дБ
Одиночний екран із сітки; одиночні екрановані двері, обладнані затискними пристроями; внутрішні рольставні на вікно; спеціальні електричні фільтри; фільтри для притоку та витяжки (вентиляційні).	40
Одиночний екран із металізованої тканини; одиночні екрановані двері, обладнані затискними пристроями; екрановане вікно з екранованим склом, внутрішні ролети на вікно; спеціальні електричні фільтри; фільтри для притоку та витяжки (вентиляційні).	60
Подвійний екран із сітки чи металізованої тканини; подвійна екранована дверима-тамбуром та затискними пристроями конструкція; спеціальні електричні фільтри; фільтри для притоку та витяжки (вентиляційні).	80
Суцільний сталевий екран; пневматичні екрановані двері; спеціальні електричні фільтри; фільтри для притоку та витяжки (вентиляційні).	100

Екрановані споруди

- В екранованих спорудах (камерах) встановлюються екрановані двері, технологічні отвори, системи контролю та сигналізації екранованих дверей, фільтри перешкододавлюючі (електричні, повітроводні, трубопровідні, світлові, телекомутаційні), системи вентиляції та кондиціювання, системи пожежної сигналізації, димовидалення та автоматичного пожежогасіння. (рис 6.)

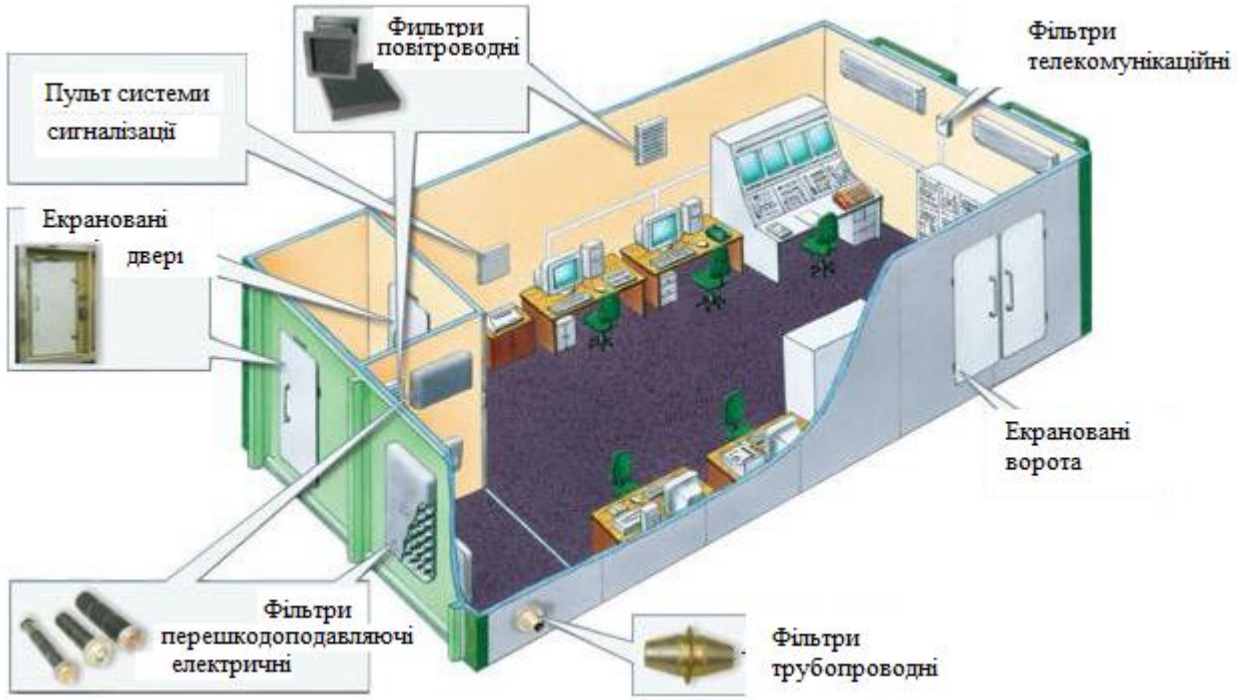


Рис. 6. Схема екранованої споруди

Екрановані двері

- Двері призначені для організації оперативного входу-виходу обслуговуючого персоналу в екрановану споруду. Вони мають контактне магнітне ущільнення і в них відсутні механічні запори та притиски, що забезпечує безпеку проходу в екстремальних умовах.
- При зачиненні екранованих дверей повинен забезпечуватись надійний електричний контакт зі стінками приміщення (з дверною рамою) по всьому периметру. Стандартні розміри дверей становлять 900х2000 мм та 1500х2000 мм. Встановлення кількох дверей через систему тамбурів у комплекті із системою сигналізації забезпечує прохід персоналу без порушення захисних функцій екранованого приміщення. Зовнішній вигляд деяких дверей екранованих представлений на рис. 7.



Рис. 7. Екрановані двері: а) без тамбуру; б) та в) з тамбуром

Завадодавні фільтри

- Фільтри завадодавні електричні (рис. 8) призначені для придушення побічних електромагнітних випромінювань і наведень (ПЕМІН) в ланцюгах електроживлення та сигналізації, а також організації введення цих ланцюгів в спорудження, що захищаються і екрановані, і приміщення. Фільтри повітроводні (рис.9а) призначені для повітрообміну внутрішнього об'єму екранованої споруди із зовнішнім середовищем з метою життєзабезпечення обслуговуючого персоналу та димовидалення, а також введення світловолоконних кабелів. Фільтри трубопровідні (рис. 9б) призначені для подачі в екрановані споруди рідин та газів.



Рис. 8. Фільтри завадодавні електричні: а) типу ФП (індуктивно-ємнісні багатопровідні); б) типу ФСПП (на основі електродинамічних сповільнюючих структур, однопровідні та багатопровідні)

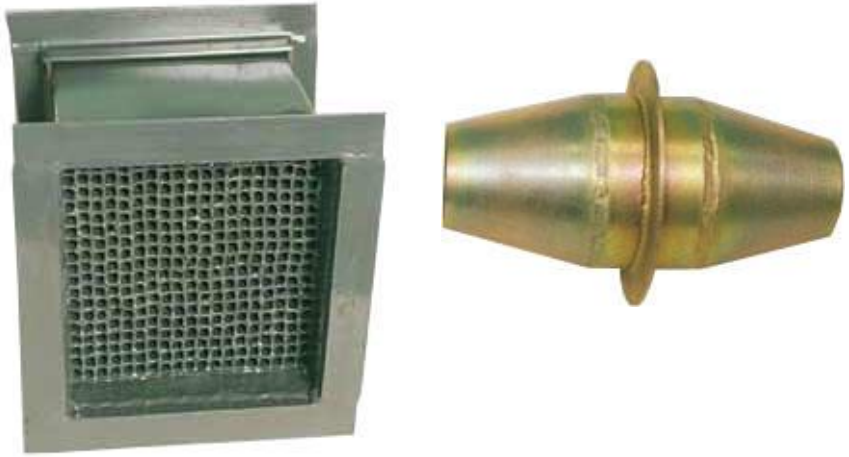


Рис.9. Фільтри: повітроводний (а) та трубопровідний (б)

Криптографічний захист$_1$

- Криптографічне закриття інформації, або шифрування, є радикальним способом її захисту. Шифрування здійснюється або програмно, або апаратно за допомогою вбудовуваних засобів.
- Такий спосіб захисту виправдовується при передачі інформації на великі відстані по лініях зв’язку. Використання шифрування для захисту інформації, що міститься у службових сигналах цифрового електронного засобу, у даний час неможливе.

КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ



Склад комплексу:

- Шифратор О371-Е(РЕ)
- Пристрій генерації ключових даних О372-Е
- Централізована система керування (ЦСК)

Шифратор О371-Е(РЕ) призначений для криптографічного захисту трафіку IP-мереж високого рівня таємності.

Використовується для захисту каналів проводового, супутникового, радіорелейного та стільникового (3G, 4G) зв’язку.

Виготовляється у варіантах для використання на стаціонарних (О371-Е) та рухомих (О371-РЕ) об’єктах.

Пристрій генерації ключових даних О372-Е призначений для генерації, зберігання та розподілу ключових даних.

Централізована система керування (ЦСК) призначена для віддаленого керування мережею шифрованого зв’язку.

Криптографічний захист$_2$

ЛАВИНА-Е

КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ



Активне радіотехнічне маскування$_1$

- Активне радіотехнічне маскування передбачає формування й випромінювання маскуючого сигналу в безпосередній близькості від засобу, що захищається. Розрізняють наступні методи активного радіотехнічного маскування.
- При енергетичному маскуванні методом “білого шуму” випромінюється широкосмуговий шумовий сигнал із постійним енергетичним спектром, що суттєво перевищує максимальний рівень випромінювання електронної техніки. У даний час найпоширеніші пристрої ЗІ, що реалізують саме цей метод. До його недоліків слід віднести створення недопустимих завад радіотехнічними та електронними засобами, що знаходяться поблизу від апаратури, що захищається.
- Спектрально-енергетичний метод полягає в генеруванні завади, що має енергетичний спектр, який визначається модулем спектральної густини інформативних випромінювань техніки і енергетичним спектром атмосферної завади. Даний метод дозволяє визначити оптимальну заваду з обмеженою потужністю для досягнення необхідного співвідношення сигнал/завада на межі контрольованої зони.

Активне радіотехнічне маскування$_2$

- Перераховані методи можуть бути використані для ЗІ як в аналоговій, так і в цифровій апаратурі. Як показник захищеності в цих методах використовується співвідношення сигнал/завада.
- Наступні два методи призначені для ЗІ в техніці, що працює з цифровими сигналами. У методі “синфазної завади” як маскуючі сигнали використовуються імпульси випадкової амплітуди, що збігаються за формою й часом існування з корисним сигналом. У цьому випадку завада майже повністю маскує сигнал, прийом сигналу втрачає сенс, оскільки апостеріорна ймовірність наявності й відсутності сигналу залишається такою, що дорівнює їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність помилки на межі мінімально допустимої зони безпеки. Проте через відсутність апаратури для безпосереднього вимірювання даної величини виконується перерахунок зазначеної величини в необхідне співвідношення сигнал/завада.

Активне радіотехнічне маскування$_3$

- Статистичний метод ЗІ полягає у зміні ймовірнісної структури сигналу, що приймається розвідприймачем, шляхом випромінювання у спеціальний спосіб формованого маскуючого сигналу. Як контрольовані характеристики сигналів використовуються матриці ймовірності зміни станів.У разі оптимальної захищеності матриці ймовірності зміни станів ПЕМВ відповідатиме еталонній матриці (всі елементи цієї матриці однакові). До переваг даного методу варто віднести те, що рівень формованого маскуючого сигналу не перевершує рівень інформативних ПЕМВ техніки. Проте статистичний метод має деякі особливості реалізації на практиці.
- Відновлення інформації,яка міститься в ПЕМВ, найчастіше під силу тільки професіоналам, що мають у своєму розпорядженні відповідне устаткування. Але навіть вони можуть бути безсилі в разі грамотного підходу до забезпечення ЗІ від витоку через ПЕМВ.

Активне радіотехнічне маскування$_4$

- Для здійснення активного радіотехнічного маскування ПЕМВ використовуються пристрої, що створюють шумове електромагнітне поле в діапазоні частот від кількох кГц до 1000 МГц із спектральним рівнем, що суттєво перевищує рівні природних шумів і інформаційних випромінювань засобів ЕОМ. Для цих цілей використовуються малогабаритні надширокосмугові передавачі шумових маскуючих коливань ГШ- 1000 і ГШ-К-1000, які є модернізацією виробу “Шатер-4”.



ГШ-К-1000



ГШ- 1000

Оцінка рівня ПЕМВ

Оцінка рівня ПЕМВ$_1$

- Оцінка рівня ПЕМВ засобів цифрової електронної техніки може здійснюватися відповідно до рівнів наступних норм і вимог:
  - санітарно-гігієнічні норми (ГОСТ 12.1.006-84);
  - норми електромагнітної сумісності (ЕМС);
  - норми і вимоги із ЗІ про витік через ПЕМВ.
- Залежно від того, відповідність яким нормам потрібно встановити, використовуються ті або інші прилади, методи й методики здійснення вимірювань.
- Слід зазначити, що норми на рівні ЕМВ з точки зору ЕМС суттєво жорсткіші за санітарно-гігієнічні норми (на кілька порядків). Очевидно, що норми, методики й прилади, які використовуються в системі забезпечення безпеки життєдіяльності, не можуть бути використані при розв’язанні задач ЗІ.

Оцінка рівня ПЕМВ$_2$

- Рівні ПЕМВ цифрової електронної техніки з точки зору ЕМС регламентовані цілим рядом міжнародних і вітчизняних стандартів(публікаціїCISPR – спеціального міжнародного комітету з радіозавад, ГОСТ 29216-91). Встановлені наступні норми напруженості поля радіозавад від обладнання інформаційної техніки (табл. 1).

Таблиця 1.

Норми напруженості поля радіозавад

Смуга частот,МГц	Квазіпікові норми,дБ(мВ/м)
30÷230	30 (31,6)
230÷1000	37 (70,8)

Рівні напруженості поля завад

- Рівні напруженості поля випромінюваних завад нормуються на відстані 10 або 30 м від джерела завад залежно від того, де експлуатуватиметься обладнання (у житлових приміщеннях або в умовах промислових підприємств).
- Основні характеристики вимірювальної апаратури, що використовується:
  - діапазон робочих частот – 9 МГц ÷ 1000 МГц;
  - можливість зміни смуги пропускання;
  - наявність детекторів квазіпікового, пікового, середнього і середньоквадратичного значень;
  - можливість слухового контролю сигналу, що має амплітудну і частотну модуляцію;
  - наявність виходу проміжної частоти і виходу на осцилограф;
  - наявність комплекту стандартних калібрувальних антен.

Прилади визначення ЕМС

Таблиця 2.

Прилади, що використовуються для визначення ЕМС

Прилад	Діапазон робочих частот, МГц	Виробник
SMV-8	26÷1000	Messelecktronik, Німеччина
SMV-11	0,009÷30	-//-
SMV-41	0,009÷1000	-//-
„Элмас”	30÷1300 ПО „Вектор”,	С.-Петербург
ESH-2	0,009÷30	RHODE&SHWARZ, Німеччина
ESV	20÷1000	-//-
ESH-3	0,009÷30	-//-
ESVP	20÷1300	-//-

Аналізатори спектра

- Для вимірювання побічних ЕМВ засобів цифрової електронної техніки можуть бути використані аналізатори спектра в комплекті з вимірювальними антенами (табл. 3).

Таблиця 3.

Аналізатори спектра

Прилад	Діапазон робочих частот, МГц	Діапазон вимірювання	Виробник
СЧ-82	$3\cdot 10^{-4}\div 1500$	1мВ÷3В СНД	
СКЧ-84	$3\cdot 10^{-5}\div 110$	70нВ÷2,2В	-//-
СЧ-85	$1\cdot 10^{-4}\div 39{,}6\cdot 10^{3}$	1мВ-3В $10^{-16}\div 10^{-2}$ Вт	-//-
РСКЧ-86	25÷1500	40нВ÷2,8В $3\cdot 10^{-17}\div 1$ Вт	-//-
РСКЧ-87	1000÷4000	$10^{-12}\div 0{,}1$ Вт	-//-
РСКЧ-90	1000÷17440	$10^{-12}\div 0{,}1$ Вт	-//-
HP8568B	$1\cdot 10^{-4}\div 1500$	$10^{-16}\div 1$ Вт	Hewlett-Packard, США
HP71100A	$1\cdot 10^{-4}\div 2900$	$10^{-16}\div 1$ Вт	-//-
HP8566B	$1\cdot 10^{-4}\div 22000$	$10^{-16}\div 1$ Вт	-//-
2756P	$1\cdot 10^{-2}\div 3{,}25\cdot 10^{3}$	$10^{-16}\div 1$ Вт	Tektronix, США
2380-2383	$1\cdot 10^{-4}\div 4200$	$10^{-18}\div 1$ Вт	Marconi Instruments, Англія

Методи оцінки інформативних ПЕМВ$_1$

- Необхідно проаналізувати й визначити характеристики небезпечних сигналів:
  - використаний код: послідовний, паралельний;
  - періодичне повторення сигналу: наявність, відсутність;
  - часові характеристики сигналу;
  - спектральні характеристики сигналу.

- Після цього можна розпочинати визначення рівнів інформативних ПЕМВ. Тут використовуються наступні методи:
  - метод оцінних розрахунків;
  - метод примусової(штучної) активізації;
  - метод еквівалентного приймача.

Методи оцінки інформативних ПЕМВ$_2$

Метод оцінних розрахунків

Визначаються елементи конструкції обладнання, в яких циркулюють небезпечні сигнали, складаються моделі, здійснюється оціночний розрахунок рівня випромінювань. Цей метод добре реалізується за наявності програмного забезпечення для ЕОМ у вигляді експертної системи, що містить банк моделей випромінювачів.

Метод примусової активізації

Активізується (програмно або апаратно) канал (одне небезпечне коло) еталонним сигналом, який дозволяє ідентифікувати випромінювання, і вимірюються рівні ПЕМВ. Для вимірювань у даному методі можуть бути використані вимірювальні приймачі і аналізатори спектра.

Метод еквівалентного приймача

Синтезується приймач для відновлення інформації, що міститься в ПЕМВ. Після калібрування такий приймач може бути використаний для вимірювання рівнів інформаційних випромінювань.

Методи оцінки інформативних ПЕМВ$_3$

- При здійсненні спеціальних досліджень необхідно вимірювати рівень ПЕМВ і розрахувати радіус зони R2, що характеризує мінімальну відстань від технічних засобів, на межі і за межами якого відношення сигнал/шум не перевищує нормованого значення (рис. 3). У загальному випадку ця відстань може знаходитися в ближній, проміжній або дальній (хвильовий) зонах.
- У межах кожної із зон згасання електромагнітної хвилі описується різними аналітичними залежностями. Для отримання об’єктивної величини слід правильно визначати межі зон.

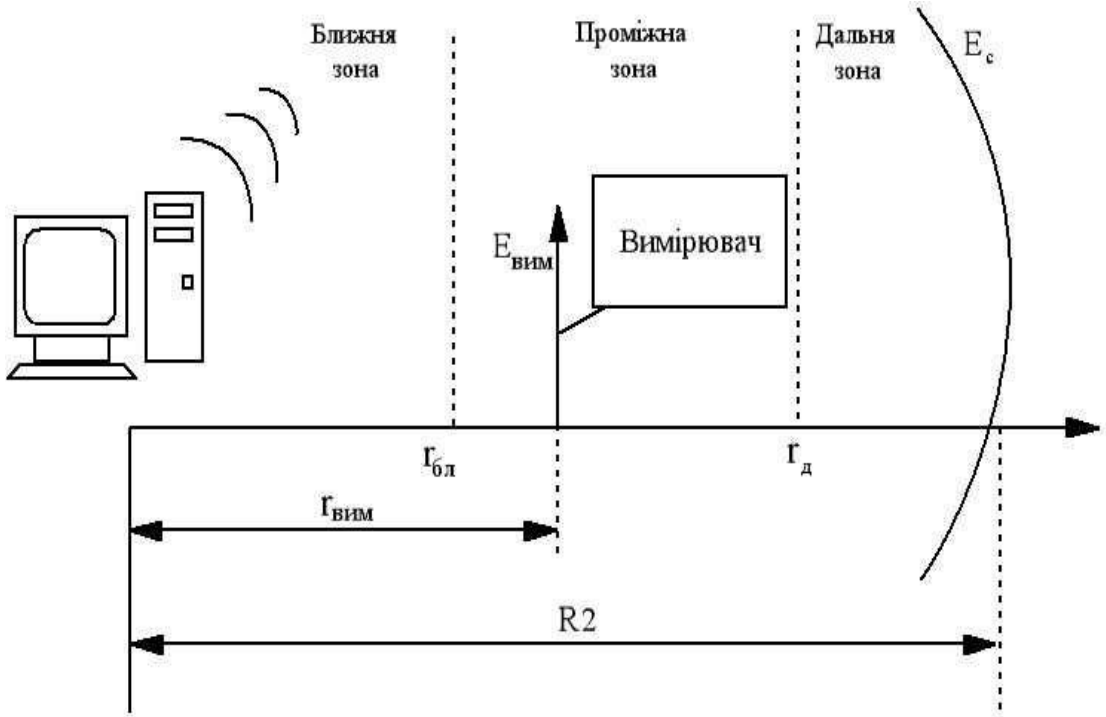


Рис. 3. Визначення радіусу зони R2

Донецький національний технічний університет



Тема 5. Розвідка та добування інформації. Лекція 12. Основи розвідувальної діяльності.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.



Лекційні питання

- Загальні положення
- Класифікація видів розвідок
- Розвідувальна діяльність
- Стратегічні принципи розвідки
- Тактичні принципи розвідки
- Адміністративно-управлінські та оперативні принципи розвідки
- Форми, методи і засоби розвідувальної діяльності

Загальні положення

Розвідка

- Спецслужба, якою є розвідка, — найважливіша і неодмінна складова частина державного механізму, політичної системи будь-якої країни, незалежно від чинного суспільно-політичного ладу, панівної ідеології.
- Таємна діяльність держав одна проти одної була завжди. Єгипетські фараони, римські і китайські імператори, грецькі і візантійські полководці та інші давні правителі активно поєднували політичні і військові методи мистецтва пригнічення і розгрому зовнішнього і внутрішнього ворога з використанням сил, засобів і прийомів розвідки та контррозвідки.





Розвідувальна діяльність$_1$

- Розвідувальна діяльність, за своїми характерними рисами визначається як таємна, конспіративна, прихована, негласна діяльність, яка призначена для здійснення «делікатних» заходів, пов’язаних з порушенням загальноприйнятих моральних, етичних, правових норм, виходом за межі правомірної поведінки, а також в окремих випадках навіть злочинними діями.



Розвідувальна діяльність$_2$

- Загальновідомо, що політика виникла у світі разом із появою держави, а разом із політикою з’явилася і розвідувальна діяльність, яка може проводитися на:

→ на міжнародному (міждержавному) рівні: іноземна держава, організація, регіон або у глобальному світовому масштабі.

→ внутрішньодержавному рівні, тобто в різних територіальних межах — держава, регіон, область, місто, селище тощо;

Тому розвідувальну діяльність можна визначити як специфічний різновид суспільно-політичного, політичного і правового явищ.

Розвідка$_1$

- Основні значення терміну «розвідка»:

→ засіб таємного отримання інформації про те, що свідомо приховується;

→ добування, збір, обробка та вивчення даних про воєнно-політичну обстановку в окремих країнах і коаліціях, їх збройні сили, воєнно-економічний потенціал, склад, положення, характер дій;

→ спецслужба, що сприяє здійсненню зовнішньополітичного курсу держави, зміцненню безпеки, обороноздатності, економіки країни .



Розвідка$_2$

- ПО-ПЕРШЕ, розвідка не може займатися тільки «таємницями», або навпаки, винятково відкритою інформацією, що комусь уявляється політкоректністю. Державам також необхідно зберігати і захищати свої таємниці, а значить, потрібні фахівці, які вміють це робити. Отже, робоче визначення поняття «розвідка» повинне включати аспект таємності.



Розвідка$_3$

- ПО-ДРУГЕ, розвідка для політиків відрізняється від розвідки для інших осіб, які відповідальні за ухвалення рішень і працюють в конкурентному середовищі, позаяк розвідка в інтересах держави — це питання «життя і смерті», її успішності чи неуспішності, конкурентності, здатності реалізувати національні інтереси.
- Це пояснює, чому саме явище розвідки пов’язане із становленням національних держав. Народження розвідки належить до тих далеких часів, коли суверенні держави розпочали боротьбу за контроль над територією і населенням (коли почалося переслідування і покарання зрадників).



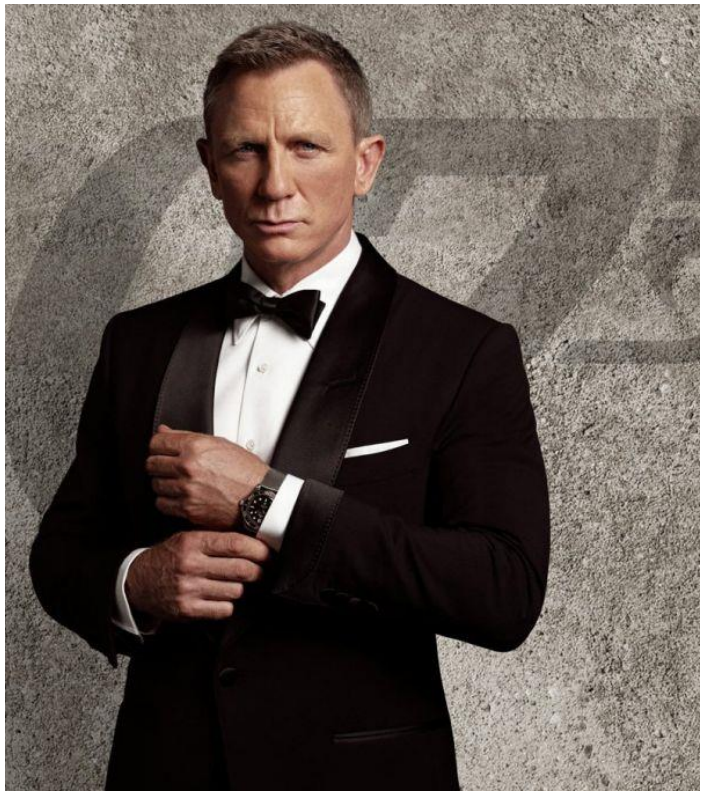
Розвідка$_4$

- ПО-ТРЕТЄ, поняття «розвідка» включає як таємну інформацію, так і нетаємну, як нелегальну діяльність (таємні операції), так і легальну.



Розвідка$_5$

- Отже, дослідники спецслужб можуть надати таке визначення терміну «розвідка»:
  - **розвідка** — це широке поняття, яке охоплює цілу низку видів діяльності від збирання інформації до її аналізу і надсилання кінцевого продукту у вигляді розвідувальної інформації (знання) до споживачів, що здійснюється таємно та спрямоване на підтримку і зміцнення національної безпеки шляхом запобігання реальним або потенційним загрозам в результаті своєчасного здійснення превентивної політики або стратегії.



Класифікація видів розвідок

Види розвідки за призначенням$_1$

- **Політична розвідка** — державний інститут, призначений добувати інформацію про функціонування як своєї, так і інших політичних систем та їхніх структурних елементів. Інше формулювання — тип розвідувальної діяльності, об’єктом якого є політичні сили, засоби, плани і таємниці супротивника, а також його відомості внутрішньополітичного та зовнішньополітичного характеру, що не охороняються.



Види розвідки за призначенням$_2$

- **Воєнна розвідка** (англ. Military intelligence, також Defense/Defence intelligence) — комплекс заходів воєнного відомства держави з отримання і обробки даних про діючого або вірогідного супротивника, його військові ресурси, бойові можливості та уразливість, а також про театр військових дій.



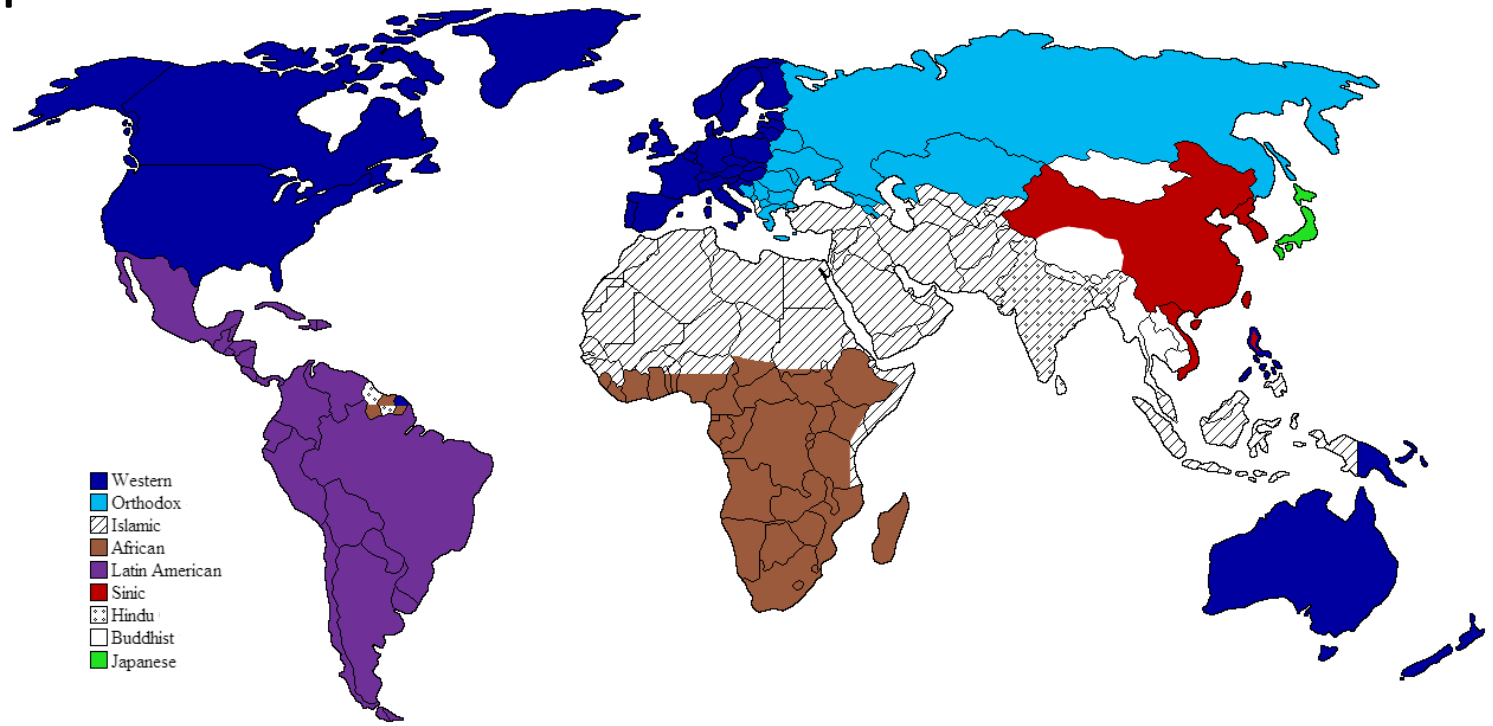
Види розвідки за призначенням$_3$

- **Економічна розвідка** — вид зовнішньої розвідки, об’єктами якої є промисловість, транспорт, торгівля, фінансові і грошово-кредитні системи, природні ресурси і т. п. країни, яку розвідують.



Види розвідки за призначенням$_4$

- **Геополітична розвідка** — вид зовнішньої розвідки щодо визначення впливу геополітичних факторів на зовнішню політику держави.



Види розвідки за призначенням$_5$

- **Науково-технічна розвідка** — розвідувальну діяльність, об’єктами якої є закордонні науково-технічні розробки і досягнення.



Види розвідки за масштабами завдань$_1$

- **Стратегічна розвідка** — добування даних про стратегічний потенціал та стратегічні наміри, стан, склад, дислокацію збройних сил ймовірного або дійсного супротивника, на різних театрах воєнних дій.
- Впливає на вироблення стратегії держави, її погляди на характер і способи ведення війни, воєнно-економічний потенціал, стан і перспективи розвитку збройних сил, озброєння і воєнної техніки, заходи щодо безпосередньої підготовки до війни і плани її ведення, обладнання тощо, необхідних для підготовки країни до оборони й успішного ведення війни і стратегічних операцій. Організовує її вище воєнне керівництво, здійснює орган воєнної розвідки держави, ведеться вона безперервно за мирного і воєнного часу.



Види розвідки за масштабами завдань$_2$

- **Оперативна розвідка** — добування розвідувальних даних, необхідних для підготовки і проведення операцій.
- Організовують командувачі і штаби оперативних об’єднань видів збройних сил з метою добування даних про супротивника і театр військових дій, необхідних для успішного ведення операцій і найбільш ефективного застосування в них усіх родів військ (сил). Здійснюють розвідувальні органи і підпорядковані сили і засоби розвідки.
- Найважливіші завдання оперативної розвідки — розкриття задумів і планів супротивника, складу, розташування і дій його головних угруповань військ (сил) в смузі дій об’єднань і на флангах, виявлення нових засобів і способів збройної боротьби супротивника.



Види розвідки за масштабами завдань$_3$

- **Тактична розвідка** — добування розвідувальних даних, необхідних для підготовки і успішного ведення бою.
- Організовують командири і штаби з’єднань, частин і підрозділів, начальники родів військ (сил), спеціальних військ і служб з’єднань і частин усіх видів збройних сил з метою правильного планування і успішного ведення бою. Основні завдання тактичної розвідки — виявлення складу, озброєння, характеру дій і угрупування військ (сил) супротивника, розкриття його задумів.



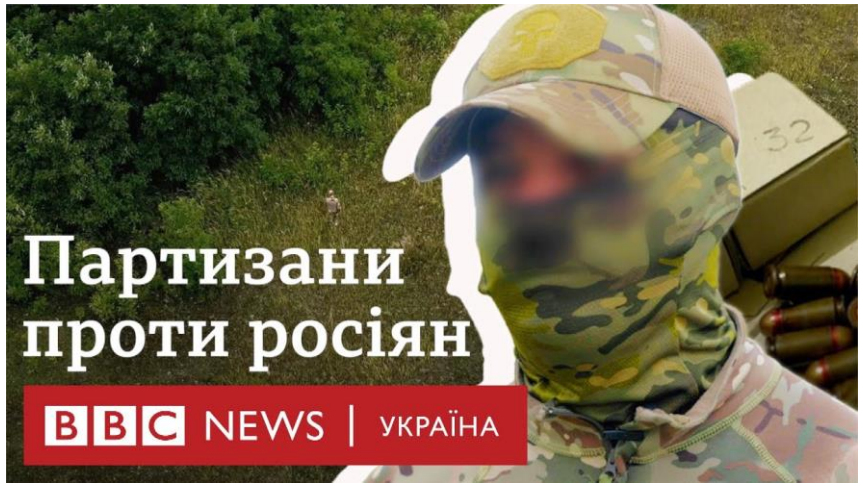
Види розвідки за завданнями, силами, засобами і способами$_1$

- **Агентурна розвідка** — добування відомостей про стан збройних сил, воєнно-економічний потенціал і мобілізаційні можливості противника, за допомогою агентурної мережі — спеціально завербованих нелегальних таємних агентів, а також розвідників, які діють під «дипломатичним прикриттям».
- Основне завдання агентурної розвідки — отримання доступу до найбільш важливих секретів, об'єктів, збирання відомостей, добування документів, зразків виробів, які неможливо придбати неагентурним шляхом. Ведеться як в мирний час, так і з початком військових дій.



Види розвідки за завданнями, силами, засобами і способами$_2$

- **Спеціальна розвідка** — вид оперативної (воєнної) розвідки збройних сил, який являє собою сукупність заходів, що проводять штаби об’єднань і з’єднань, частини та підрозділи спеціального призначення з метою здобування відомостей про супротивника, проведення спеціальних заходів на його важливих об’єктах, а також організації партизанського руху.
- Ведеться в загрозливий період і з початком військових дій. У своїй діяльності поєднує методи військової та агентурної розвідки. На спеціальну розвідку можуть покладатися завдання щодо силових акцій, диверсій, саботажу у відповідний період.



Види розвідки за завданнями, силами, засобами і способами$_3$

- **Технічна розвідка** — організація розвідувальної діяльності, що заснована на застосуванні технічних засобів.
- Залежно від природи сигналів, які сприймаються технічними засобами, виділяються такі види технічної розвідки:
  - засновані на перехопленні електромагнітних хвиль (радіоелектронна) — радіорозвідка, радіотехнічна розвідка, радіолокаційна розвідка і телевізійна розвідка;
  - засновані на перехопленні світлових хвиль (видова) — фоторозвідка і інфрачервона розвідка;
  - заснована на перехопленні звукових хвиль — акустична розвідка;
  - заснована на сприйнятті сейсмічних хвиль — сейсмічна розвідка;
  - заснована на перехопленні випромінювання при розпаді радіоактивних елементів — радіаційна розвідка.



Види розвідки за завданнями, силами, засобами і способами$_4$

- **Військова розвідка** — найважливіший вид бойового забезпечення військ, вид оперативно-тактичної і тактичної розвідки, що організується командирами та штабами в інтересах загальновійськових об’єднань, з’єднань, частин та підрозділів з метою здобування відомостей про супротивника.
- Вона полягає у здобуванні, збиранні та узагальненні відомостей про бойовий склад, положення, стан угруповань військ супротивника, характер його дій і наміри, сильні та слабкі сторони, а також ступінь та характер інженерного обладнання займаних ним районів та позицій, системи загороджень, нові засоби боротьби та способи дій в бою.



Види розвідки за територією дій

- **Внутрішня розвідка** — збирання відомостей про злочинну діяльність у своїй країні (англ. domestic intelligence, criminal intelligence). У деяких країнах це поняття охоплюється термінами «оперативно-розшукова діяльність», «контррозвідувальна діяльність».
- **Зовнішня розвідка** — збір відомостей про іноземні держави і про те, що відбувається на їх території. До зовнішньої розвідки належить і зовнішня контррозвідка, об'єктами якої є розвідувальні служби іноземних держав, добування відомостей про їх діяльність, добування відомостей про міжнародні терористичні організації, про міжнародну організовану злочинність тощо.
- **Партизанська розвідка** — це комплекс спеціальних заходів і дій зі здобування розвідувальної інформації у зоні відповідальності партизанського підрозділу, її первинної обробки і доведення в інтересах підготовки і проведення операцій (бойових дій) як для виконання завдань на окупованої території, так і для збройних сил країни, з використанням способів, форм і методів агентурної, військової і спеціальної розвідки, вчинення диверсій і саботажу на окупованій, анексованій або зайнятій супротивником території.

Розвідувальна діяльність

Розвідувальна інформація

- Розвідувальна інформація (англ. військ. Intelligence information, дипл. Surveillance information):
  - усні та зафіксовані на матеріальних носіях (зокрема у зразках виробів і речовин) відомості, які неможливо отримати офіційним шляхом, про реальні та потенційні можливості, плани, наміри і дії іноземних держав, організацій та окремих осіб, що загрожують національним інтересам своєї держави, а також про події і обставини, що стосуються національної безпеки і оборони;
  - відомості про інші держави (партії, організації, установи тощо), що добуваються розвідкою та частково контррозвідкою або під їх керівництвом іншими державними та приватними організаціями та особами відповідно до розвідувальних завдань;
  - дані про цілі, плани, дії, реальні і потенційні можливості іноземних держав, організацій і осіб, які спрямовані проти національних інтересів, а також про інші явища і обставини, пов’язані з державною безпекою;
  - дані про реальні чи потенційні можливості, дії, плани чи наміри іноземних держав, організацій та осіб, які викликають чи спроможні викликати зовнішні загрози, фактори ризику чи небезпеку для держави, а також інші дані для забезпечення національної безпеки.

Характеристики інформації

- При доборі необхідної інформації обов’язково слід враховувати такі характеристики (параметри) інформації:

Кількісні показники: повнота, достатність, обсяг.

Якісні показники: актуальність, адекватність, об’єктивність, корисність, доступність, своєчасність, точність, можливість перевірки.

Ціннісні показники: цінність (значимість, важливість, потрібність інформації для прийняття рішення), вартість (ціна).

Дані, інформація, знання

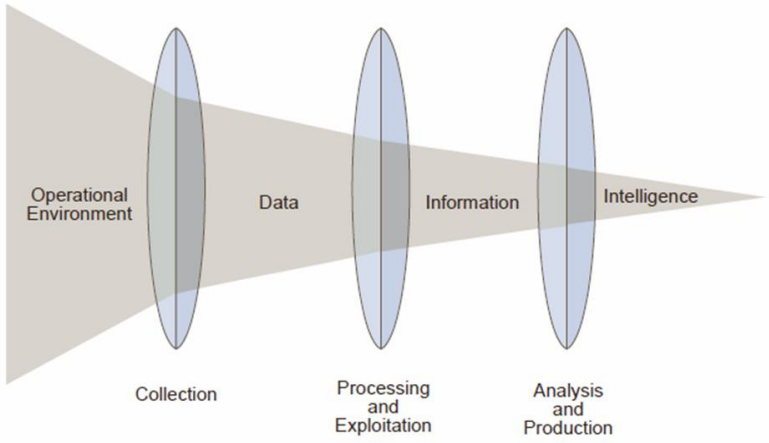
- Слід розрізняти поняття «дані», «інформація» і «знання».
  - **Дані** засновані на фактах. Це може бути статистика, уривки інформації про все те, що становить оперативний інтерес. Ніхто не може дійти правильного висновку, виходячи тільки з даних, незалежно від того, наскільки вони точні або значні.
  - **Інформація**, навпаки, це певна сукупність даних, які були відібрані, оброблені і проаналізовані, після чого їх можна використовувати для подальших дій.
  - А вже вироблені на основі аналізу і синтезу інформації пропозиції і рекомендації для прийняття рішення становлять кінцевий інформаційний продукт — **знання**. Особі, що ухвалює рішення, потрібні саме знання, у крайньому разі — інформація, а не просто дані.



Розвідувальна діяльність

- Розвідувальна діяльність полягає в добуванні та обробці інформації стосовно життєво важливих інтересів держави щодо реальних і потенційних можливостей, дій, планів і намірів іноземних держав, організацій та осіб, а також у сприянні в реалізації заходів, що здійснює держава в інтересах забезпечення її безпеки.
- В Україні законодавчо визнано, що **розвідувальна діяльність** — це діяльність, яка ведеться спеціальними засобами і методами з метою забезпечення визначених законом органів державної влади розвідувальною інформацією, сприяння реалізації та захисту національних інтересів, протидії за межами України зовнішнім загрозам національній безпеці України.

Relationship of Data, Information and Intelligence



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Способи отримання розвідувальної інформації

- Найчастіше в розвідувальній діяльності застосовуються шість основних способів отримання розвідувальної інформації:
  - **розвідка з відкритих джерел (OSINT)** — публічно доступна інформація, яка з'являється в джерелах, що не мають грифів таємності або обмежень доступу;
  - **агентурна розвідка (HUMINT)** — найстаріший спосіб збору інформації від її носіїв — інформація, зібрана з людських джерел;
  - **видова розвідка (IMINT)** — представлення об'єктів, що відтворюються в електронному або оптичному засобі на плівці, електронних дисплеях або інших носіях;
  - **радіоелектронна розвідка (SIGINT)** — перехоплення сигналів, чи то між людьми, між машинами або комбінацією обох;
  - **інструментальна розвідка (MASINT)** — розвідка фізичних полів, наукова і технічна розвідувальна інформація, що використовується для визначення, виявлення та опису специфічних ознак конкретних цілей;
  - **геопросторова розвідка (GEOINT)** — зображення та геопросторові дані, створені за допомогою інтеграції зображень та географічної інформації

Цінність розвідданих

- Розвідувальні дані, отримані з різних джерел, можуть представляти для кінцевого користувача різні інтерес і ступінь важливості, тобто мати різну цінність, а інформація з відкритих джерел іноді може своєю цінністю перевершувати секретну інформацію.
- Під загальною цінністю розвідданих розуміють такі їх аспекти, як:
  - швидкість доступу,
  - об’єми,
  - якість,
  - ясність,
  - легкість подальшого використання і
  - вартість отримання.

Швидкість доступу

- Коли в якій-небудь точці планети вибухає криза, а можливості розвідки в цьому регіоні дуже обмежені, то і аналітики розвідслужб, і структури, що формують політику держави, найчастіше звертаються за поточною інформацією в Інтернет.
- Події, що нестримно розвиваються, в моменти криз найзмістовніше відбиваються в поточних новинах, тому за падінням Берлінської стіни, скажімо, і у Вашингтоні, і в штаб-квартирі ЦРУ в Ленглі стежили не за зведеннями розвідслужб, а припавши до екранів телевізорів, з репортажів CNN з місця подій.



Об’єм

- У світі завжди буде набагато більше всіляких блогерів, журналістів, незалежних експертів, телерепортерів та інших обізнаних людей, ніж кадрових розвідників, кількість яких може дозволити собі мати будь-яка спецслужба.
- Два-три професійних розвідника з хорошою агентурною мережею, безперечно, можуть перевершувати і сотню репортерів за можливостями доступу до секретів.
- Проте, як показує досвід, грамотно зібрані фрагменти інформації з відкритих джерел за своєю сукупною значимістю можуть бути цілком еквівалентні, а іноді і перевершити суто секретні розвідувальні звіти.



Якість

- У роботі розвідслужб будь-якої країни раз у раз бувають ситуації, коли кадрові співробітники готують свої звіти на основі отриманої від таємних агентів інформації, що умисне сфабрикована або просто переписана з повідомлень ЗМІ та прикрашена для видимої важливості.
- В порівнянні з такими «розвідданими» звичайна інформація з відкритих джерел виявляється більш прийнятною вже тому, що не «замазана брехнею агентів».



Достовірність

- Для аналітиків розвідки і політичних архітекторів серйозну проблему становить невизначена міра достовірності здобутої інформації, навіть якщо вона отримана через агентурні джерела. Наприклад, коли співробітник Аналітичного управління ЦРУ читає доповідь про іноземного лідера, складену на основі відомостей від «джерела з неперевіреною надійністю», то більш-менш ясно, як цей документ слід сприймати. Проблема стає куди складніше, якщо цікавий звіт складений за даними від «надійного джерела».
- Принципово важливо, ким саме являється це джерело: міністром в кабінеті лідера, братом міністра, або ж коханкою брата дружини міністра? Аналітик в Ленглі, як правило, ніколи не знає відповідь на це запитання, тому що співробітники Оперативного управління (DO) ЦРУ ретельно оберігають свої джерела і методи отримання інформації. Отже, якщо у разі OSINT надійність джерел відкритої інформації буває як ясною, так і неясною, то у випадку з таємно здобутими даними світу їх надійності для аналітиків неясна майже завжди.

Легкість використання

- Будь-які таємниці прийнято оточувати бар’єрами з грифів секретності, принципів ізоляції інформації і особливих режимів доступу.
- Усе це робить надзвичайно непростим не лише процес передачі здобутих відомостей в політичні структури, що приймають рішення, але і поширення важливих даних серед колег-розвідників або суміжників з контррозвідки, не кажучи вже про поліцію. Що ж до даних OSINT, то зрозуміло, що їх можна легко передавати в будь-які зацікавлені інстанції.



Вартість

- Супутник видової розвідки, що розробляється, запускається і підтримується в працездатному стані на орбіті за рахунок витрат в мільярди доларів, може надати фотографії того, як виглядає дах військового заводу або корпус нового підводного човна.
- З іншого боку, в правильно вибраному іноземному журналі з ціною річної підписки близько сотні доларів можна знайти фотографії, зняті в цехах заводу, що цікавить, або усередині тієї ж самої нової субмарини.



Розвідувальний цикл (процес)

- Згідно з загальноприйнятими підходами розвідувальний цикл (процес) включає в себе шість основних елементів:
  - планування і націлювання — визначення завдань розвідці, підготовка плану збору інформації, доведення завдання до виконавців і контроль за ходом виконання;
  - збір — добування інформації і її передача;
  - обробка — первинна обробка зібраної інформації, надання їй певної форми;
  - оцінка — узагальнення, систематизація та аналіз, всебічна оцінка і інтерпретація всіх наявних даних відповідно до вимог споживача;
  - поширення інформації;
  - отримання висновків, рекомендацій, зворотна реакція споживача, та в разі необхідності, уточнення на дорозвідку.

Стратегічні принципи розвідки

Випередження супротивника

- Розвідка передусім повинна своєчасно виявляти загрози.
- Цей принцип розвинув і вдосконалив Черчилль — розвідка повинна постійно перебувати в стані війни.



Обізнаність

- Знання — сила (значення обізнаності).
- «Знай свого супротивника — або помри».



Взаємодія та координація

- Розвідка, якщо вона прагне бути ефективною, повинна з особливою увагою організовувати взаємодію і координацію наявних в її розпорядженні сил та засобів. На сьогодні вважається, що узгодженість спільних зусиль і взаємодія всіх суб’єктів, задіяних у вирішенні конкретного розвідувального завдання, є вирішальним фактором для досягнення перемоги над супротивником.



Фінансування

- Розвідка — механізм витратний і дорогий. Прямої фінансової вигоди за великим винятком не приносить.
- Дешева розвідка — це такий же нонсенс, як дешева медицина, заощаджувати на розвідці — означає заощаджувати на «здоров'ї» державного механізму і ефективності існування держави.



Об’єктивність

- Потребує вивчення об’єктів розвідки на основі всебічно перевірених фактів, зіставлення одного з одним. Однією з найбільш важливих вимог до розвідки визнається здатність не піддатися природному тяжінню до переоцінки або недооцінки супротивника.



Імпровізація

- Принцип імпровізації — відсутність шаблону, гнучкість.



Агресивність

- Агресивність — нав’язування ініціативи.



Несподіваність

- Передбачає несподівані для протиборчої сторони дії за часом, місцем, масштабам, складом і способам вживаних невідомих супротивникові сил та засобів.



Досвід

- Досвід (в значенні спадкоємність) в розвідці є ключем до її успіху. Розвідник здатний бачити далеко уперед тільки у тому разі, якщо він базується на досвіді своїх попередників. Аналіз і використання позитивного і негативного досвіду — запорука успіху розвідки.



Попередні уроки

- Уроки розвідки - (облік прорахунків і виявлених помилок) повинні аналізуватися, бо за нової епохи від цієї здатності розвідки часто залежить смерть або життя нації



Цілеспрямованість, розумність і практична корисність

- Принцип, що припускає наявність певної мети, заради якої і організовується вивчення об’єктів дослідження і дії. Не розпиляти зусилля на розв’язання другорядних для розвідки проблем.



Економічна доцільність і принцип самоокупності

- Як правило, будь-яка довгострокова операція британської розвідки має бути узгоджена і затверджена, зокрема санкцією міністра фінансів уряду Великобританії, який і визначає економічну доцільність передбачуваних оперативних видатків.



Тактичні принципи розвідки

Конспірація

- Існує непорушне правило — дотримуйся таємниці операцій, що про-водяться, і не попадайся. Жоден агент не повинен знати нічого понад те, що йому не-обхідно для його дій, і не вельми бути посвяченим без крайньої потреби в роботу ін-ших агентів.



Оригінальність мислення

- Повторювати пройдене — означає помилятися. Пройдене відоме супротивникові, який зробив необхідні висновки.



Індивідуальність

- Розвідник бореться в умовах абсолютної таємності і самотності, протиставляючи свій розум об’єднаним зусиллям контррозвідки супротивника і напружуючи до краю свої нерви. Відомими стають тільки ті, хто «провалився».



Правда природності

- Британці вважають, що правда природності — найбільший союзник розвідника. Вона — вищий пілотаж, вища школа і вищий наставник.
- Цей принцип вимагає, щоб національний характер народу, у середовищі якого діє розвідник, розглядався як чинник першорядної ваги.



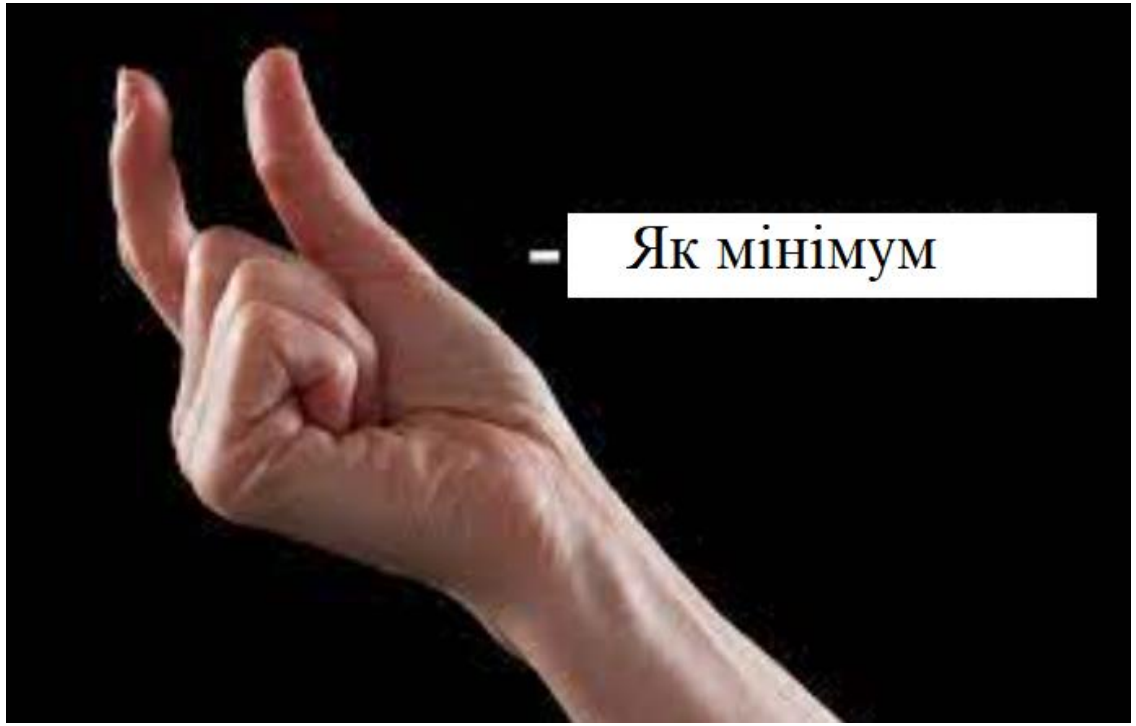
Недовіра — зброя розвідника

- Бути розвідником — це значить, насамперед, служити керівникам, завдання яких полягає в тому, щоб вам не довіряти, і це є головною умовою розвідки.
- Отже, розвідник приречений на те, щоб постійно перебувати між двома вогнями. Розвідник і сам не довіряє нікому. Цей принцип означає: не довіряй на-віть своїм союзникам і не надавай інформацію, здатну викрити важливе або делікатне джерело, чи дозволити офіцерам спецслужб супротивника вивчати свою організацію.



Розумна достатність

- Принцип розумної достатності потребує точного визначення того мінімуму, який потрібний і достатній для проведення тієї або іншої операції розвідки.



Дроблення розвідувальних операцій



Принципи «око за око» і «рівність»

- Застосовується при видворенні з країни розвідників, що діють під дипломатичним прикриттям.



Адміністративно-управлінські та оперативні принципи розвідки

Єдиноначальність

- На чолі органу управління розвідкою призначається одна особа, правомочна приймати юридично обов’язкові для підлеглих рішення. При цьому не заперечуються і певні елементи колегіальності, коли до вироблення рішень залучаються відповідні уповноважені особи.



Лінійний принцип

- **Лінійний принцип** — дозволяє предметно простежувати діяльність конкретних держав, стан оперативної обстановки в регіонах в усіх її різновидах і проявах, бачити проблему в цілому і ухвалювати обґрунтовані рішення.



Об’єктовий принцип

- **Об’єктовий принцип** полягає в зосередженні уваги усіх сил і засобів на розробці визначених об’єктів, наприклад, атомної енергетики, проникнення до яких забезпечить виконання завдань, що стоять перед спецслужбою.



Агентура потребує коштів

- Найдавнішими правилами і методами вербування агентів є насамперед підкуп, обіцянка підвищення по службі і великих винагород, а в крайніх випадках — шантаж і залякування того, кого вербують, аж до погроз спалити його будинок, розорити, понівечити і навіть знищити дружину і дітей.



Система прикриття

- Найбільш поширеними в розвідці є прикриття дипломатичні, комерційні, журналістські. Вважається, що комерційні прикриття гарантують більшу безпеку розвідувальних операцій і дають розвідникам більш вільного і добре легендованого доступу до важливої інформації.
- Використання журналістики для прикриття розвідувальної діяльності вперше було реалізовано англійською розвідкою.



Форми, методи і засоби розвідувальної діяльності

Форма, метод

- Форми — це відносини, які складаються між учасниками розвідувального процесу, спосіб організації розвідувальної діяльності.
- Методи — це різні варіанти впливу розвідувального органу на об’єкт (суб’єкт), щодо якого здійснюється розвідка; взаємодія розвідувального органу і об’єкта (суб’єкта) розвідки, у ході якого отримується розвідувальна інформація.

Методи ведення розвідки

- Розвідка може вестися за допомогою легальних (гласних), напівлегальних і нелегальних (негласних) методів.
  - **Легальні (гласні) методи розвідки** — дії органів, які ведуть розвідувальну діяльність без приховування, по-перше, самого факту здійснення будь-яких дій, а по-друге, осіб, які їх здійснюють. При гласному проведенні заходів може зашифровуватися (приховуватися) їх справжня мета.
  - **Напівлегальні методи розвідки** — це розмови в неофіційній обстановці, проведення завідомо неправдивих конкурсів і переговорів, отримання інформації від клієнтів, постачальників через контрольні органи.
  - **Нелегальні (негласні) методи розвідки** — передбачають приховування від зацікавлених осіб факту здійснення будь-яких дій і осіб, що їх виконують. Приклади нелегальних (негласних) методів: викрадення зразків продукції та обладнання, викрадення, копіювання, підміна, ознайомлення, знищення документів з цікавою інформацією, знімання інформації із технічних каналів, проникнення в локальні обчислювальні мережі, впровадження агентів, проникнення на територію тощо.

Засоби розвідки

- Засобами розвідки є об’єкти, предмети матеріального світу, за допомогою яких досягається (забезпечується) здійснення розвідувальної функції.
- До засобів розвідки належать агентура, технічні та оперативні засоби, фінанси, транспорт та інші матеріальні об’єкти, що використовуються в процесі роботи розвідки.







Обмеження

- Законодавство держави визначає певні обмеження щодо застосування методів і засобів в оперативній (розвідувальній) діяльності. Зокрема, в Законі України «Про оперативно-розшукову діяльність» вказані такі обмеження:
  - для одержання інформації забороняється застосовувати технічні засоби, психотропні, хімічні та інші речовини, які пригнічують волю або завдають шкоди здоров'ю людей та навколишньому середовищу;
  - забороняється залучати до виконання оперативно-розшукових завдань осіб, професійна діяльність яких пов'язана зі збереженням професійної таємниці, а саме: адвокатів, нотаріусів, медичних працівників, священнослужителів, журналістів, якщо така співпраця буде пов'язана з розкриттям конфіденційної інформації професійного характеру .



Донецький національний технічний університет



Тема 5. Розвідка та добування інформації.
Лекція 13. Оптична розвідка.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Засоби оптичної розвідки
- Методи визначення відстаней
- Високотехнологічні засоби оптичної розвідки

Засоби оптичної розвідки

Оптична розвідка

Оптична розвідка є складовою частиною розвідки.
Вона проводиться з наземних спостережних пунктів, розгорнутих на місцевості за допомогою ***оптичних та електронноoптичних приладів***.



Позитивними властивостями оптичної розвідки є:
-швидкість розгортання;
-швидкість та точність визначення координат цілей, орієнтирів та реперів;
-простота та надійність роботи приладів;
-довгочасність і безперервність ведення розвідки.

Репер (від фр. repère - Мітка, знак, вихідна точка в геодезії - знак, який знаходиться в певній точці земної поверхні з відомою абсолютною висотою. Ця висота визначається за допомогою нівелювання щодо вихідної рівненої поверхні. На реперах закріплюється металевий диск діаметром 5 сантиметрів (марка) із номером та зазначенням відомства.



Бінокль

Бінóкль, розм. далековúд (лат bini — два і лат. oculus — око) — оптичний прилад, складений з двох паралельно з'єднаних зорових труб. Застосовують його для спостереження за віддаленими предметами. Є два типи біноклів: театральний і польовий.

В *театральному біно*клі використовуються труби Г.Галілея, в яких окуляром служить розсіювальна лінза, що дає можливість спостерігати предмети без зміни їхньої орієнтації відносно глядача. Оптичні осі окулярів і об'єктивів цих труб суміщаються з оптичними осями очей людини, тому стереоскопічність при користуванні театральним біноклем така ж, як і при спостереженні очима.

Театральний бінокль тільки збільшує кут зору, що психофізично сприймається як наближення видимої картинки картини.





Театральний бінокль

Польовий бінокль

Польовий бінокль — паралельно з'єднані дві труби Й.Кеплера, він являє собою спостережний і вимірюваний прилад, бо дає можливість робити наближені вимірювання віддалі до предметів.

Для цього у фокальній площині (*площина, утворена всіма фокусами (головним та допоміжними) оптичної системи*) об'єктива зорової труби Й. Кеплера перед окуляром розміщують вимірювальні шкали.

Щоб зображення було пряме, в оптичну систему польового бінокля вводять дві прямокутній призми, внаслідок чого оптичні осі об'єктивів трохи зміщуються відносно оптичних осей окулярів та очей і стереоскопічність зору підвищується.

Кратність (ступінь збільшення кута зору) театральних біноклів становить від 2,5 до 3×; польових — від 3 до 18×.



Польовий бінокль

Призменні бінокліі

Призменні бінокліі (рис. 1.) належать до приладів спостереження і вимірювання кутів і відстаней. Призменний бінокль складається із двох зорових труб, з'єднаних між собою шарніром. Оптичні осі зорових труб паралельні. Кожна зорова труба складається із окулярної частини, корпуса та об'єктивної частини.

Оптична система зорової труби містить об'єктив, дві призми, що повертаються, для отримання прямого зображення і зменшення довжини трубки та окуляра для збільшення відображення отриманого у фокальній площині об'єктива. Труби шарнірно закріплені на загальній осі, що дозволяє змінювати відстань між окулярами відповідно до відстані між зіницями очей спостерігача. На головці шарнірної осі, що повернена до окулярів, нанесена шкала відстаней між центрами вихідних зіниць у міліметрах (від 54 до74 мм).

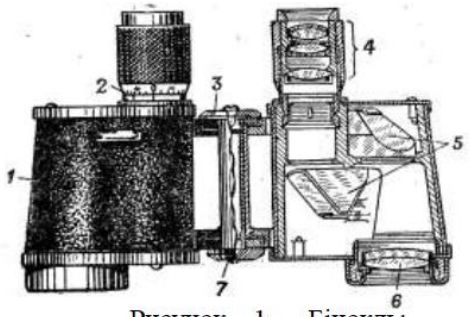


Рисунок 1 – Бінокль:

1– корпус; 2 – діоптрійне кільце; 3 – шкала відстаней між окулярами; 4 – окуляр; 5 – призми обертаючої системи; 6 – об'єктив; 7 – шарнірна вісь

Основні параметри бінокліів

Основні параметри бінокліів:

- збільшення (кратність);
- діаметр лінзи об'єктиву.

Зазвичай ці параметри указуються на корпусі бінокля, наприклад Б10×40.

Перша цифра (10) — це кратність, вона повідомляє нас про те, що за допомогою цього бінокля ми зможемо побачити зображення об'єкта в 10 разів більше (у кутовій мірі), ніж при спостереженні неозброєним оком.

Друга цифра (40) показує діаметр зовнішньої лінзи об'єктиву в міліметрах. Чим більше лінза, тим більшою світлосилою вона володіє, тим більше світла вона збирає і дає яскравіше зображення.









Об'єктив, окуляр

- Основними частинами будь-якого оптичного приладу є об’єктив та окуляр.
- **Об’єктивом** називається оптична система скла приладу, яка обернена у бік предмета, що розглядають. Вона призначена для побудови зображення предмета у приладі.
- **Окуляром** називається оптична система скла приладу, яка обернена у бік ока спостерігача. Вона призначена для розгляду зображення, що передає об’єктив.
- Основними характеристиками оптичних приладів є:
  - збільшення;
  - величина поля зору
  - роздільна здатність
  - світлосила
  - діаметри вхідної і вихідної зіниць
  - пластичність
  - перископічність.









Збільшення

- **Збільшення** – основна властивість оптичних приладів. Під збільшенням розуміють відношення величини відображення предмета, видимого в приладі до величини відображення того самого предмета при спостереженні його неозброєним оком.
- Збільшення чи кратність приладу позначається цифрою (числом) і значком Х. Позначенням 8х, 10х означають восьмикратне, десятикратне збільшення.

Поле зору

600

- **Полем зору** називається частина простору, видимого в прилад. Воно характеризується кутом, під яким видно в приладі дві діаметрально протилежні крайні точки видимого в приладі простору.
- Вимірюються в градусах чи поділках кутоміра.









Світлосила

- **Світлосила** приладу характеризується мірою освітлення зображення предмета, що спостерігається в прилад на сітчатці ока. Світлосила залежить від розмірів поперечного розтину пучка променів, що проходять через оптичну систему приладу і надходять в око спостерігача, від прозорості оптичної системи і кількості лінз і призм, які становлять оптичну систему даного приладу. Для збільшення світлосили оптичних приладів їх лінзи і призми піддаються спеціальній обробці, а на поверхні наносять особливу плівку, що зменшує відбиття світлових променів.
- Такі прилади називаються приладами з «проясненою» оптикою, тобто з оптикою, що добре пропускає світло.
- За зовнішнім виглядом вона має блакитний відтінок. Для порівняння світлосили приладів використовують штучну величину, що дорівнює квадрату діаметра вихідної зіниці.









Вхідна та вихідна зіниці

- **Вхідною зіницею** називається найменший отвір об'єктива приладу який обмежує надходження світлових променів у прилад. Вимірюється в міліметрах.
- **Вихідною зіницею** називається розмір зображення вихідної зіниці на виході із окуляра. Відстань від останньої лінзи окуляра до площини вихідної зіниці називається віддаленням вихідної зіниці. Для повного використання поля зору приладу під час роботи необхідно поєднати зіниці очей з площиною вихідної зіниці. За недотримання цієї умови частина поля зору буде зрізатися.
- Для забезпечення правильного положення ока окуляри приладів забезпечуються очними раковинами або гумовими наочниками.









Роздільна здатність

- **Роздільна здатність** оптичного приладу це найменший кут між двома точками чи предметами, зображення яких у приладі отримують окремими.
- Вимірюється в кутових секундах.
- Межа роздільної здатності людського ока 10 секунд. Чим більші збільшення приладу і діаметр вхідної зіниці, тим більша його роздільна здатність.









Пластичність

- **Пластичністю** називається властивість приладу давати спостерігачу відчуття глибини і рельєфності простору, що спостерігається в прилад. Пластичність мають бінокулярні прилади, тобто прилади, призначені для спостереження двома очима одночасно.









Пластичність

- **Перископічністю** називається конструктивна здатність приладу, що дозволяє спостерігати із-за укриття. Вона вимірюється в міліметрах та показує величину відстані по вертикалі між центром вхідного отвору та оптичною віссю окуляра.











Кутомір$_1$

За одиницю виміру кутових величин в артилерії беруть поділку кутоміра.
Одна поділка кутоміра – це центральний кут, що від повідає дузі 1/6000 кола (рис. 2).

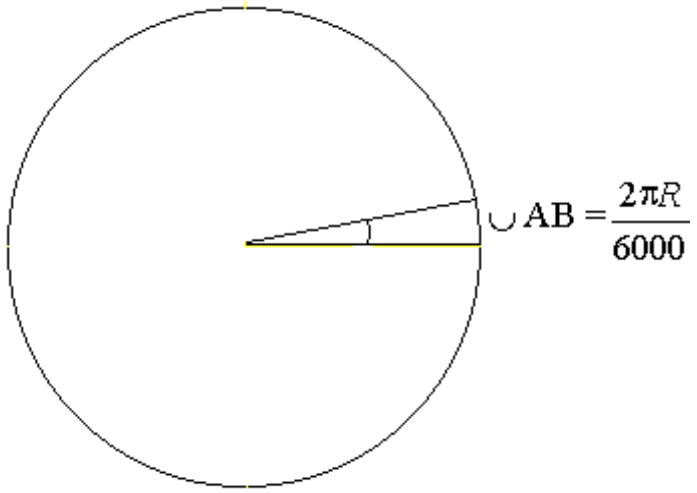


Рисунок 2 – Поняття поділки кутоміра

Центральний кут, довжина дуги якого дорівнює 1/6000 частини довжини кола, називається поділкою кутоміра:

$$\cup AB = \frac{2\pi R}{6000} = \frac{2*3{,}14*R}{6000} = \frac{3{,}14R}{3000} = \frac{1}{955}R = 0{,}001105R \approx {}^{1}\!/_{1000}\,R$$

Довжина дуги, що відповідає куту в одну поділку кутоміра, дорівнює 2πR/6000 = 6,28/6000·R = 1/955, де R –довжина радіуса кола. Округлено довжина дуги, що відповідає куту в одну поділку кутоміра, дорівнює 1/6000 радіуса, яким проведено коло (при цьому помилка округлення дорівнює 5 % у менший бік). Тому поділку кутоміра називають також «***тисячними дальності***», або скорочено «***тисячними***».

Кутомір$_2$

- Оскільки коло має 3600, або 360×60 = 21 600', то одна поділка кутоміра дорівнює 21 600 / 6000 = 3,6', а 100 поділок (одна «велика поділка кутоміра») дорівнює 3,6×100 = 360' = 60. 10 = 6000 / 360 ≈ 17 поділок кутоміра (точніше 16,5).
- У системі вимірювання кутів у «тисячних» існує проста залежність між кутовими і лінійними величинами:
- лінійна відстань між двома рівновіддаленими від спостерігача точками дорівнює кутовій відстані між ними у поділках кутоміра, помноженому на 0,001 дальності.

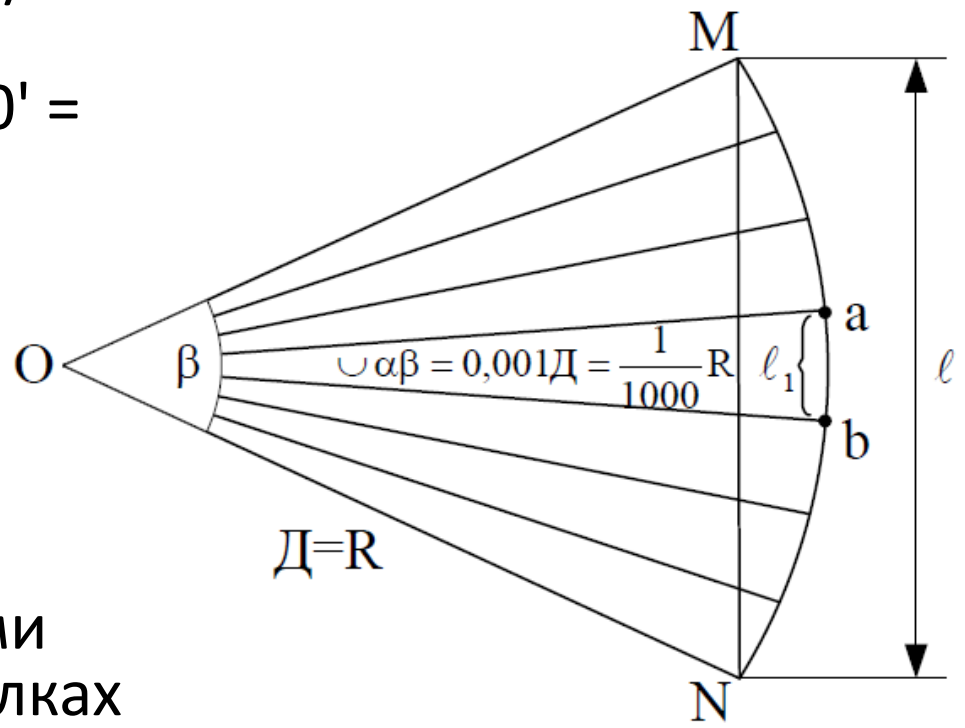


Рисунок 3 – Залежність між кутовими і лінійними величинами

Кутовимірювальна сітка$_1$

- У правій зоровій трубі бінокля розташована кутовимірювальна сітка, (рис. 3), за допомогою якої можна вимірювати кутові відстані між точками місцевості.

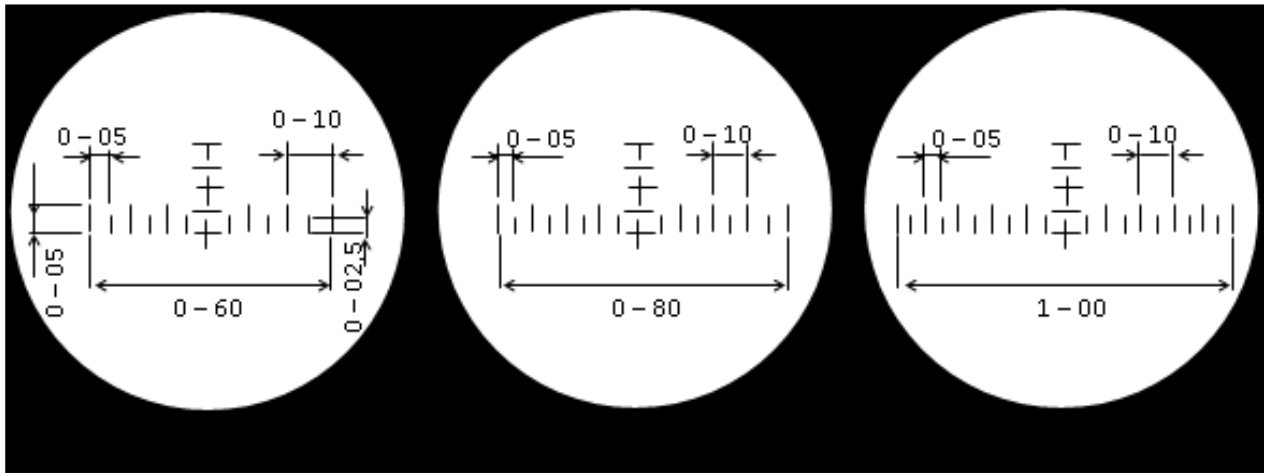


Рисунок 3 – Кутовимірювальні сітки біноклів
а – сітка бінокля Б-15; б – сітка бінокля Б-12;
в – сітка біноклів Б-6 і Б-8

Кутовимірювальна сітка$_2$

- Горизонтальні й вертикальні кути вимірюють за допомогою кутомірної сітки (рис. 4). При малих кутових відстанях між предметами (менше 0 – 50) центр кутомірної сітки потрібно сумістити з одним із предметів і відраховують число поділок кутоміра до іншого предмета.

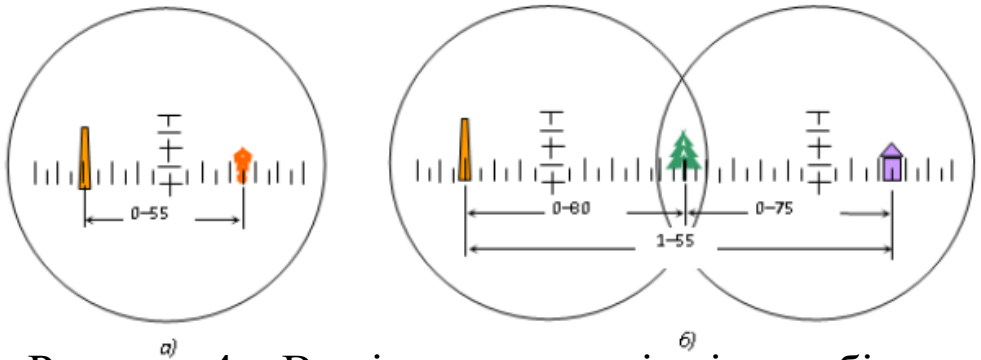
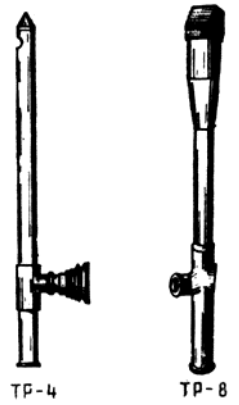


Рисунок 4 – Вимірювання кутів сіткою бінокля
а – кут у межах сітки прилада; б – кут між орієнтирами перевищує межі сітки приладу

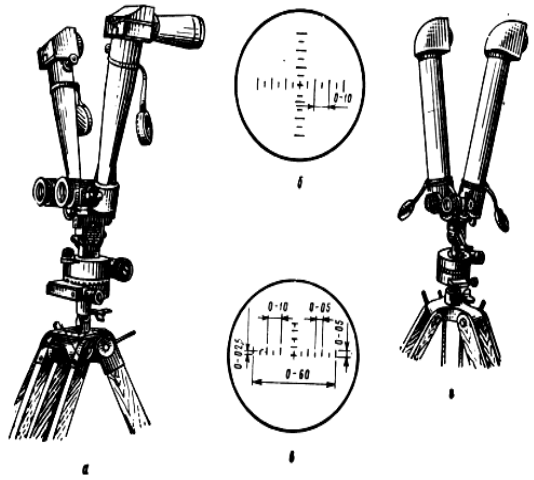
Перископ

- Перископи мають чотири і восьмикратне збільшення, поле зору 11° і 8°, масу в робочому положенні 1 і 0.8 кг відповідно. Перископічність (відстань між центрами окуляра і об’єктива) дорівнює 403 і 405мм. Присутня кутовимірювальна сітка. Перископ тримається в руці або закріплюється на вишці.



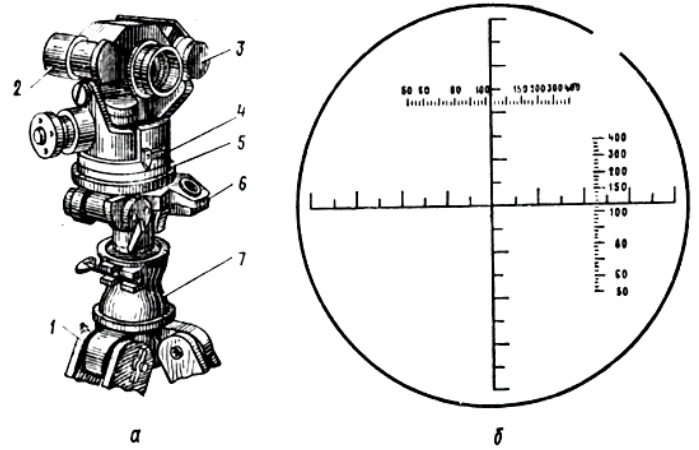
Стереотруба

- За своєю будовою являє ніби комбінацію двох перископів, скріплених біля основи на загальній шарнірній осі.
- У військах використовується велика стереотруба і артилерійська стереотруба. Остання відрізняється лише деякими деталями конструкції і кутомірною сіткою. Велика стереотруба має десятикратне збільшення, поле зору 5°, перископичність 325 мм, масу робочому положенні 11,5 кг. Вона забезпечує точність вимірювання кутів до 0-01.



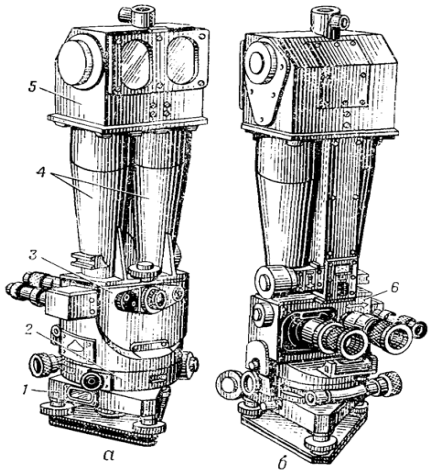
Бусоль

- Є основним приладом для цілевказування, підготовки даних для стрільби і навігаційної апаратури. Завдяки їй можна вирішувати всі задачі, що вирішуються за допомогою бінокля, перископа або стереотруби, і крім того визначати магнітний азимут на ціль.
- Бусоль ПАБ - 2А має восьмикратне збільшення, поле зору 5°, перископічність (при використанні в комплекті перископа) 350 мм, масу в робочому положенні 2,5 кг.
- При користуванні бусоллю керуються її індивідуальною документацією.



Розвідувальний теодоліт РТ

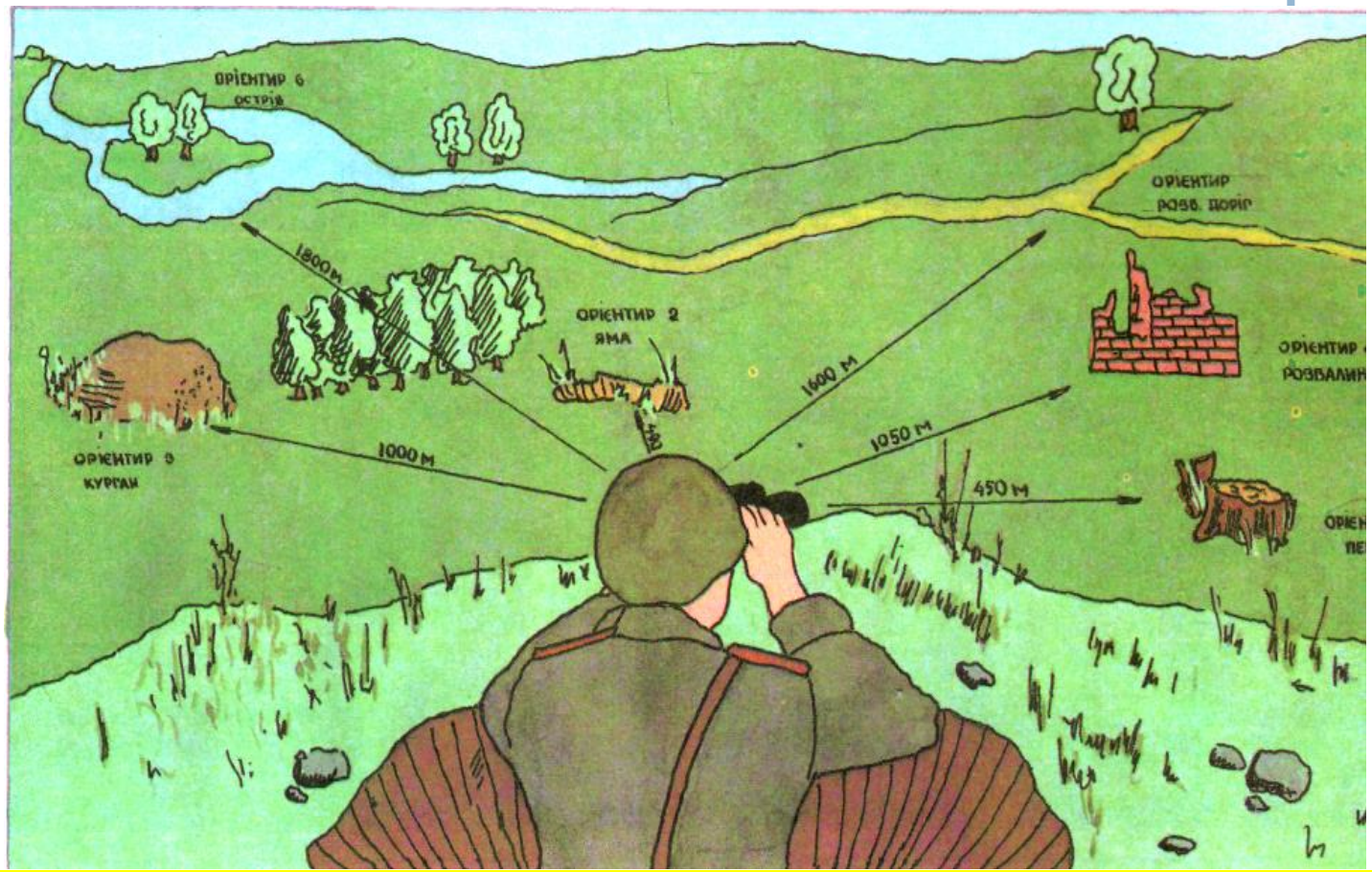
- Розвідувальний теодоліт РТ є основним спостережним і кутовимірювальний приладом підрозділів оптичної розвідки. Теодоліт призначений для:
  - ведення розвідки;
  - виміру горизонтальних і вертикальних кутів;
  - визначення магнітних азимутів;
  - виміру відстаней (з використанням далекомірної рейки)
  - при топографічній прив'язці.
- Розвідувальний теодоліт РТ має десятикратне збільшення, поле зору 5°, перископічність 185 мм.



Методи визначення відстаней

Визначення відстаней на око

- Визначення відстаней на око, полягає в здатності спостерігача уявляти й відкладати на місцевості певні відстані.



Визначення відстаней за кутовими розмірами$_1$

Визначення відстаней за кутовими розмірами предметів за допомогою бінокля (приладів оптичної розвідки), допоміжними способами, використовуючи формулу тисячної.

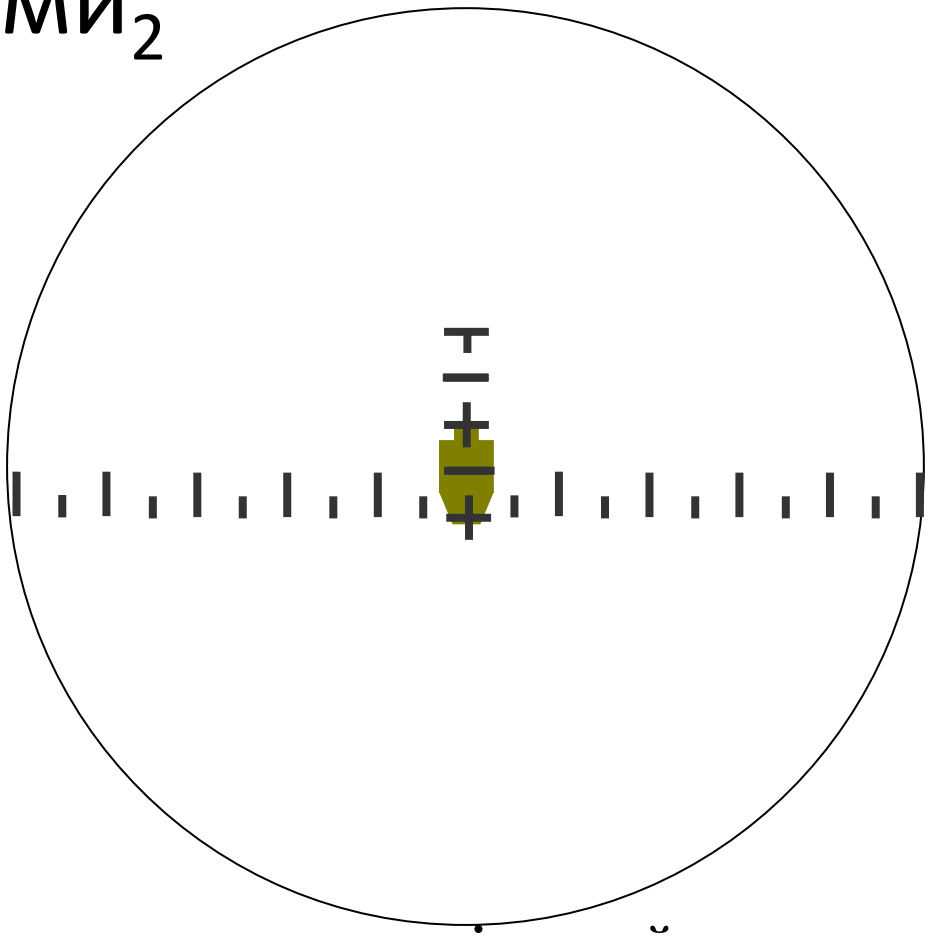
$$Д = \frac{В}{У} \times 1000$$

Д – відстань до об'єкту в метрах

В – висота (ширина) об'єкту в метрах

У – кут у тисячних (поділках кутоміру)

Визначення відстаней за кутовими розмірами$_2$



В = 1,7 м.

У = 0-10 = 10

$$Д = \frac{1{,}7\ м. \cdot 1000}{10} = 170\ м.$$

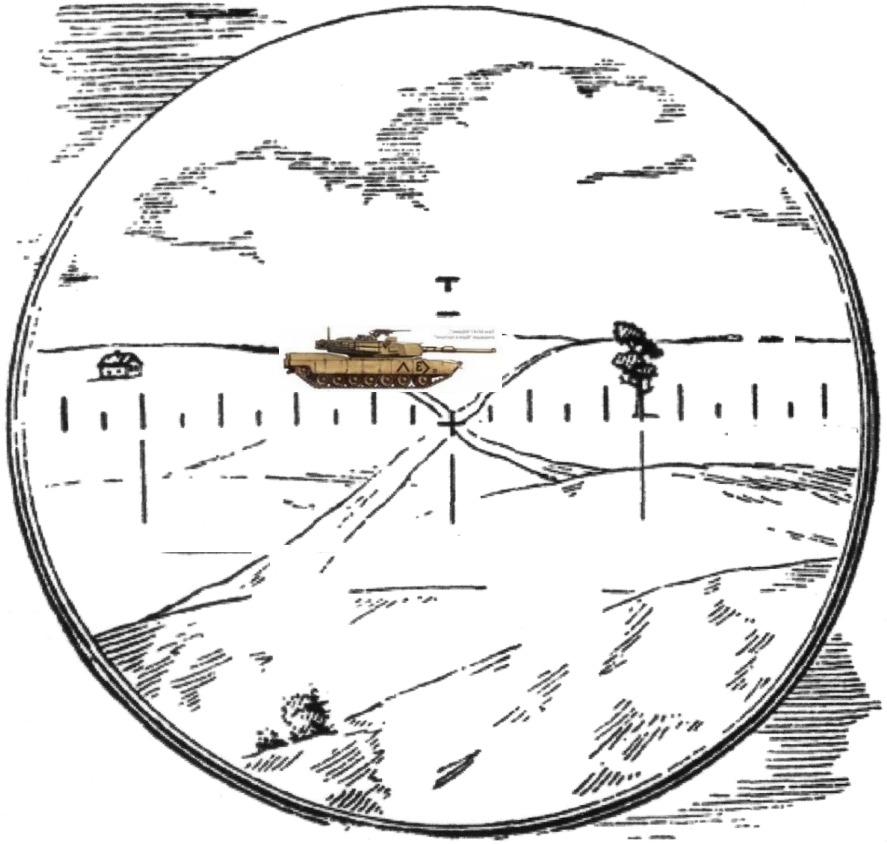
Для точнішого визначення відстаней цим способом корисно запам'ятати лінійні розміри типових предметів, приведених в таблиці наступного слайду:

Визначення відстаней за кутовими розмірами$_3$

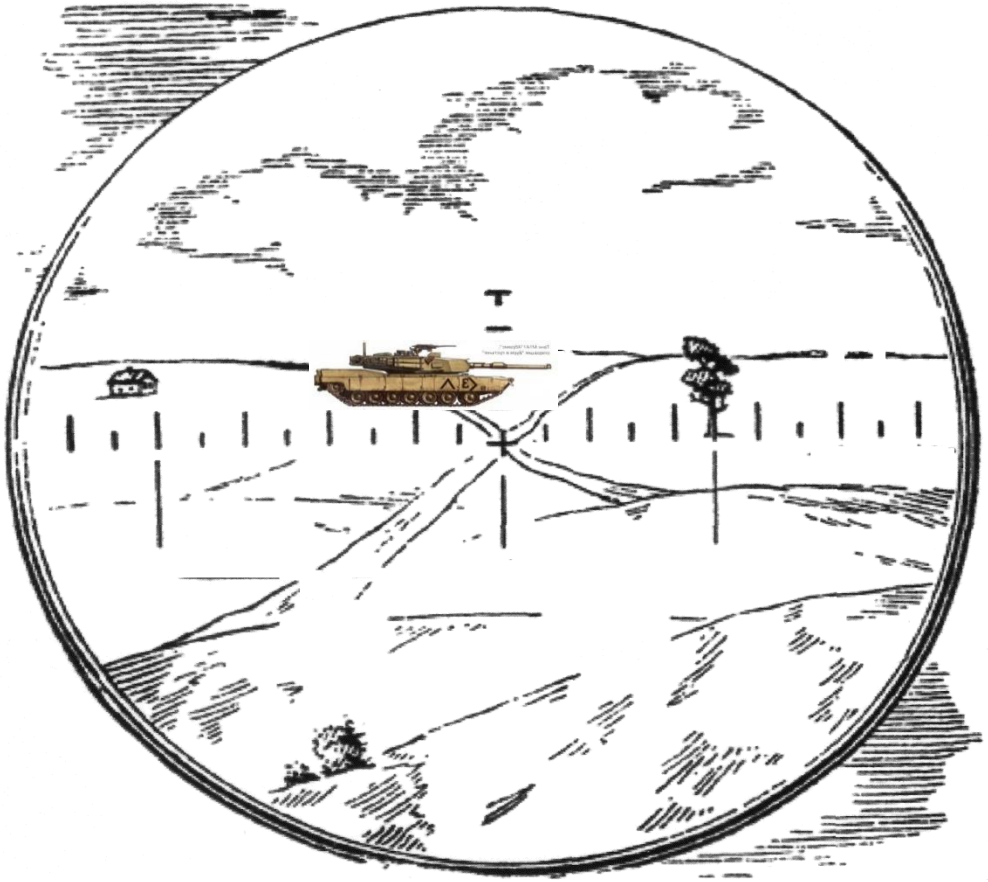
Найменування предметів	Висота	Довжина	Ширина
Людина середнього зросту(в взутті)	1,65-1,75		
Стрілець з коліна	1,05-1,20		
Телеграфний стовб	6,00		
Звичайний змішаний ліс	6,50-8,40		
Залізнична будка	4,00		
Одноповерховий будинок з дахом	6-8 метрів		
Вершник	2,20-2,30		
Танки	2,30-2,70	6,8-7,7	3,1-3,7
БТР и БМП	1,8-2,0	4,6-6,5	2,5-2,7
Один поверх житлового капітального будинку	3-4	-	-
Один поверх промислової будівлі	5-6	-	-
Відстань між стовпами ліній зв'язку		50-60	-
Відстань між опорами електро мережі високого струму		100	
Заводська труба	30	-	-
Вагон пасажирський суцільнометалевий	4,25	24-25	2,75
Вагони товарні:			
Двохосні	3,8	7,2	2,75
Багатоосні	4	13,6	2,75
залізничні цистерни:			
Двохосні	3	6,75	2,75
Чотирьохосні	3	9	2,75
Залізничні платформи			
Двохосні	1,6	9,2	2,75
Чотирьох осні	1,6	13	2,75
Автомобілі			
Вантажівка двохосна	2	5-6	2-2,5
Легкові	1,5-1,8	4-5	1,5
Важкий крупнокаліберний кулемет	0,75	1,65	0,75
Станковий кулемет	0,5	1,5	0,5
Мотоцикліст на мотоциклі з коляскою	1,5	2	1,2

Задача_1$_1$

Яка відстань до танку, якщо в бінокль він спостерігається під кутом в 0 – 22? Довжина танка – 6 метрів (задача).



Задача_1$_2$



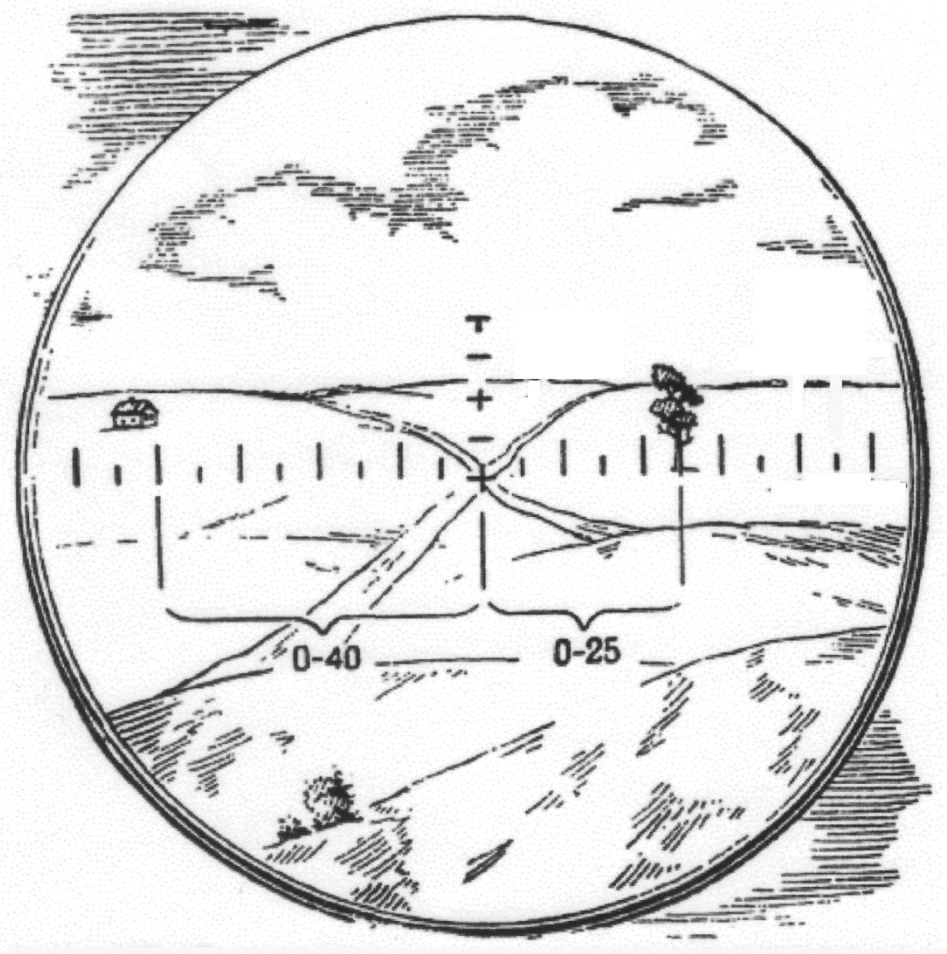
Використовуємо формулу тисячної

$$D = l\frac{1000}{u} = 6\frac{1000}{0-22} \approx 273\text{м}$$

де l – довжина танка,

u – кут, під яким спостерігається танк у бінокль

Вимірювання горизонтального кута



Кут між будинком і деревом буде дорівнювати

0 - 65

Задача_2$_1$



Задача_2$_2$



Рішення

$$l = \frac{1500}{1000} 1 - 00 = 150\text{м}$$

Задача_3

Визначити відстань до лінії електрозв'язку



1-спосіб – по куту

10мм = 0 – 20, тоді

$$D = 6\frac{1000}{0-20} = 300\text{м}$$

Задача_4

Визначення відстані від вибуху у ночі за часом співвідношення швидкості світла й звуку

$$Д = t * 333 = 3196,8 \approx 3200м$$ **або** $$Д = \frac{t * 1000}{3} = 3200м$$



t – час проходження звуку від моменту спалаху;
333 м/с – швидкість розповсюдження звуку пострілу

Визначення відстаней по ступені видимості предметів (цілей)

Об’єкти і ознаки	Відстані, з яких вони стають видимими в метрах
Окремий невеликий будинок	5000
Труби на даху	3000
Літак на землі, танк на місці	1200
Стволи дерев, стовпи ліній зв’язку	1000
Рухи рук та ніг людини, яка йде або біжить	700
Міномети, протитанкові гармати, рами на вікнах	500
Ручний кулемет, автомат, колір і частини одягу	250-
Черепиця на дахах, листя дерев, дріт на кілках	200
Ґудзики і пряжки	150- 170
Риси обличчя, кісті рук	100

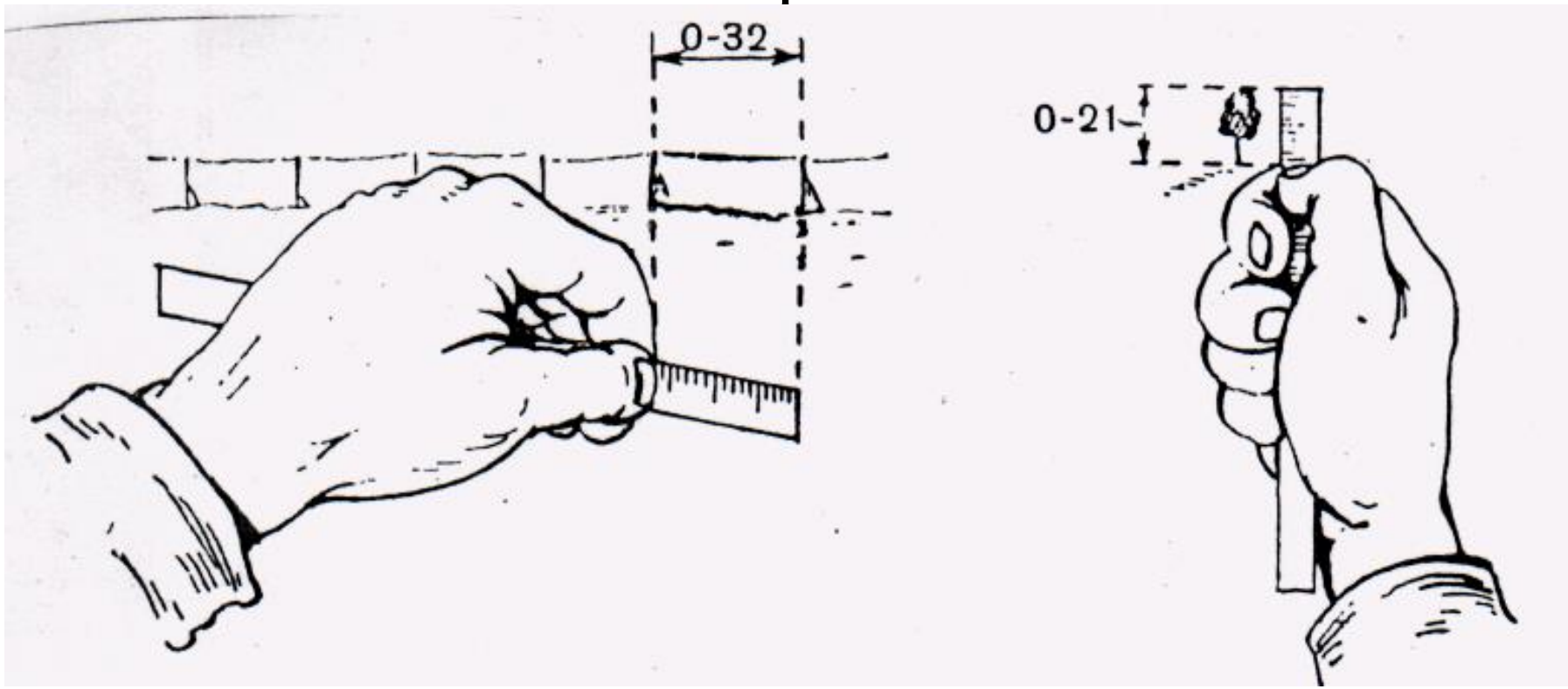
Демаскуючі ознаки

Звукові демаскуючі признаки	Середня відстань чутності в метрах
Неголосні розмови, кашель, зарядження зброї	100
Неголосні команди, брязкотіння зброєю, спорядженням	200
Забивання в землю кілків вручну	300
Вирубка (спилювання) лісу	300-500
Падання зрубаних дерев, різкий шум, тріскіт сучків	800
Голосний крик, відривка окопів вручну, удари лопатою по каменях	1000
Сигнал автомобіля, одиночні постріли	2000 - 3000

Джерело шуму	Відстань чутності в метрах
Кроки людини	40
Тріскіт зламаної гілки	80
Зарядження зброї	100
Рух автомобіля	800
Рух танка	2000

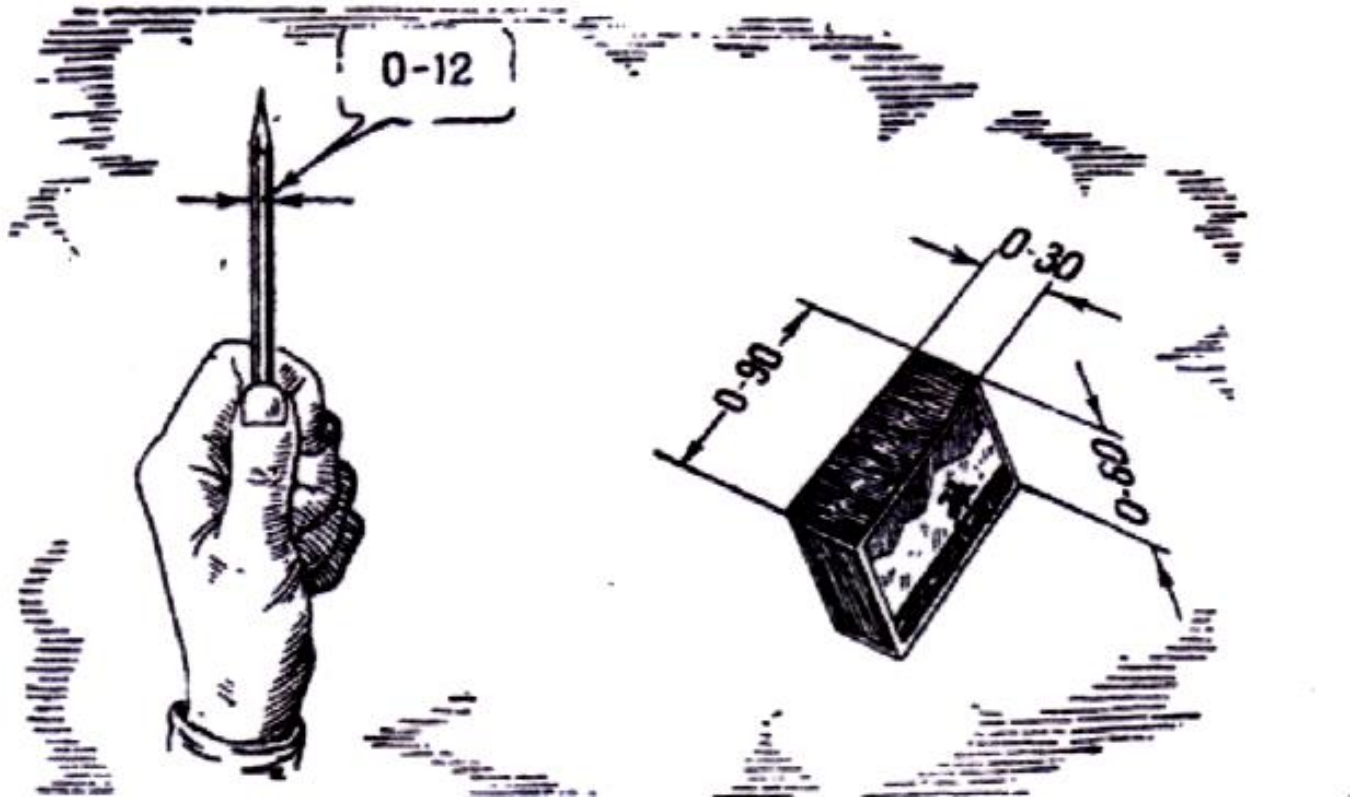
Вимірювання кутів допоміжними засобами$_1$

За допомогою лінійки, яка розташовується в 0,5 метрах від очей спостерігача



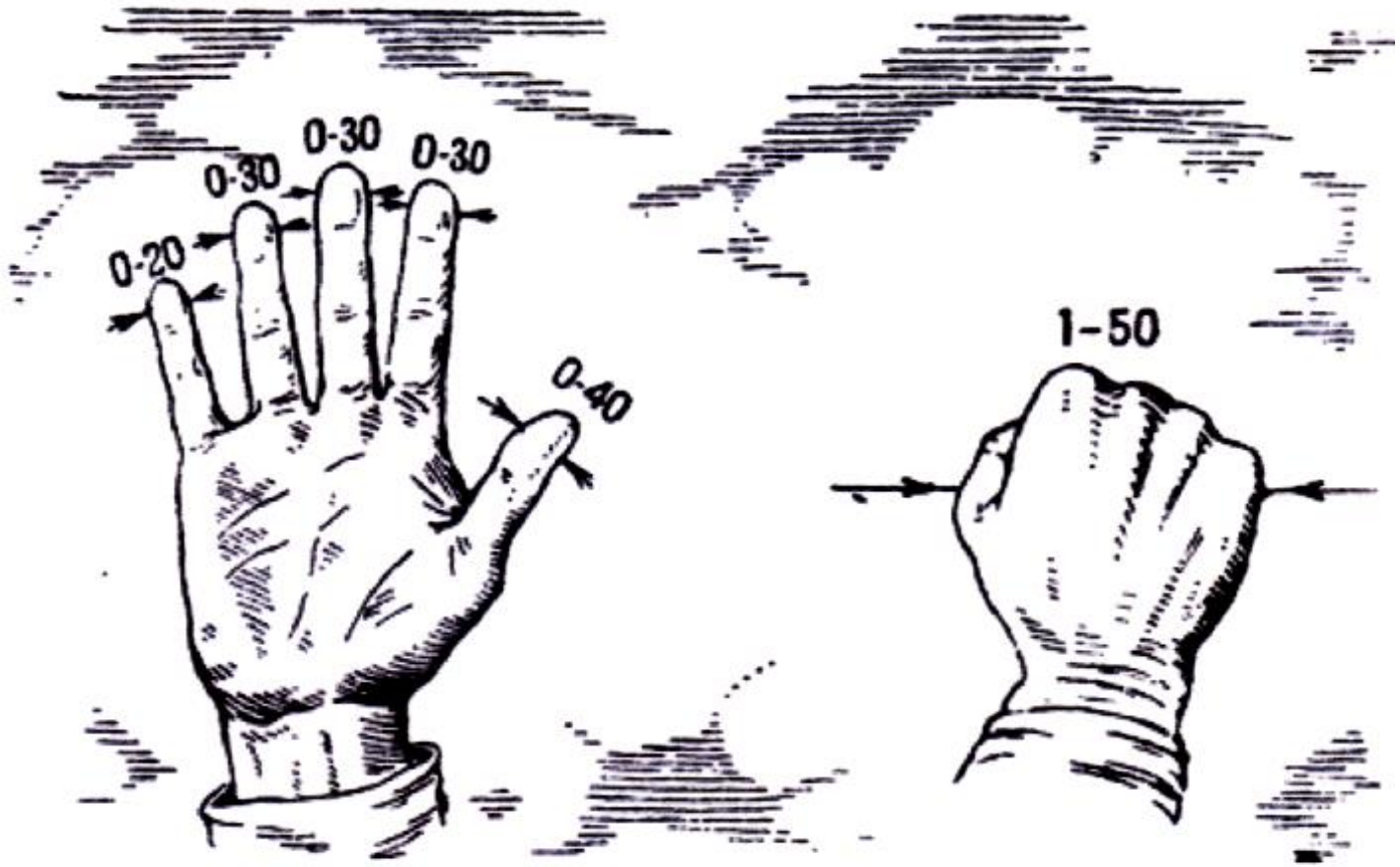
1мм = 0 – 02; 5мм = 0 – 10; 10мм = 0 – 20; 10см = 2 – 00; 20см = 4 – 00; 30см = 6 - 00

Вимірювання кутів допоміжними засобами$_2$



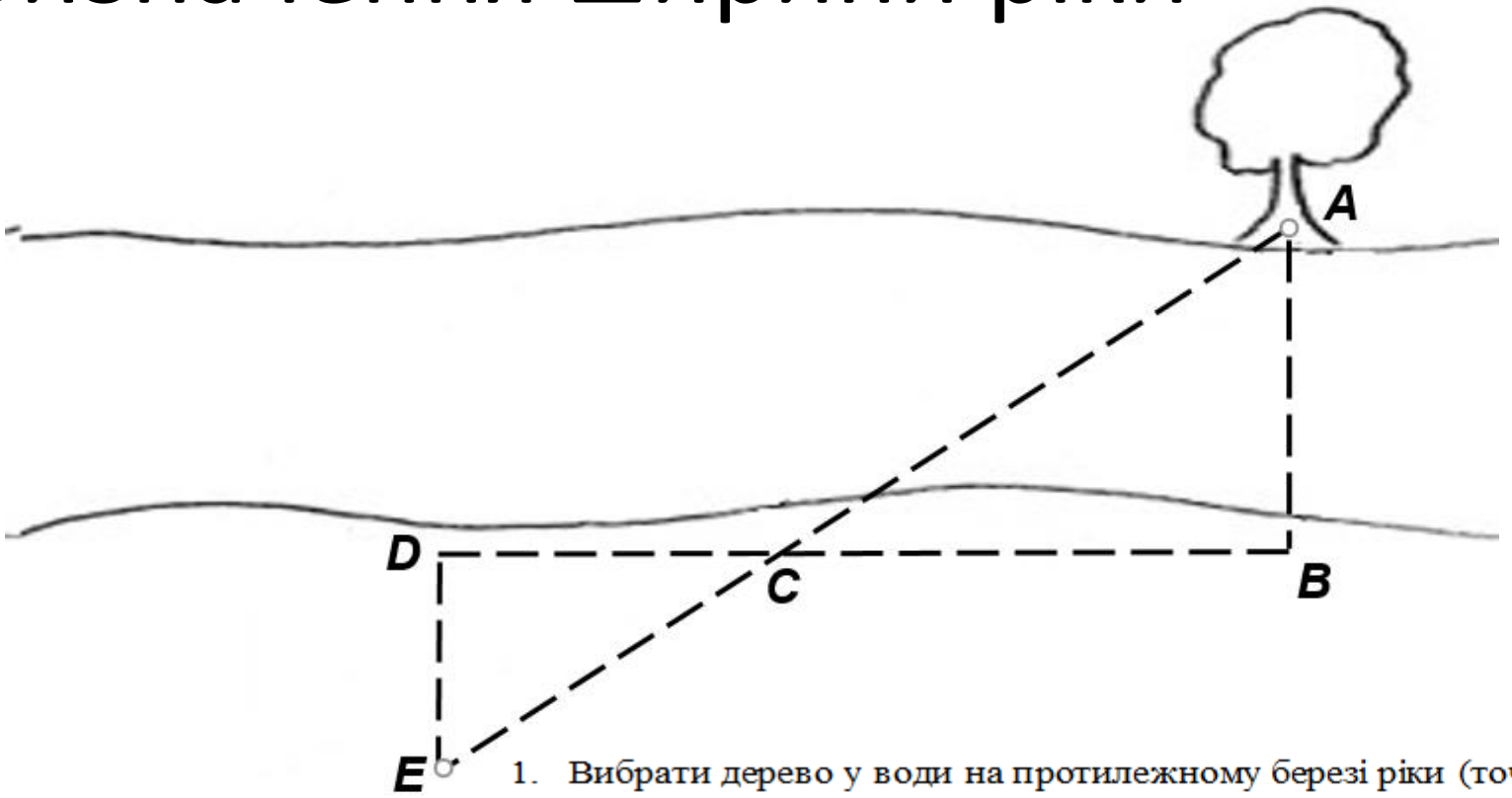
За допомогою олівця, коробки сірників також можна вимірювати кути

Вимірювання кутів допоміжними засобами$_3$



Пальці Вашої руки та стиснутий кулак можуть служити Вам найпростішим кутомірним приладом

Визначення ширини ріки

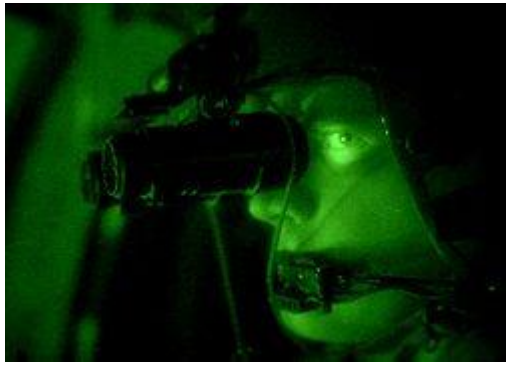


1. Вибрати дерево у води на протилежному березі ріки (точка A).
2. Уткнути гілку точно напроти дерева (точка B).
3. Відійти на 40 кроків уліво від лінії AB і уткнути другу гілку (точка C).
4. Пройти в тому ж напрямку ще 20 кроків і уткнути третю гілку (точка D).
5. Відійти, лічачи кроки, від точки D у протилежному від ріки напрямку так, щоб опинитися на одній прямій із точками A і C, і уткнути четверту гілку (точка E).
6. Відстані DE буде дорівнює половині ширини ріки. Помноживши цю відстань на два, отримаємо ширину ріки в кроках.

Високотехнологічні засоби оптичної розвідки

Прилад нічного бачення

Прила́д нічно́го ба́чення, ПНБ — оптичний прилад, що слугує для отримання у темряві видимого зображення об'єктів та місцевості. Призначений для виявлення, розпізнавання та спостереження цілей в умовах пониження освітленості.
https://www.youtube.com/watch?v=qM-vK16tDvg

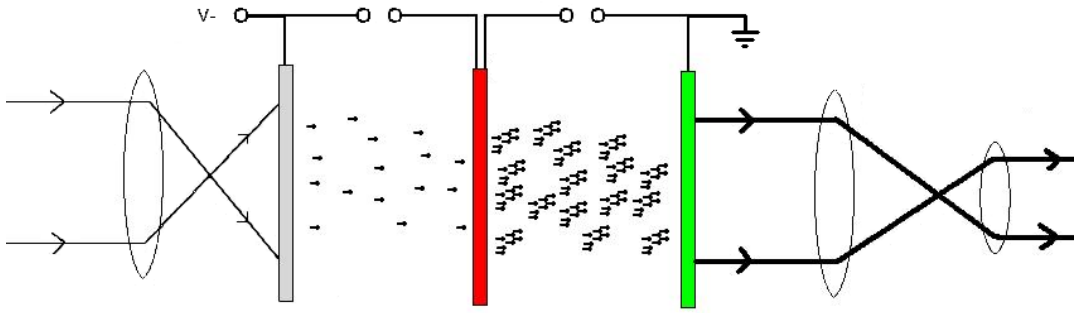


Першу інфрачервону телекамеру для потреб британської ППО у 1929 році винайшов Кальиан Тіхань. Перший практичний комерційний пристрій нічного бачення розробив у США відомий винахідник Володимир Кузьмич Зворикін (працював на «Radio Corporation of America») в 1930-х роках, та він не мав успіху через великий розмір і вартість. Але слід зазначити, що передумовою для створення приладів нічного бачення стало відкриття у XIX столітті інфрачервоного (теплового) випромінювання. Однак пристрій, здатний «бачити» предмети не в оптичному (видимому), а в інфрачервоному (тепловому) діапазоні спектра, було створено лише у 1934 році. Саме з винаходу першого електронно-оптичного перетворювача у 1934 й почалася історія приладу нічного бачення.

Принцип дії ПНБ

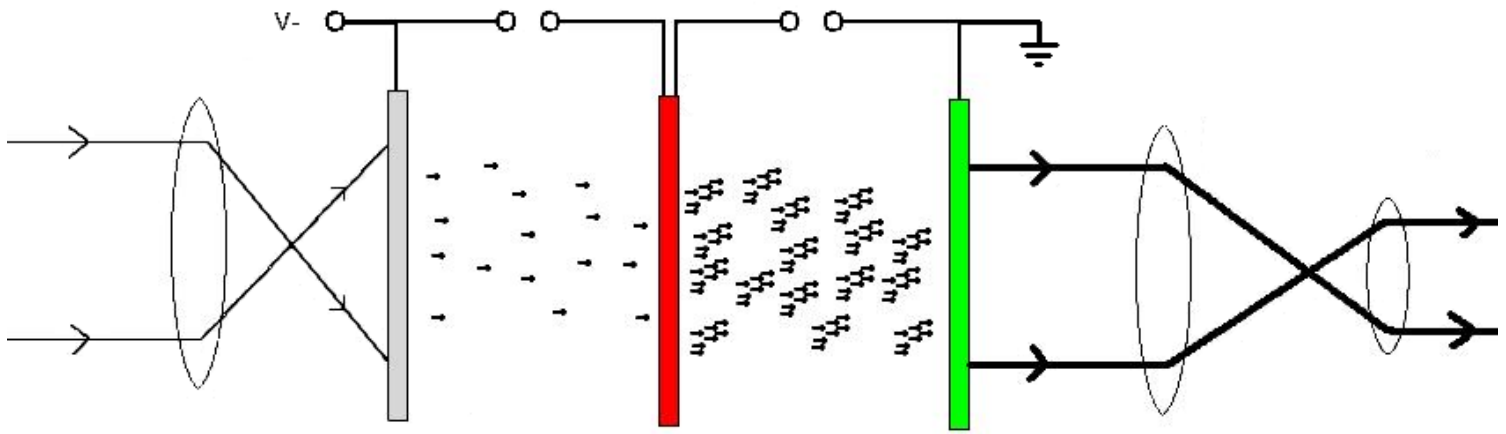
,

- В основі роботи всіх ПНБ лежить один й той же принцип. Зображення в окулярі утворюється за рахунок посилення відбитого від об'єкта спостереження випромінювання (як видимого, так й інфрачервоного).
- Практично будь-який ПНБ складається з двох основних частин: випромінювач і приймач ІЧ-випромінювання. Випромінювач, як електричний ліхтарик, освітлює об'єкт спостереження. При цьому ІЧ-промені, віддзеркалюючись від об'єкта у точній відповідності з формою й властивостями його поверхні, утворюють невидимий світловий портрет цього об'єкту. У приймачі світлова картинка перетворюється у видиме оком зображення; це забезпечує найважливіша деталь — ЕОП (електронно-оптичний перетворювач); фактично, це і є сам прилад нічного бачення плюс використання спеціальної оптики. Саме у ЕОП знаходиться фотокатод, який, вбираючи фотони світла, випромінює електрони. Електрони під дією електростатичного поля потрапляють на шар люмінафору, тим самим викликаючи випромінювання світла, яке спостерігають на виході ЕОП. Таким чином ЕОП перетворює невидиме оком інфрачервоне або якесь інше випромінювання у видиме, а також підсилює яскравість видимого зображення. Якщо власне ІЧ-випромінювання об'єкта спостереження досить для візуалізації його зображення, випромінювач не вмикають. Конструктивно прилади нічного бачення оформлюються у вигляді бінокля, прицілу до різних видів зброї, фото- та відеокамери.
- Живлення прилади нічного бачення отримують від акумуляторів. Основне застосування приладів нічного бачення у військовій та розвідувальній апаратурі, незамінні вони на суднах, в автомобілях під час руху у темряві, тумані, в умовах поганої видимості.



ПБН за поколіннями

- Пристрої II, III і IV покоління використовують мікроканальні пластини для посилення. Фотони з затемненого джерела входять у лінзу об’єктиву (зліва) і вдаряють у фотокатод (сіра плитка). Фотокатод випускає електрони, які прискорюються до вищої напруги у мікроканальній пластині (червона). Кожен електрон викликає звільнення кількох електронів від мікроканальної пластини. Електрони притягуються до люмінесцентного екрану високої напруги (зелений). Електрони, що потрапляють на люмінесцентний екран, змушують люмінафор виробляти фотони світла у видимій області екрану через окуляр.





Тепловізор

- Тепловізор (інфрачервона камера) — оптико-електронний прилад для візуалізації температурного поля та вимірювання температури. Переважно працює в інфрачервоній частині електромагнітного спектру — теплові зображення утворюються завдяки зміщенню максимумів спектрів власного випромінювання тіл під час їх нагрівання у короткохвильову область.
- Тепловізори поділяють за принципом дії на сканувальні та з багатоелементним приймачем випромінювання. Приймач випромінювання може бути неохолоджуваним або охолоджуваним, наприклад, за допомогою елемента Пельтє.



Види тепловізорів

- Спостережні прилади. Здійснюють виключно відображення об’єкта. Застосовуються в силових або охоронних організаціях, в рятувальних або військових операціях.

- Вимірювальні прилади. Виводить радіометричну картинку, яка допомагає зняти показання температури в радіусі спостережень. Використовується в медичних, промислових і будівельних цілях. А також для перевірки механічного та електричного обладнання.

- Візуальні пірометри. Розроблено для спостереження і визначення зон, що мають аномальні діапазони температури.



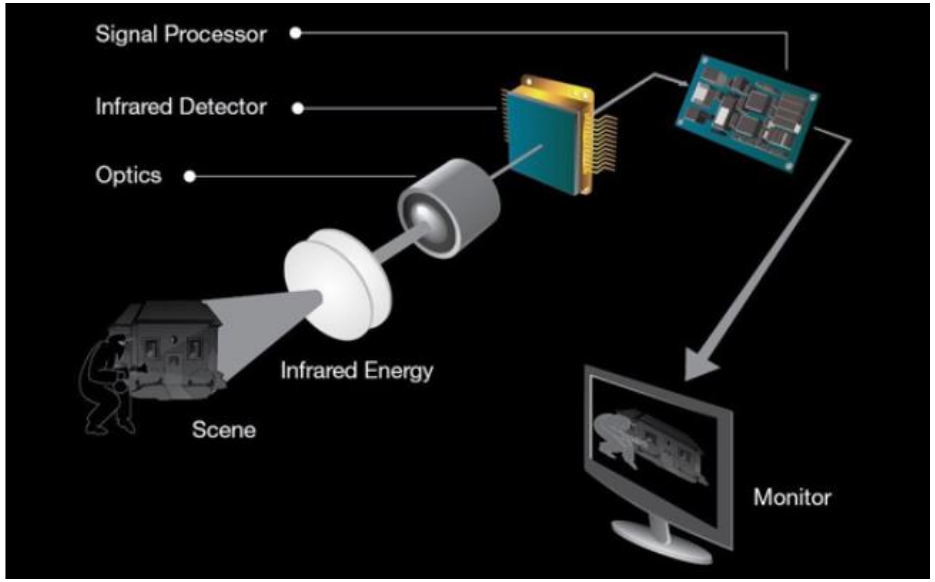
Основа інших приладів

- Сьогодні на основі тепловізорів виробляються багато оптичних пристроїв, такі як бінокулі та приціли.
- Виходячи з вимірювального діапазону можна поділити прилади на 3 види:
  - Високотемпературні – можуть визначити показання понад 1000 градусів Цельсія.
  - Промислові – застосовуються для тестування промислових і електричних систем. Ліміт понад 350 градусів Цельсія.
  - Будівельні – використовуються для перевірки будівельних об’єктів, з метою виявлення місць витоків тепла, порушення ізоляції, працюють з температурою до 350 градусів Цельсія.
    Завдяки своїм можливостям дана технологія стала тісно пов’язаною з промисловими і цивільними завданнями.



Конструкція тепловізора

- Основою конструкції тепловізорів є спеціальна матриця, що має здатність вловлювати самі довші хвилі інфрачервоного спектру — термальні, (від 3000 до 30 000 нанометрів). З метою фокусування та формування чіткої картинки в тепловізорі представлена лінза, яка виготовлена з селеніду цинку або германію.
- Сигнал з фотоматриці перетворюється на електричні імпульси. Дані імпульси процесор згаданого пристрою починає у відповідності до встановленого алгоритму розмальовувати у кольори видимого для нашого зору спектру. Таким чином на дисплеї появляється чітке зображення з різнокольоровими об’єктами, які ми можемо спостерігати.
  - Об'єктив тепловізора формує на сенсорі температурну карту (або карту різниці потужності випромінювання) всієї області, що спостерігається в полі зору
  - Мікропроцесор та інші електронні компоненти конструкції зчитують дані з матриці, обробляють їх та формують на дисплеї приладу зображення, яке є візуальною інтерпретацією цих даних, яке безпосередньо чи через окуляр розглядає спостерігач.



Далекомір$_1$

Лазерний далекомір (англ. laser rangefinder) — прилад, що вимірює відстані використовуючи лазерний промінь.

Застосовується в інженерній геодезії, при топографічній зйомці, в військовій сфері, в навігації, в астрономічних дослідженнях , в фотографуванні.

Лазерні дальноміри за принципом дії поділяються на імпульсні та фазові.

Імпульсний лазерний далекомір

Імпульсний лазерний далекомір складається з імпульсного лазера та детектора випромінювання. Вимірюючи час затрачений імпульсом на шлях до перешкоди і назад, помноживши його на швидкість світла, дізнаємось відстань від лазера до перешкоди.

$$L = \frac{c}{2n}t$$

де L — відстань до перешкоди, c — швидкість світла, n— показник заломлення середовища, t — час проходження імпульса до перешкоди і назад.

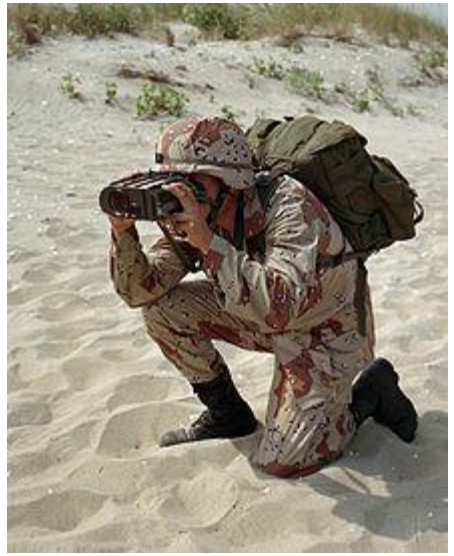
Точність вимірювання відстані визначається точністю вимірювання часу. А також, чим коротше фронт імпульса, тим краще для точності.



Далекомір$_2$

Фазовий лазерний далекомір

Фазовий лазерний далекомір вимірює відстані на основі порівняння фаз посланого і відбитого променів. У нього більша точність порівняно з імпульсним далекоміром. Також він більш дешевий у виробництві, а тому більш поширений у користувачів.



Комплекс оптичної розвідки КОРДОН-3

- Комплекс оптичної розвідки КОРДОН-3 – мультиспектральний модульний оптикоелектронний прилад, призначений для використання у складі систем спостереження і розвідки. Комплекс КОРДОН-3 може застосовуватись як автономно, з використанням портативного пульту керування RMC-03, так і в складі автоматизованих систем спостереження. Комплекс легко інтегрується з іншими засобами технічної розвідки.
- Оптичний модуль комплексу КОРДОН-3 складається з тепловізійної камери, денної камери, лазерного далекоміра. Електронний модуль комплексу КОРДОН-3 забезпечує первинну цифрову обробку зображень, автоматичне виявлення цілей, супроводження цілей, запис первинних даних, передачу даних до центрального посту спостереження в цифровому вигляді.
- Камери встановлені на опорно-поворотній гіростабілізованій платформі, що забезпечує наведення камер по азимуту і куту місця в ручному і напівавтоматичному режимі або автоматичному режимі патрулювання.
- Платформа встановлюється стаціонарно або на телескопічній щоглі.





Повітряна оптична розвідка

- Досвід ведення бойових дій в сучасних військових конфліктах переконливо свідчить про те, що повітряна розвідка є однією з найважливіших умов успіху бойових дій авіації та інших родів військ. Її завданням є своєчасне забезпечення командування і штабів повними і достовірними даними про противника. Одним із основних видів повітряної розвідки є телевізійна розвідка, що здійснюється за допомогою телевізійних систем, що мають у своєму складі літакову передавальну й наземну приймальню станції, і дозволяють спостерігати за об'єктами й діями військ противника.
- Основними характеристиками телевізійних систем, які впливають на якість отримуваного зображення є:
  - спектральна чутливість;
  - масштаб телевізійного зображення;
  - контраст телевізійного зображення;
  - розділювальна здатність. (відео)



Донецький національний технічний університет



Тема 5. Розвідка та добування інформації.
Лекція 14. Акустична розвідка.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Загальні положення
- Класифікація акустичних каналів витоку інформації
- Акустична розвідка
- Закладні методи
- Фізичні перетворювачі
- Вплив небезпечних акустичних сигналів на технічні системи

Загальні положення

Акустична розвідка$_1$

АКУСТИЧНА РОЗВІДКА – отримання інформації шляхом прийому та аналізу акустичних сигналів інфразвукового, звукового ультразвукового діапазонів, що поширюються у повітряному середовищі від об'єктів розвідки. Акустична розвідка забезпечує отримання інформації, що міститься безпосередньо у мовній або відтвореній мові (акустична мовна розвідка), а також у параметрах акустичних сигналів, супутніх роботі озброєння та військової техніки, механічних пристроїв оргтехніки та інших технічних систем (акустична сигнальна розвідка).

Завдання, які вирішує акустична розвідка

- дистанційне перехоплення смислової мовної інформації;
- визначення технічних та тактичних характеристик озброєння (О) та військової техніки (ВТ) (оцінка потужності вибухів боєприпасів та вибухових речовин при їх випробуваннях, визначення параметрів авіаційних та ракетних двигунів при їх стендових випробуваннях тощо);
- визначення характеру та спрямованості робіт на військово-промислових об'єктах;
- визначення шумових сигнатур О та ВТ.

Акустична розвідка$_2$

Акустична розвідка (АР) використовує портативну апаратуру прийому та реєстрації акустичних сигналів та стаціонарну апаратуру їх обробки та аналізу.

Апаратура АР полягає в використанні властивостей середовища передавати звукові коливання. Акустичні прилади забезпечують отримання найрізноманітнішої інформації (таємна мовна інформація, акустичні сигнали та шуми, що створюються різними видами техніки).

Інформаційна цінність отриманої мовної інформації залежить від її якості, що визначається співвідношенням фізичних характеристик мови та шуму у місці прийому.

До основних фізичних характеристик мови, що визначає її сутність, відносяться: спектр мовного сигналу, що визначає смугу звукових частот; спектр огинаючої мовного сигналу, що визначає моменти переходу звукових коливань мовного сигналу через нуль.

Канали перехоплення мовної інформації

Через акустичне поле шляхом прослуховування

Через паразитні електричні сигнали

Класифікація акустичних каналів витоку інформації

Основні визначення акустики

ОСНОВНІ ВИЗНАЧЕННЯ АКУСТИКИ

Звук → механічні коливання частинок пружного середовища (повітря, води, металу тощо), що суб'єктивно сприймаються органом слуху. Звукові відчуття викликаються коливаннями середовища, що відбуваються в діапазоні частот від 16 Гц до 20000 Гц

Звуковий тиск → змінний тиск у середовищі, обумовлений поширенням звукових хвиль.

Рівень звукового тиску → відношення величини звукового тиску P до нульового рівня, за який прийнято звуковий тиск

$P_0=2\cdot10^{-5}$ Н/м^2

$$N = 20\lg\frac{P}{P_0}$$

Сила звуку

Сила (інтенсивність) звуку → кількість звукової енергії, яка проходить за одиницю часу через одиницю площі; вимірюється у ватах на квадратний метр (Вт/м^2). Слід зазначити, що звуковий тиск і сили звуку пов'язані між собою квадратичною залежністю, тобто. збільшення звукового тиску вдвічі призводить до збільшення сили звуку вчетверо.

Рівень сили звуку — відношення сили даного звуку I до нульового (стандартного) рівня, за який прийнята сила звуку $I_0=10^{-12}$ Вт/м^2, яка обчислюється в децибелах (дБ)

$$N = 10 \lg \frac{I}{I_0}$$

Рівні звукового тиску та сили звуку, виражені в децибелах, збігаються за величиною.

Поріг чутливості

Поріг чутливості

найбільш тихий звук, який здатний чути людина на частоті 1000 Гц, що відповідає звуковому тиску $2 \cdot 10^{-5}$ Н/м^2

Спектральний рівень мовлення

$$B = 10\lg\frac{I\Delta F}{\Delta F I_0} = L_0\Delta F - 10\lg\Delta F$$

F, Гц	B, дБ	ΔF, Гц
350	45,5	175
500	41,5	350
1000	33,5	700
2000	25,5	1400
4000	18,5	2800

Залежність рівня звучання мови від динамічного діапазону

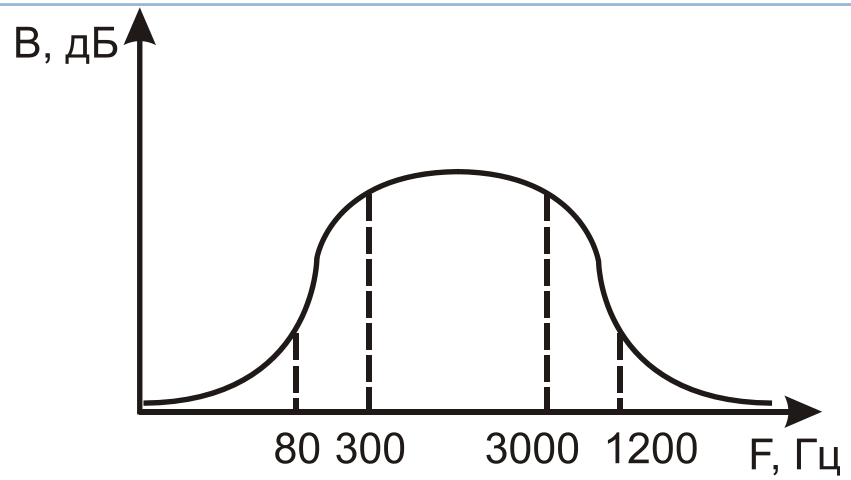
Гучність звуку

інтенсивність звукового відчуття, спричинена цим звуком у людини з нормальним слухом. Гучність залежить від сили звуку та його частоти, вимірюється пропорційно до логарифму сили звуку і виражається кількістю децибел, на яке даний звук перевищує за інтенсивністю звук, прийнятий за поріг чутності. Одиниця вимірювання гучності — фон.

Динамічний діапазон

Динамічний діапазон → діапазон гучностей звуку або різницю рівнів звукового тиску найгучнішого і тихішого звуків, виражена в децибелах.

Діапазон основних звукових частот мови знаходиться у межах від 70 Гц до 1500 Гц. Однак з урахуванням обертонів мовний діапазон звучання розширюється до (5000–8000) Гц.



Діапазон звучання мови

Акустичні канали витоку інформації$_1$

АКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

- повітряний, обумовлений поширенням мовного сигналу у повітряному середовищі;
- віброакустичний, обумовлений перетворенням мовного сигналу повітряного середовища в коливання твердого середовища та зворотним перетворенням;
- мікросейсмічний, обумовлений перетворенням акустичних мовних сигналів повітряного середовища в мікроколивання земної поверхні;
- електроакустичний, обумовлений перетворення акустичних мовних коливань повітряного середовища в електричні сигнали (мікрофонний ефект) та зворотним перетворенням.

Акустичні канали витоку інформації$_2$

- В акустичних каналах витоку інформації середовищем поширення мовних сигналів є повітря.
- Виток акустичної інформації за межі огороджувальних конструкцій можливий трьома шляхами:
  - ЗА РАХУНОК «МЕМБРАННОГО ЕФЕКТУ»
    - Так званий «мембранний ефект» обумовлений коливанням тонких (відносно довжини) і, як правило відносно легких, елементів огороджувальних конструкцій (віконного скла, фанерних, гіпсокартонних, пластикових перегородок тощо), здатних прогинатися під дією звуку;
  - ЧЕРЕЗ ТРІЩИНИ, ОТВОРИ, ЩІЛИНИ ТА ІНШІ АКУСТИЧНІ ОТВОРИ, ТОБТО ПРЯМИМ РОЗПОВСЮДЖЕННЯМ АКУСТИЧНИХ КОЛИВАНЬ
  - ЗА РАХУНОК ПЕРЕТВОРЕННЯ АКУСТИЧНИХ КОЛИВАНЬ В ВІБРОАКУСТИЧНІ, А ПОТІМ ЗНОВ В АКУСТИЧНІ
    - У даному випадку частина енергії акустичних коливань (частина відбивається), падаючи на поверхню огороджувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення речовини. Подолавши огороджувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

Акустичні канали витоку інформації$_3$

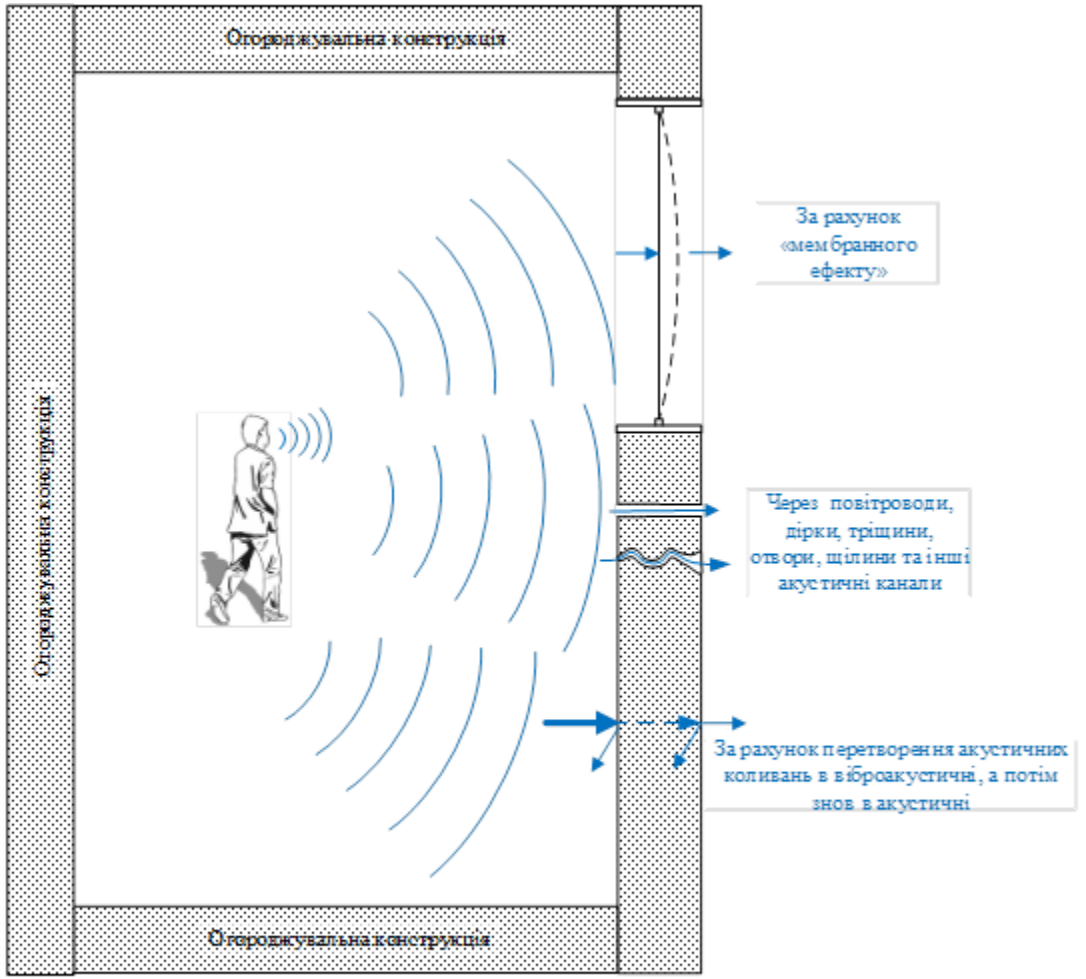


Рис. 1. Три можливих шляхи витоку акустичної інформації за межі огороджувальних конструкцій

Акустичні канали витоку інформації$_4$

- Приймання акустичної інформації можливо без використання засобів технічної розвідки при випадковому прослуховуванні (тобто без умисних дій, спрямованих на отримання цієї інформації), а також з використанням засобів технічної розвідки.
- Для перехоплення акустичної інформації можуть використовуватися високочутливі мікрофони. Якщо немає можливості застосувати такі мікрофони використовуються спрямовані мікрофони, тобто таки, які мають вузьку діаграму спрямованості.
- Перехоплена мовна інформація може записуватися на портативні записуючі пристрої (диктофони) або передаватися по радіоканалу, мережі електроживлення, оптичному каналу з'єднувальним лініям, стороннім провідникам, інженерним комунікаціям тощо.
- Схематично канали витоку акустичної інформації відображені на рисунку 2.

Акустичні канали витоку інформації$_5$

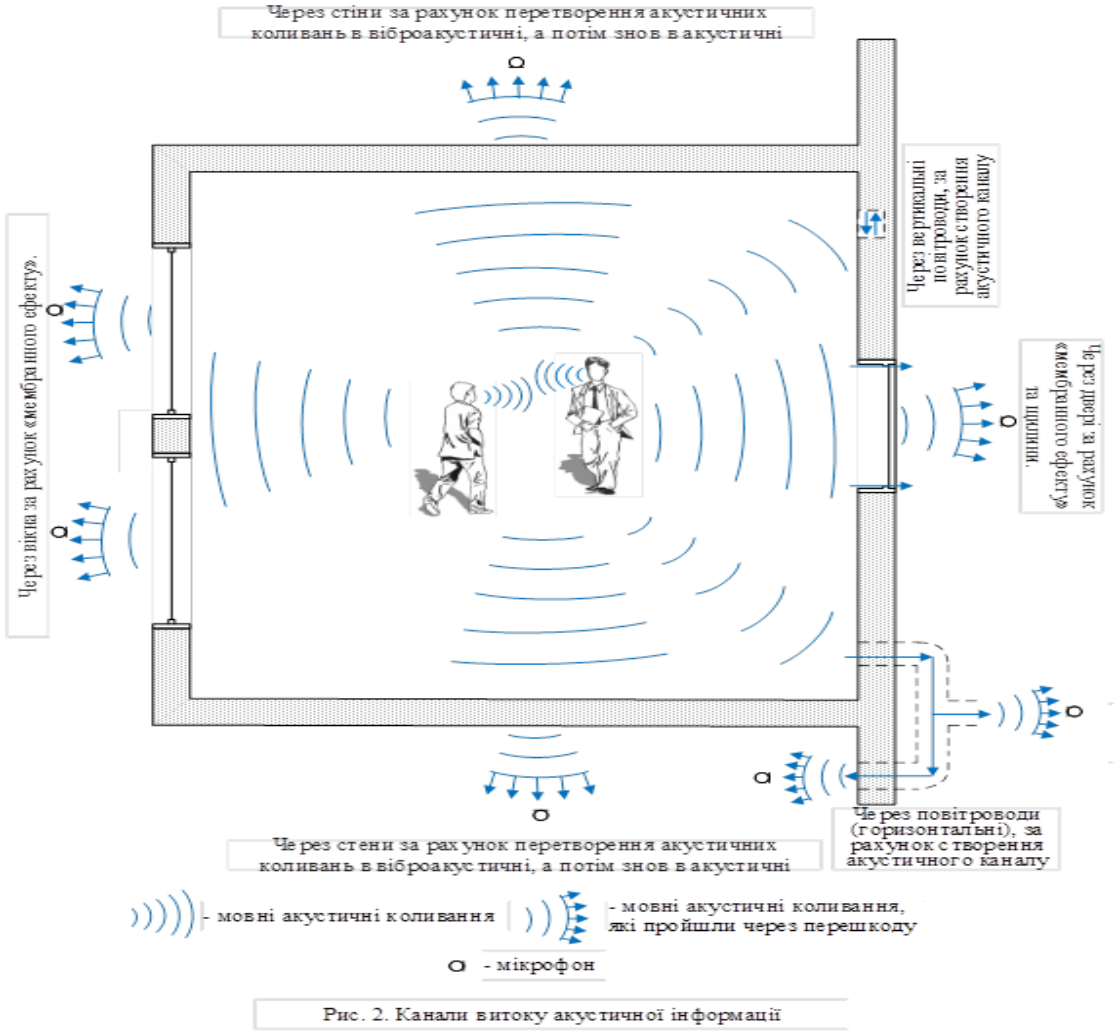


Рис. 2. Канали витоку акустичної інформації

Схема каналу перехоплення мовної інформації

Дальність дії акустичних приладів знаходиться у межах від кількох десятків метрів до кількох кілометрів і залежить від потужності акустичних сигналів та стану середовища поширення.

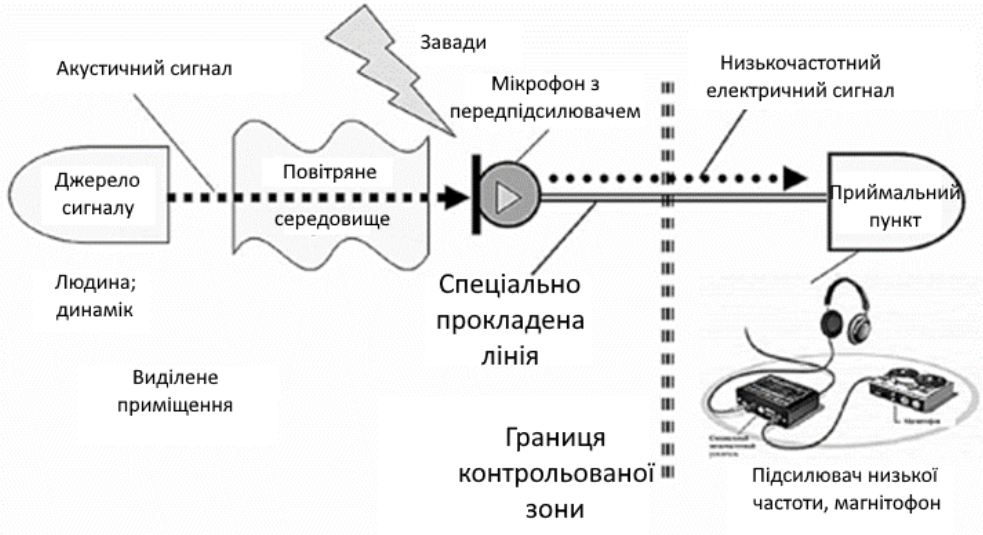
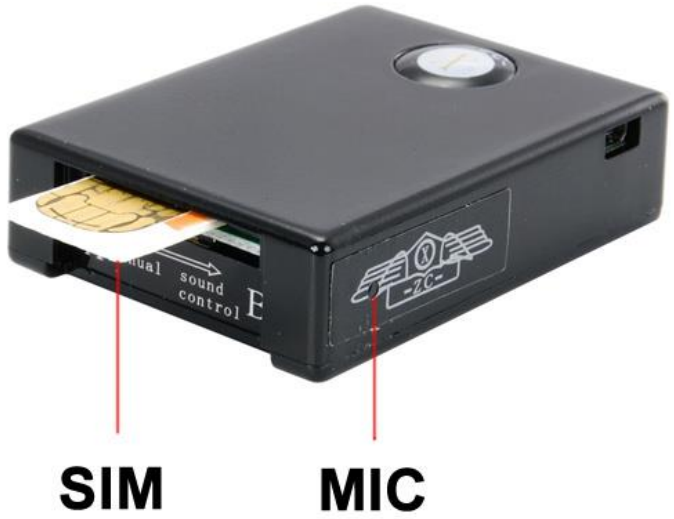


Схема каналу перехоплення мовної інформації з використанням цифрових диктофонів

Перехоплення мовної інформації

В апаратурі акустичної розвідки для перехоплення мовної інформації та її реєстрації застосовуються спрямовані мікрофони та прилади звукозапису.







Віброакустичні канали

У віброакустичних каналах витоку інформації середовищем поширення мовних сигналів є огороджувальні будівельні конструкції приміщень (стіни, вікна, двері, перекриття тощо) та інженерні комунікації. Для перехоплення мовних сигналів у цьому випадку використовують контактні мікрофони (акселерометри).

Вібродавач, з'єднаний з електронним підсилювачем називають електронним стетоскопом. Електронний стетоскоп дозволяє здійснювати прослуховування мови за допомогою голосових телефонів та її запис.

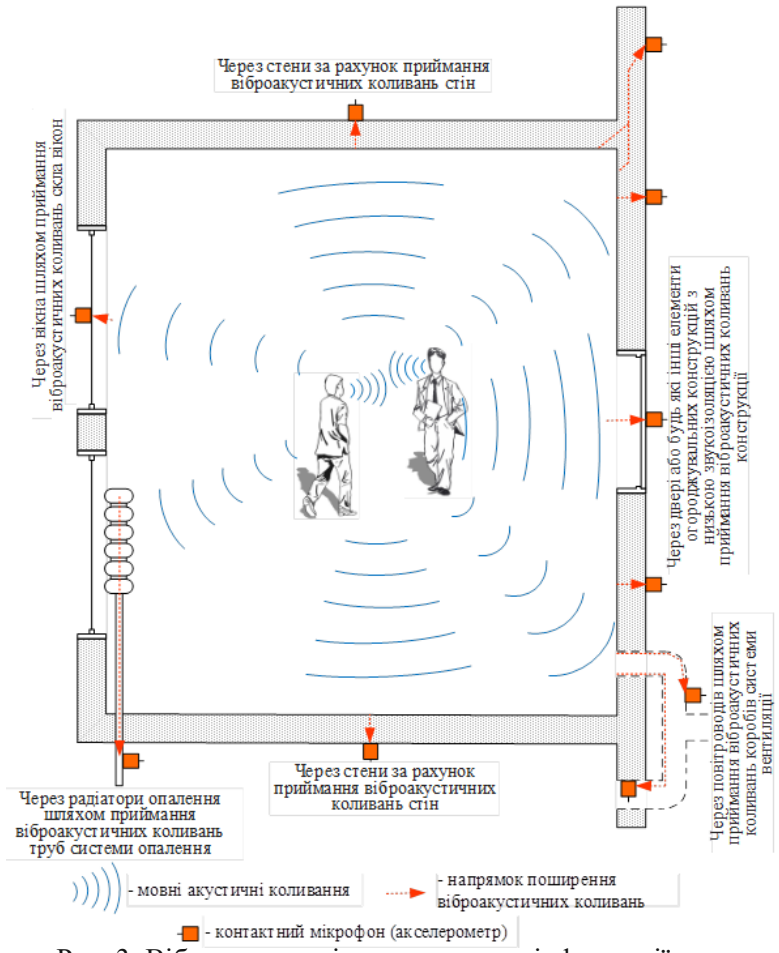


Рис. 3. Віброакустичні канали витоку інформації

Акустоелектричні канали$_1$

- Акустоелектричні канали витоку інформації виникають за рахунок перетворень акустичних каналів в електричні.
- Деякі елементи допоміжних технічних засобів і систем (ДТЗС), у тому числі трансформатори, котушки індуктивності, електромагніти вторинних годинників, телефонних дзвінків апаратів і тощо, мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу.
- Зміна параметрів призводить або до появи на даних елементах електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам згідно із змінами електричного поля.
- ДТЗС, крім зазначених елементів, можуть містити безпосередньо акустоелектричні перетворювачі. До таких відносяться деякі типи датчиків пожежної та охоронної сигналізації, гучномовці ретрансляційної мережі тощо. Ефект акустоелектричного перетворення іноді називають «мікрофонним ефектом».
- Перехоплення акустоелектричних коливань в даному каналі витоку інформації здійснюється шляхом безпосереднього підключення до з'єднувальних ліній ДТЗС спеціальних високочутливих підсилювачів низької частоти.
- Наприклад, підключаючи такі засоби до з'єднувальних ліній телефонних апаратів з електромеханічними викличними дзвінками, можна підслуховувати розмови, що ведуться в приміщеннях, де встановлені ці апарати.
- Технічний канал витоку інформації з використанням «високочастотного електромагнітного нав'язування» може бути здійснено шляхом несанкціонованого контактного введення струмів високої частоти від генератора в лінію, що має функціональні зв'язки з нелінійними або параметричними елементами ДТЗС, на яких відбувається модуляція високочастотного каналу інформаційним сигналом. Інформаційний сигнал у даних елементах ДТЗС з'являється внаслідок акустоелектричного перетворення акустичних сигналів в електричні. Промодульований сигнал відбивається від зазначених елементів і поширюється у зворотному напрямку або випромінюється.

Акустоелектричні канали,

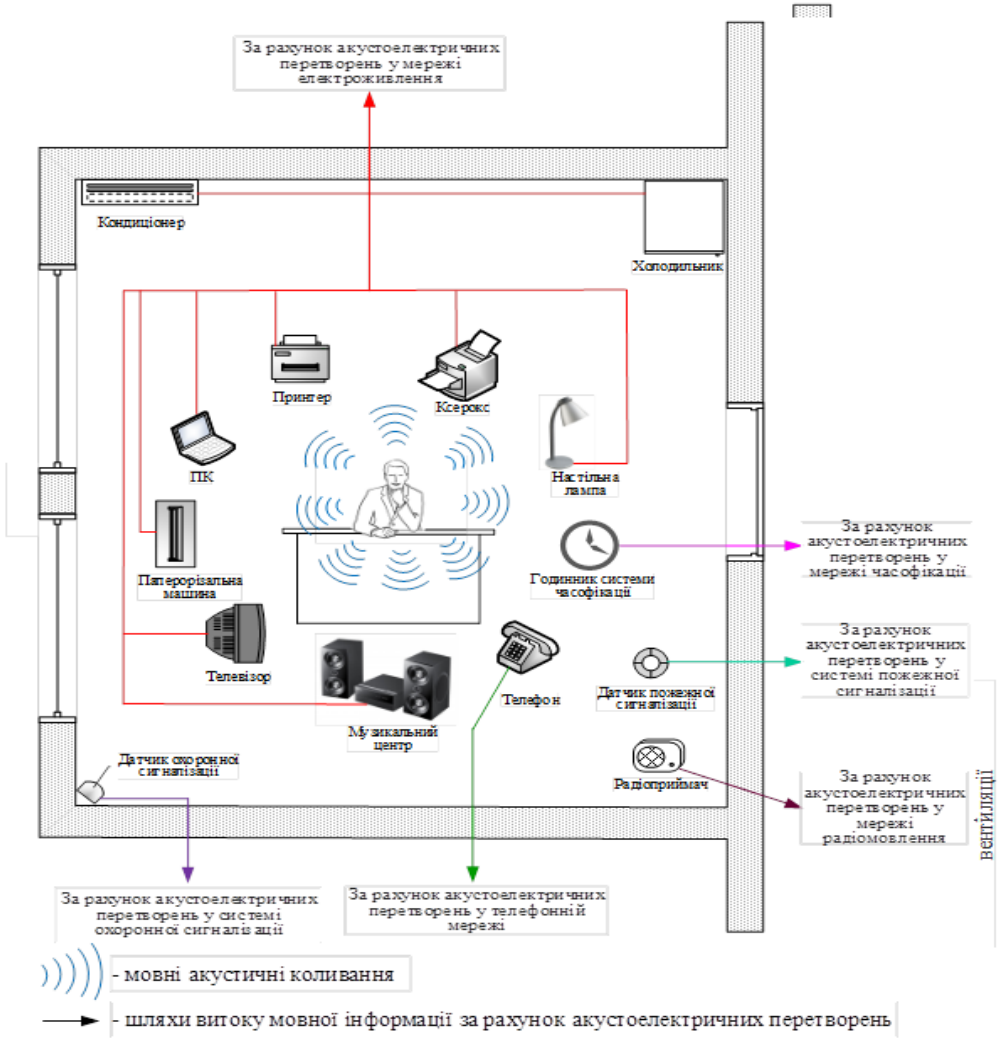


Рис. 4. Канали витоку акустичної інформації за рахунок акустоелектричних перетворювань

Оптико-електронний (лазерний) канал$_1$

- Оптико-електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих під дією акустичного мовного сигналу відбиваючих поверхонь приміщень (шибок, дзеркал тощо). Відбите лазерне випромінювання модулюється по амплітуді або фазі і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація.
- Для організації такого каналу є кращим використання дзеркального відбиття лазерного променя. Однак, при невеликих відстанях до поверхонь, що відбивають (порядку декількох десятків метрів) може бути використано дифузне віддзеркалення лазерного випромінювання.
- Для перехоплення мовної інформації з даного каналу використовуються складні лазерні системи - «лазерні мікрофони», які працюють, як правило в ближньому інфрачервоному діапазоні довжин хвиль.

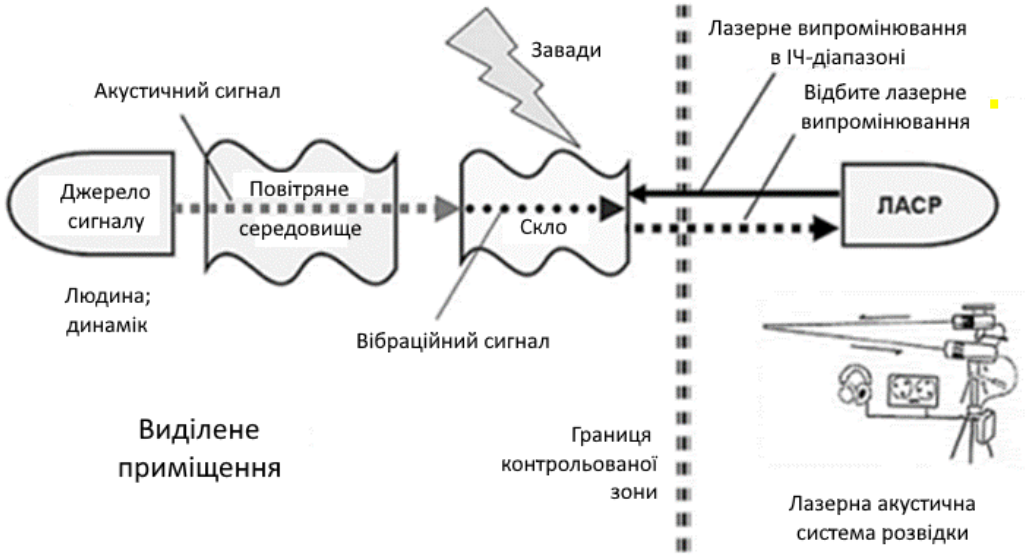


Схема каналу перехоплення мовної інформації з використанням лазерної акустичної системи

Оптико-електронний (лазерний) канал$_2$

- Головною ПЕРЕВАГОЮ лазерних акустичних систем над іншими засобами розвідки є те, що вони дозволяють вирішувати задачі знімання мовної інформації максимально безпечно для зловмисника, оскільки виключається необхідність проникнення у приміщення з метою розміщення там закладних пристроїв.

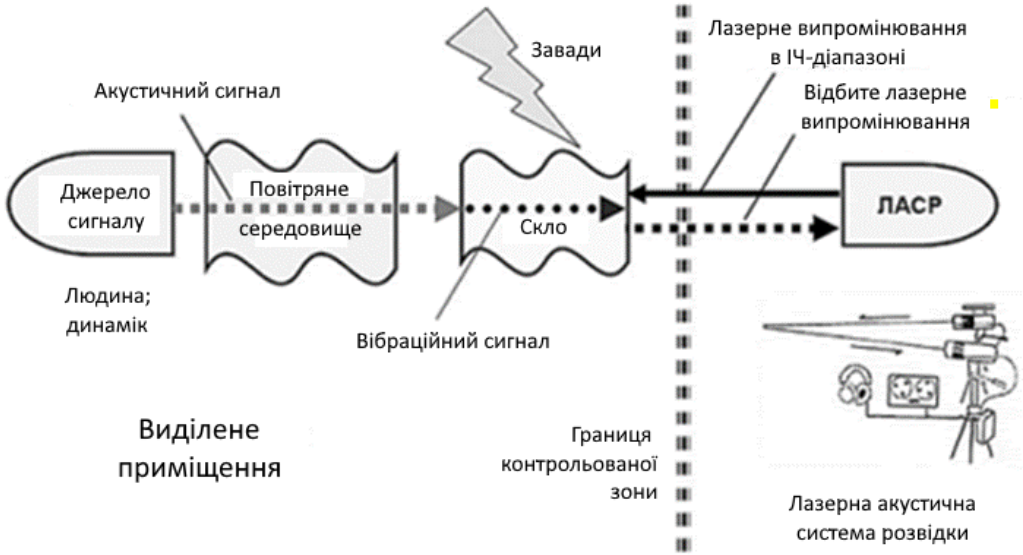


Схема каналу перехоплення мовної інформації з використанням лазерної акустичної системи

Джерела утворення акустичного каналу витоку інформації

Джерела утворення акустичного каналу витоку інформації вібрують ті елементи, що коливаються, і механізми, такі як голосові зв'язки людини, рухомі елементи машин, телефонні апарати, звукопідсилювальні системи і т.д.

Для мовних сигналів критерієм захищеності слід вважати встановлену величину розбірливості мови

Розбірливість мови визначається ставленням сигнал/шум та широтою смуги мовного сигналу

Класифікація акустичних каналів витоку інформації



Поширення звуку у просторі

Поширення звуку у просторі здійснюється звуковими хвилями. *Пружними*, або *механічними хвилями* називаються механічні обурення (деформації), що поширюються в пружному середовищі. Тіла, які, впливаючи на середу, викликають ці обурення, називають джерелами хвиль. Поширення пружних хвиль у середовищі пов'язані з перенесенням речовини. У необмеженому середовищі воно полягає у залученні у вимушені коливання дедалі більше віддалених джерела хвиль частин середовища. Пружна хвиля є поздовжньою і пов'язана з об'ємною деформацією пружного середовища, внаслідок чого може поширюватися в будь-якому середовищі — твердому, рідкому та газоподібному.

Коли у повітрі поширюється акустична хвиля, його частинки утворюють пружну хвилю і набувають коливального руху, поширюючись на всі боки, якщо на їх шляху немає перешкод. В умовах приміщень чи інших обмежених просторів по дорозі звукових хвиль виникає безліч перешкод, куди хвилі надають змінний тиск (двері, вікна, стіни, стелі, підлоги тощо), наводячи коливальний режим. Цей вплив звукових хвиль є причиною утворення акустичного каналу витоку інформації.

Утворення акустичних каналів витоку інформації

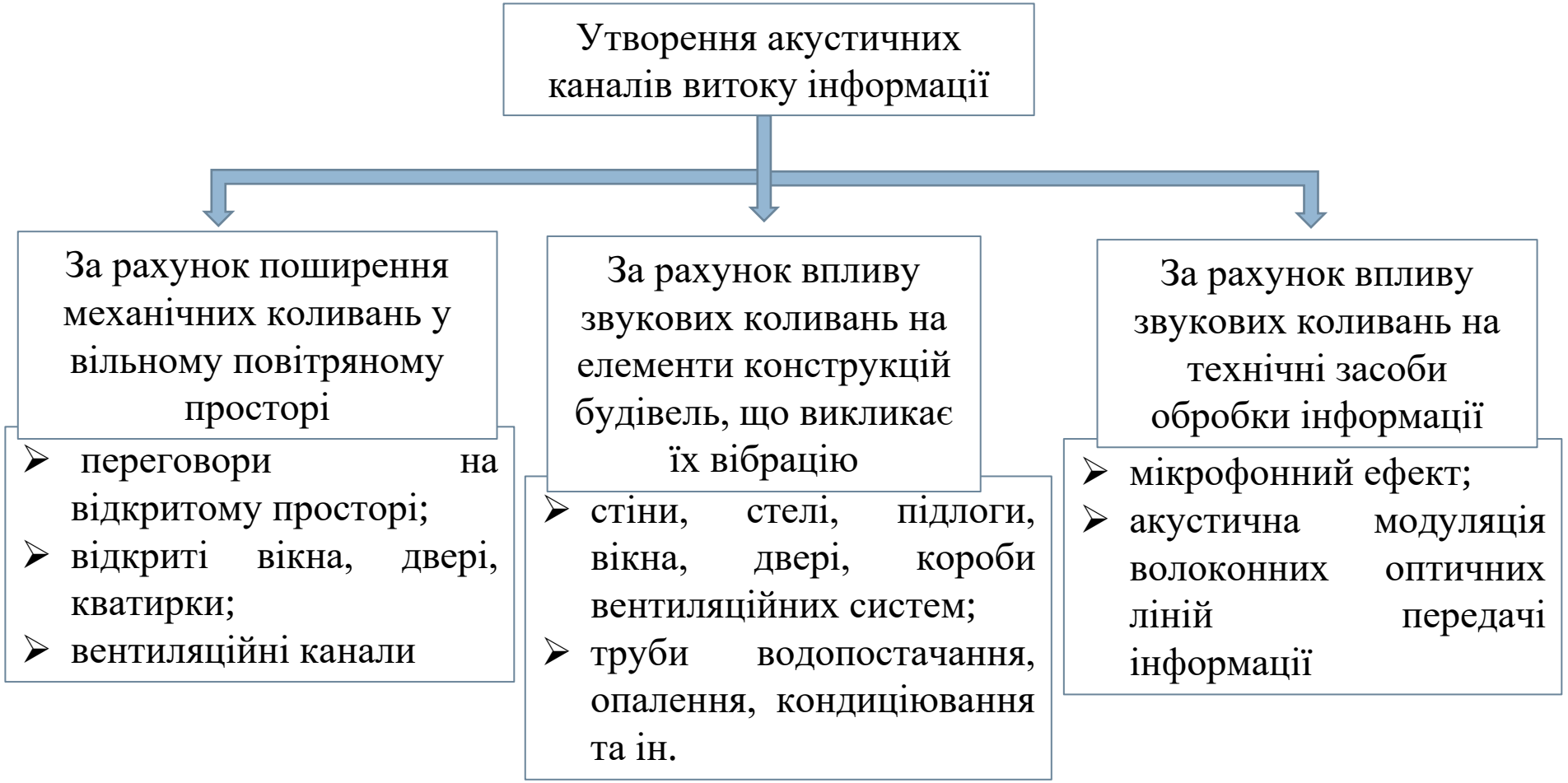
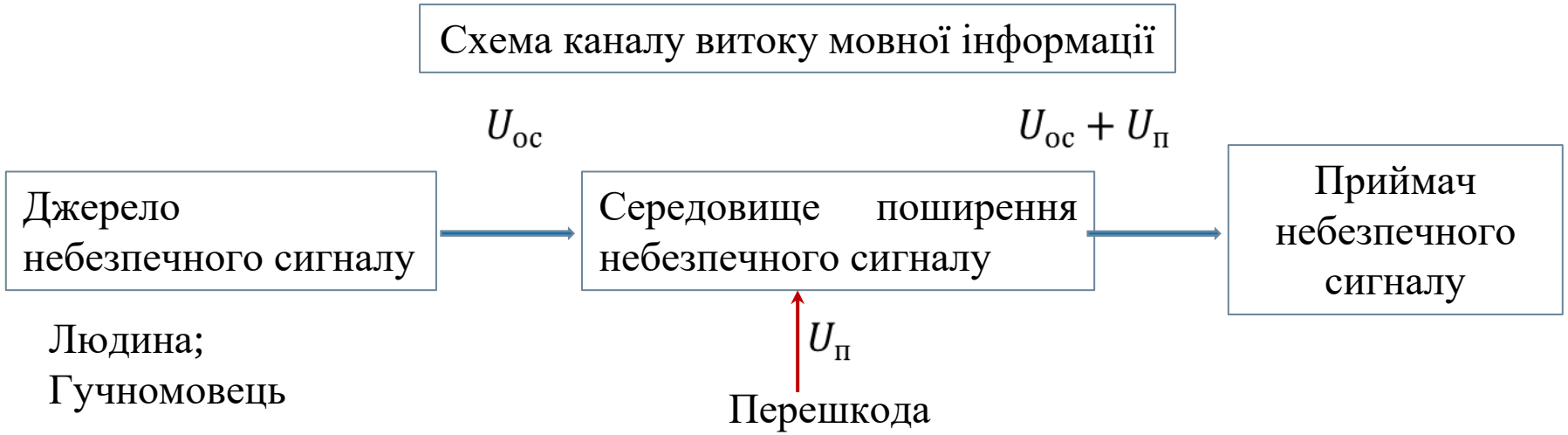


Схема каналу витоку мовної інформації



При цьому

$$N = L_P = 20 \lg \frac{P_c}{P_o}, \text{ а } P_c = 2 \bullet 10^{-5}\, 10^{\frac{L_p\,[\text{дБ}]}{20}}\,[\text{Па}]$$

Перенесення звукових хвиль

Середовища поширення мовної інформації щодо способу перенесення звукових хвиль

- з повітряним перенесенням
- з матеріальним перенесенням (моноліт)
- з мембранним перенесенням (коливання скла)

Середовище поширення визначає звукоізоляцію, що характеризується *коефіцієнтом звукопроникності* :

$$\tau_\theta = \frac{P_{пройшов}}{P_{надійшов}}$$

Дифузне поле - це результат накладання множини плоских хвиль з випадковими напрямками фаз амплітуд (однорідних, просторових) від різних джерел. Кількість джерел для створення дифузного поля

для дифузного поля

$$\tau = \int_0^{90^0} \tau_o \sin 2\theta \, d\theta$$

$$n \approx 10 \frac{L_\Sigma - L_n}{10}, \text{ іноді } L_\Sigma = L_{падаюче}$$

Акустична розвідка

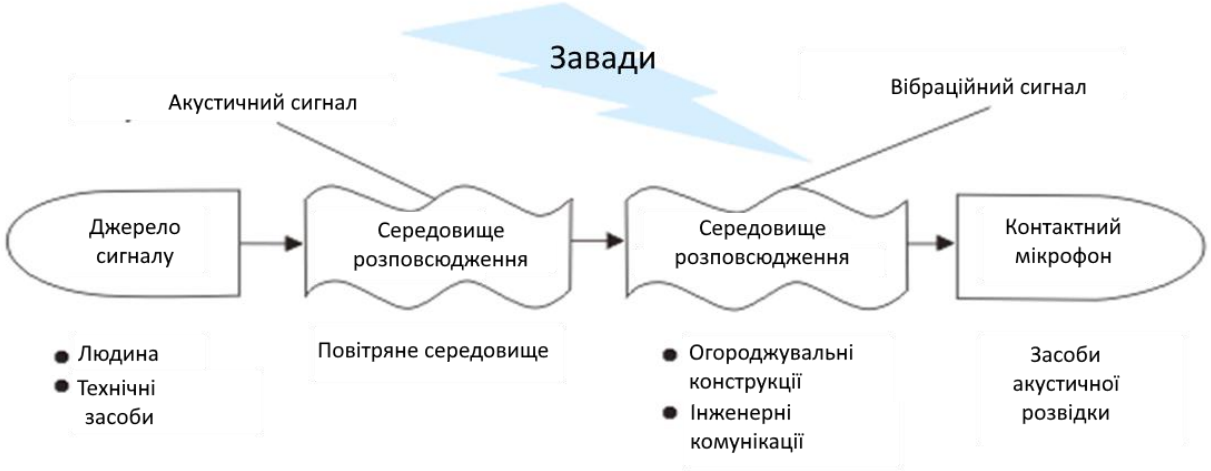
Канали розвідки 1

Повітряні канали. У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, а для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні направлені мікрофони.

Вібраційні канали. У вібраційних (структурних) каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації та інші тверді тіла. Для перехоплення акустичних коливань у разі використовуються контактні мікрофони (стетоскопи).

Електроакустичні канали. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів електричні. Перехоплення акустичних коливань здійснюється через допоміжні технічні засоби та системи (ДТЗС), що мають "мікрофонний ефект", а також шляхом "високочастотного нав'язування ".

Середовище розповсюдження



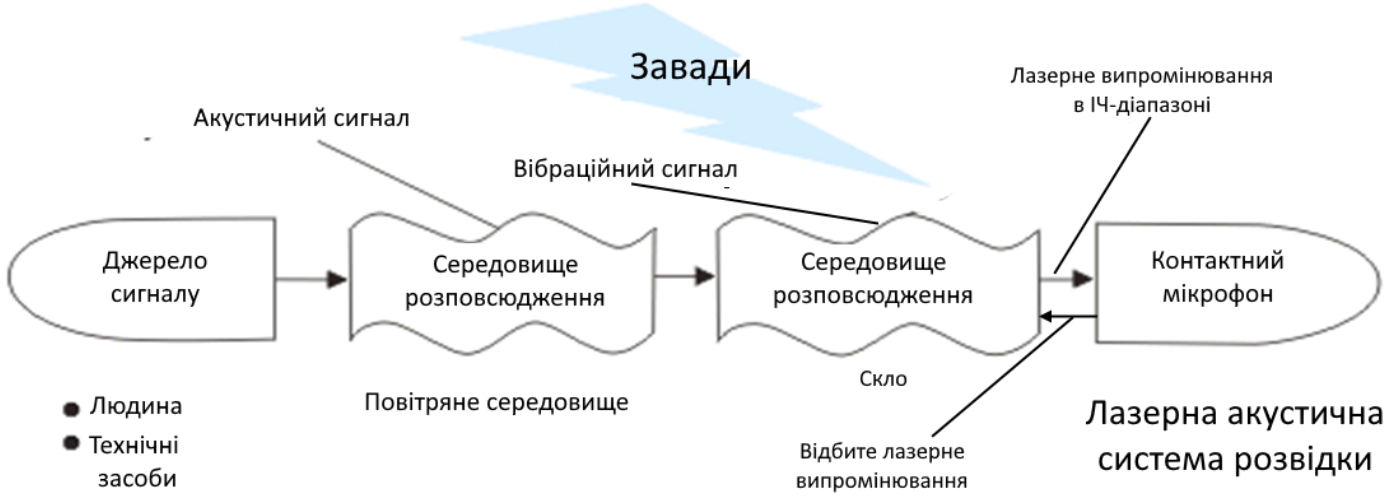
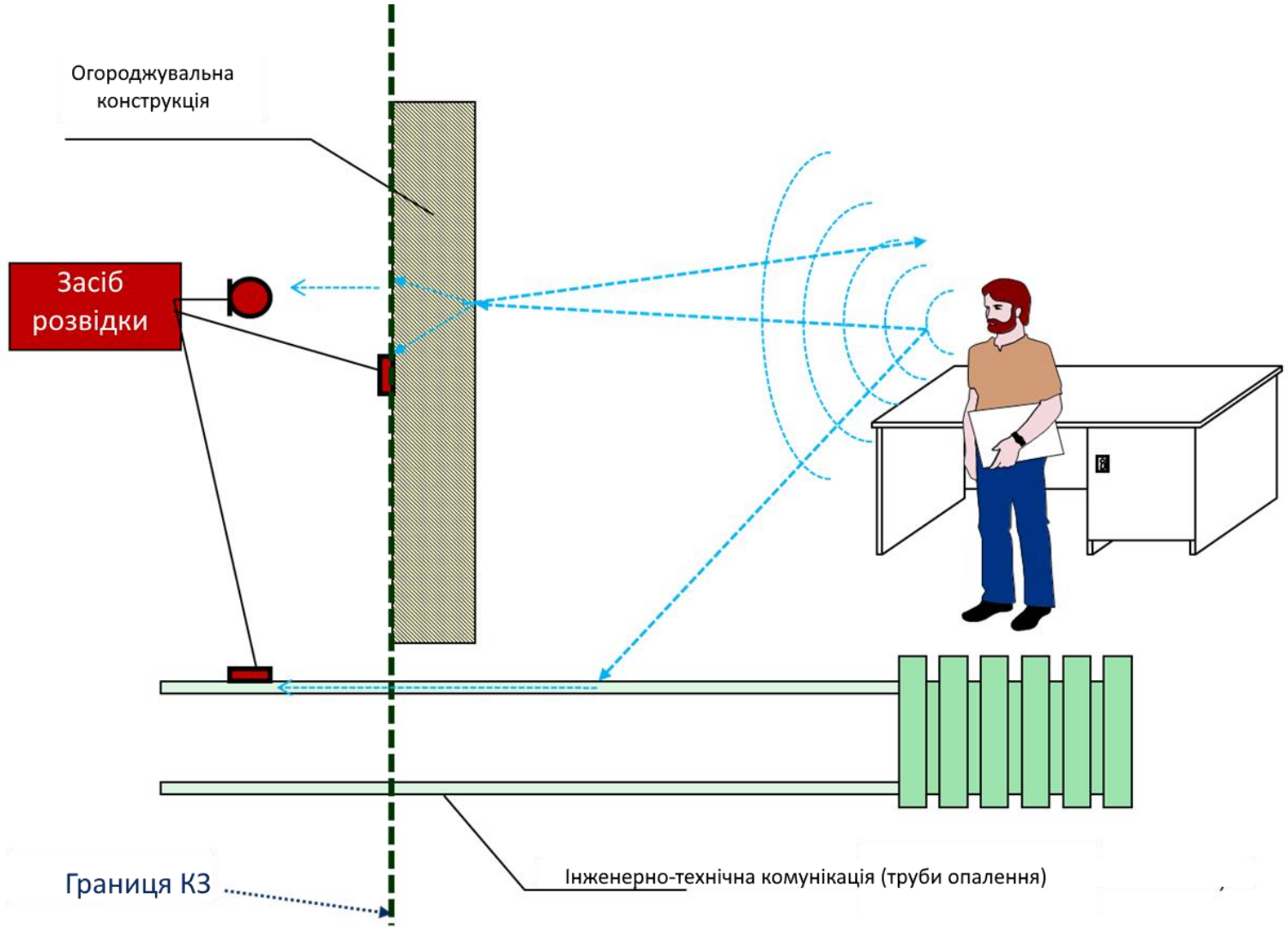


Схема розвідки



Канали розвідки 2

Оптико-електронний канал. Оптико-електронний (лазерний) канал витоку інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відбивають (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді та фазі (за законом вібрації поверхні) та приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Параметричні канали. Внаслідок впливу акустичного поля змінюється тиск на всі елементи високочастотних генераторів ТСПІ та ВТСС. При цьому змінюється (незначно) взаємне розташування елементів схем, проводів у котушках індуктивності, дроселів тощо, що може призвести до змін параметрів високочастотного сигналу, наприклад, модуляції його інформаційним сигналом.

Схема розвідки лазерним каналом

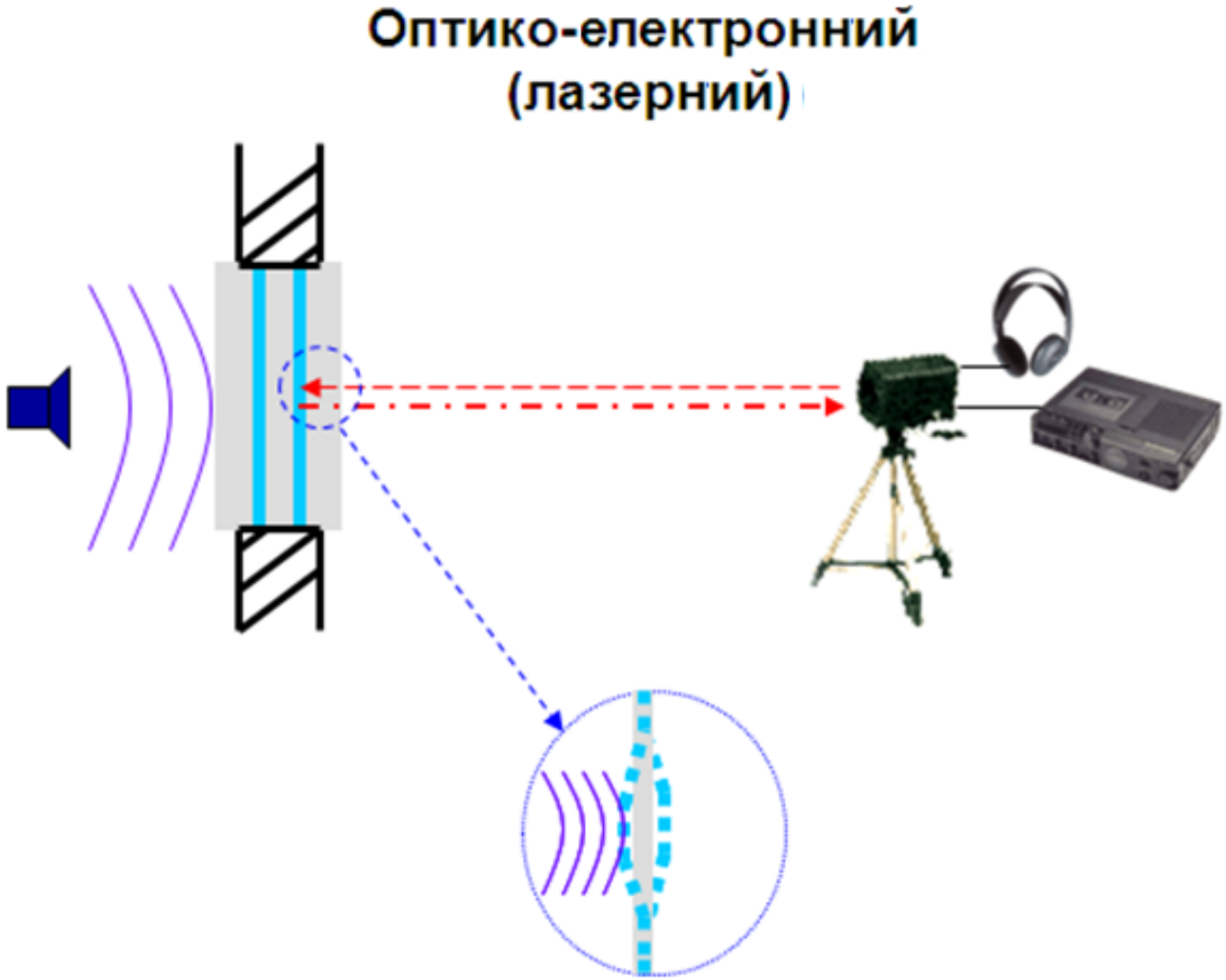
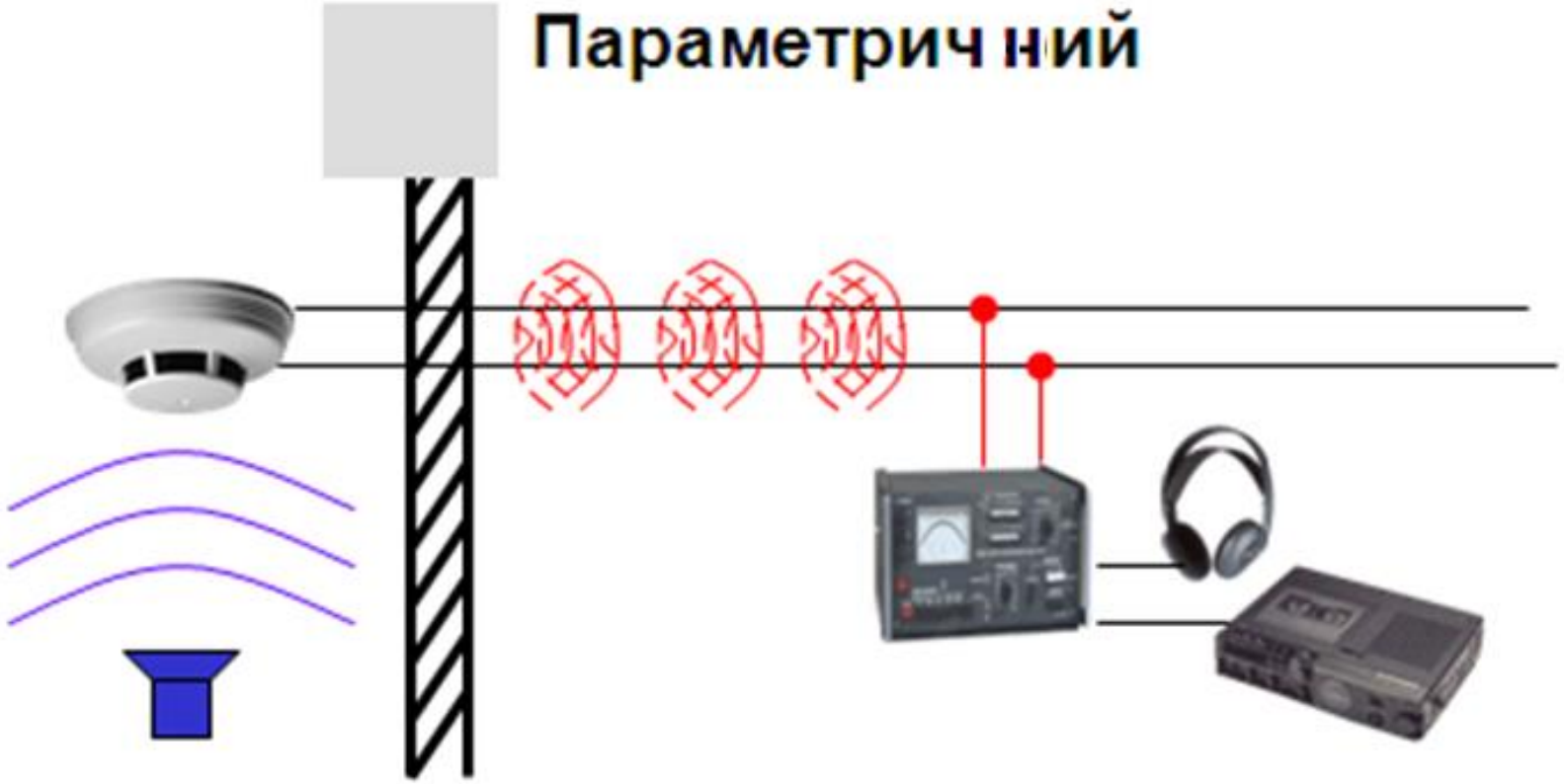


Схема розвідки параметричним каналом



Методи перехоплення інформації

В акустичній розвідці використовуються :

- ❑ пасивні методи перехоплення;
- ❑ активні методи перехоплення;
- ❑ контактні методи перехоплення.

За способом застосування технічні засоби знімання акустичної інформації можна класифікувати в такий спосіб. Засоби, що встановлюються закладними (тобто потребують таємного фізичного проникнення на об'єкт) методами :

- радіозакладки;
- закладки з передачею акустичної інформації інфрачервоним діапазоном;
- закладки з передачею інформації мережею 220В;
- закладки з передачею акустичної інформації телефонною лінією;
- диктофони;
- провідні мікрофони;
- “телефонне вухо”.

Засоби, які встановлені беззакладними методами:

- апаратура, яка має мікрофонний ефект;
- високочастотне нав'язування;
- стетоскопи;
- лазерні стетоскопи;
- спрямовані мікрофони.

Закладні та беззакладні методи

Закладні методи$_1$

Перехоплення акустичної інформації за допомогою радіопередавальних засобів
До них належить широка номенклатура радіозакладок (радіомікрофонів, "жучків"), призначенням яких є передача радіоканалом акустичної інформації, що отримується на об'єкті.

Перехоплення акустичної інформації за допомогою ІЧ передавачів
Передача інформації може здійснюватися інфрачервоним (ІЧ) каналом. Акустичні закладки даного типу характеризуються надзвичайною складністю їх виявлення.

Закладки, що використовують як канал передачі акустичної інформації через мережу 220 В та телефонні лінії

Перевага цих закладок у тому, що використовують вони у своїй роботі принцип низькочастотного ущільнення каналу передачі. Оскільки в “чистих” лініях (220 В) та телефонних лініях присутні лише сигнали на частотах 50 Гц та (300–3500) Гц відповідно, то передавачі таких закладок, транслюючи свою інформацію на частотах (100–250) кГц, не заважають роботі цих мереж.

Диктофони
Диктофони – пристрої, що записують голосову інформацію на електронні носії. Час запису різних диктофонів коливається в межах від 15 хв. до 8 год.

Закладні методи$_2$

Дротові мікрофони

Дротові мікрофони встановлюються в приміщенні, що цікавить, і з'єднуються провідною лінією з приймальним пристроєм. Мікрофони встановлюються або потайно (немасковані), або маскуються під предмети побуту, офісної техніки і т.д. Такі системи забезпечують передачу аудіосигналу на дальність до 20 м. При використанні активних мікрофонів — до 150 м.

“Телефонне вухо”

Цей пристрій зазвичай монтується або в телефоні, або в телефонній розетці.

Людина, яка хоче скористатися цим пристроєм (оператор), здійснює телефонний дзвінок за номером, на якому він "висить". “Телефонне вухо” (“ТВ”) “ковтає” перші два дзвінки, тобто у контрольованому приміщенні телефонні дзвінки не лунають. Оператор кладе трубку та знову набирає цей номер. У трубці звучатиме сигнал "зайнято", оператор чекає 30-60 с (тимчасовий пароль) і після припинення сигналу "зайнято" набирає біпером (генератором DTMF-посилок) задану кодову комбінацію (цифровий пароль). Після цього включається мікрофон "ТВ" і оператор чує все, що відбувається в контрольованому приміщенні практично з будь-якої точки світу, де є телефон. Розрив зв'язку станеться, якщо оператор покладе трубку або якщо хтось підніме телефонну трубку у контрольованому приміщенні. Для решти абонентів, які бажають додзвонитися за цим номером, буде чути сигнал "зайнято".

Беззакладні методи

Апаратура, що використовує мікрофонний ефект телефонних апаратів
Прослуховування приміщень через телефон здійснюється за рахунок використання мікрофонного ефекту.

Апаратура високочастотного нав'язування
Високочастотні коливання проходять через мікрофон або деталі телефону, що володіють мікрофонним ефектом і модулюються в акустичний сигнал з приміщення, де встановлений телефонний апарат. Промодульований сигнал демоделюється амплітудним детектором і після посилення подається на пристрій, що реєструє.

Стетоскопи це пристрої, що перетворюють пружні механічні коливання твердих фізичних середовищ на акустичний сигнал. Стетоскопи контролюють віброакустичні сигнали, що розповсюджуються по будівельних конструкціях будівель, інженерних комунікацій.

Лазерні системи акустичної розвідки
Лазерна система акустичної розвідки (ЛСАР) забезпечує знімання мовної інформації з гарною якістю із віконних рам з подвійним склом на відстані до 250 м.

Направлені акустичні мікрофони (НАМ)
Дана техніка призначена для прослуховування акустичної інформації з певного напрямку та з великих відстаней.

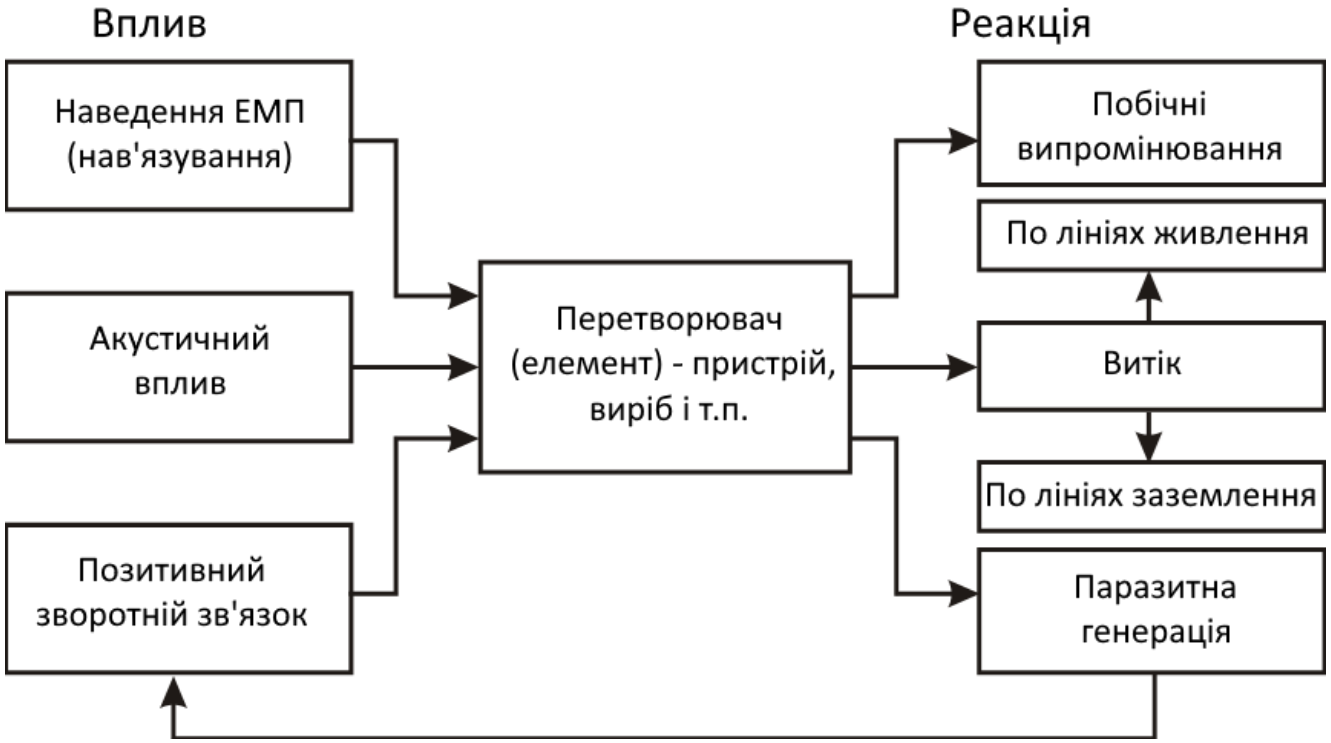
Фізичні перетворювачі

Фізичні перетворювачі$_1$

- У будь-яких технічних засобах існують ті чи інші фізичні перетворювачі, що виконують відповідні їм функції, які ґрунтуються на певному фізичному принципі дії.
- Гарне знання всіх типів перетворювачів дозволяє вирішувати завдання визначення наявності можливих неконтрольованих проявів фізичних полів, що утворюють канали витоку інформації.
- **Перетворювачем є прилад**, який трансформує зміну однієї фізичної величини на зміну іншої.
- У термінах електроніки перетворювач зазвичай визначається як прилад, що перетворює неелектричну величину на електричний сигнал або навпаки

Фізичні перетворювачі$_2$

ХАРАКТЕРИСТИКИ ФІЗИЧНИХ ПЕРЕТВОРЮВАЧІВ



Кожен перетворювач діє за певними фізичними принципами та утворює властивий цим принципам передавальний канал - тобто. канал витоку інформації

Параметри перетворювачів

ВИДИ ДАВАЧІВ

- спеціально розроблені для створення необхідного електричного сигналу;
- випадкові, що є результатом недосконалості схеми чи пристрою.

ПОДІЛ ДАВАЧІВ ЗА ФОРМОЮ ПЕРЕТВОРЕННЯ

- перетворювачі сигналів;
- перетворювачі енергії.

ПАРАМЕТРИ ПЕРЕТВОРЮВАЧІВ

Роздільна здатність, що характеризує найбільшу точність, з якою здійснюється перетворення.

Чутливість. Це відношення зміни величини вихідного сигналу до зміни сигналу на його вході.

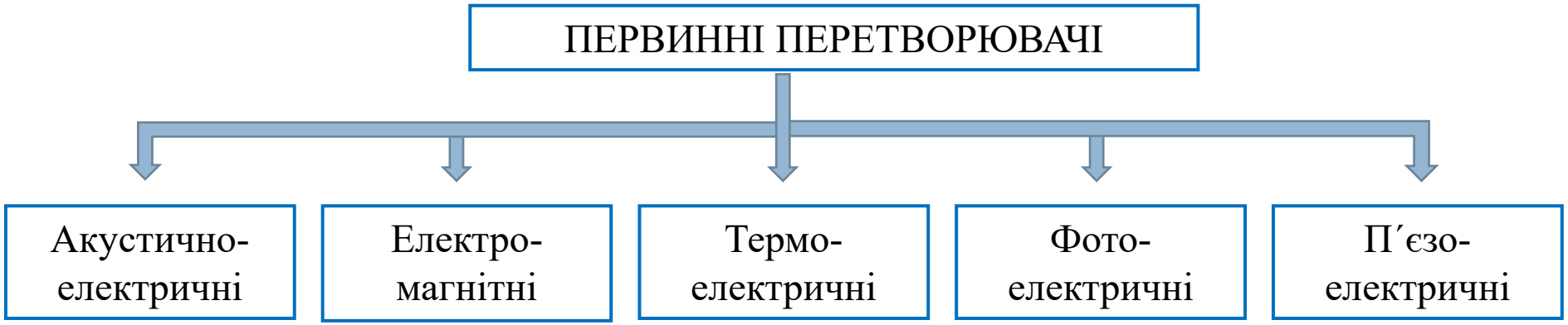
Лінійність. Характеризує рівномірність зміни вихідного сигналу залежно від зміни вхідного.

Інертність, або **час відгуку**, який дорівнює часу встановлення вихідного сигналу у відповідь на зміну вхідного сигналу.

Смуга частот. Ця характеристика показує, на яких частотах на вході ще сприймаються перетворювачем, створюючи на виході ще допустимий рівень сигналу.

Первинні перетворювачі

ПОДІЛ ПЕРЕТВОРЮВАЧІВ ЗА ФІЗИЧНОЮ ПРИРОДОЮ

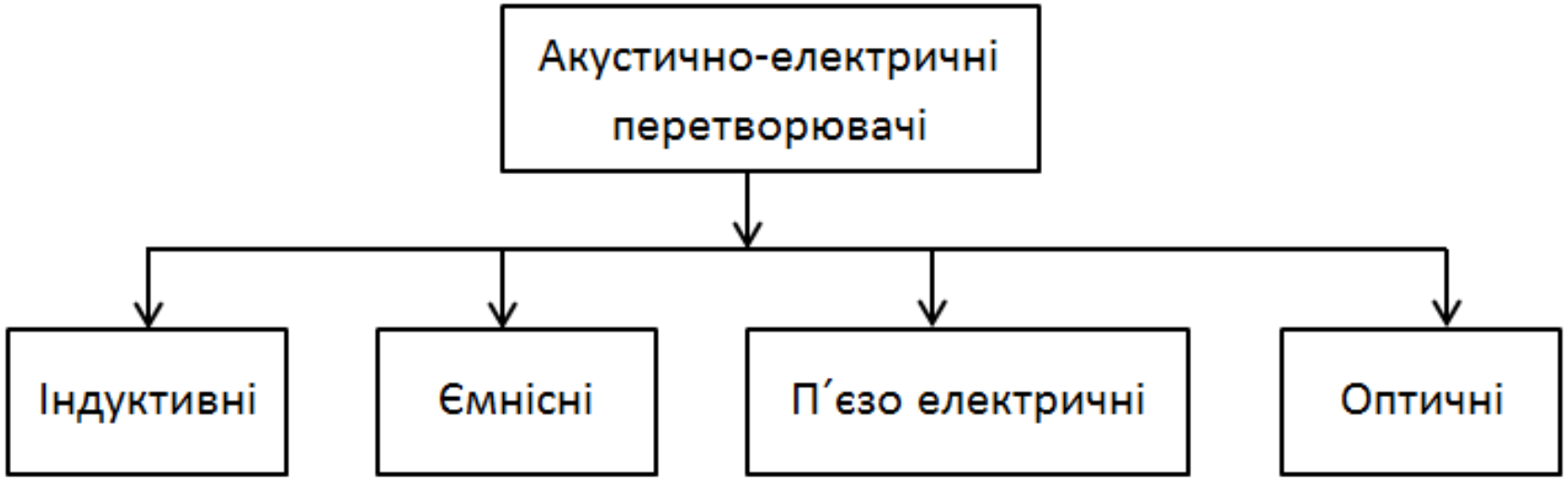


Акустично-електричні перетворювачі

Акустична енергія, що виникає під час звучання мови, може спричинити механічні коливання елементів електронної апаратури, що у свою чергу призводить до появи електромагнітного випромінювання або його зміни за певних обставин.

Найбільш чутливими до акустичних впливів елементами радіоелектронної апаратури є котушки індуктивності та конденсатори змінної ємності.

Види акустично-електричних перетворювачів



Дзвінок ТФ

Електромеханічний дзвінок телефонного апарату — типовий представник індуктивного акустично-електричного перетворювача, мікрофонний ефект якого проявляється при покладеній мікротелефонній трубці.

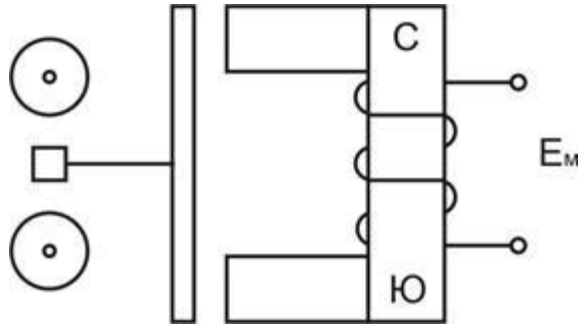


Схема виклику дзвінка

ЕРС (електро-рушивна сила) мікрофонного ефекту дзвінка може бути визначена за формулою:

$$E_{МЭ} = \eta p$$

де p – акустичний тиск;
$\eta = FS\mu 0wSI/d2zM$ – акустична чутливість дзвінка;
F — магніторушивна сила постійного магниту;
S — площа якорю (пластини); m0 — магнітна проникність сердечника; w — число витків котушки; Sμ — площа плоского наконечника; d — значення зазору; zM — механічний опір.

Слід зазначити, що ЕРС мікрофонного ефекту виникає і може використовуватися у стані спокою приладу, коли він не використовується для конкретних вимірювань.

Ємнісні перетворювачі$_1$

Ємнісні перетворюючі елементи перетворюють зміну ємності зміну електричного потенціалу, струму, напруги. Для найпростішого конденсатора, що складається з двох пластин, розділених шаром діелектрика (повітря, парафін та ін.), ємність визначається за формулою

$$C = \frac{\varepsilon S}{d}$$

де ε — діелектрична проникність діелектрика; S — площа поверхні кожної пластини; d — відстань між пластинами.

З цього співвідношення випливає, що ємність конденсатора залежить від відстані між пластинами. При наявності в ланцюгу ємності постійного джерела струму і навантаження акустичне тиск, що впливає на пластини, змінюючи відстань між пластинами, призводить до зміни ємності. Зміна ємності призводить до зміни опору ланцюга і, відповідно, зміни опору і падіння напруги на опорі навантаження пропорційно акустичному тиску. Ці залежності використовуються в конструкції конденсаторних мікрофонів.

Ємнісні перетворювачі$_2$

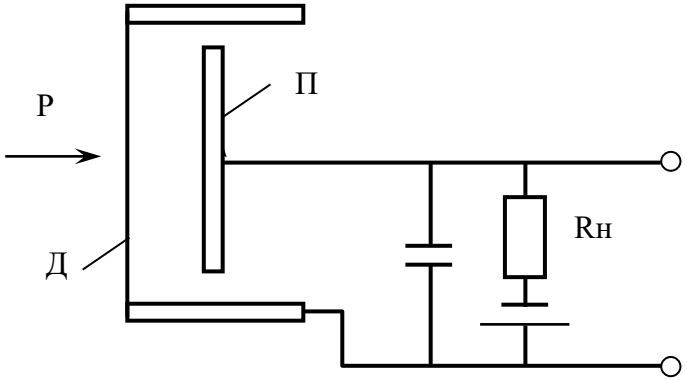
Коли на мікрофон діє хвиля звукового тиску *Р*, діафрагма *Д* рухається щодо нерухомого електрода — жорсткої пластини *П*. Цей рух викликає зміну змінної електричної ємності між діафрагмою та задньою пластиною, а отже, виробляє відповідний електричний сигнал на виході.

Конденсатори змінної ємності з повітряним діелектриком є одним з основних елементів коливальних контурів генераторних систем, що перебудовуються. Вони влаштовані так, що система пластин всувається до іншої системи пластин, що утворюють конденсатор змінної ємності.
На такий конденсатор акустичне тиск виявляється досить просто, змінюючи його ємність, а, отже, і характеристики пристрою, в якому він встановлений, призводячи до появи неконтрольованого каналу витоку інформації.

Вплив небезпечних акустичних сигналів на технічні системи

Технічна система

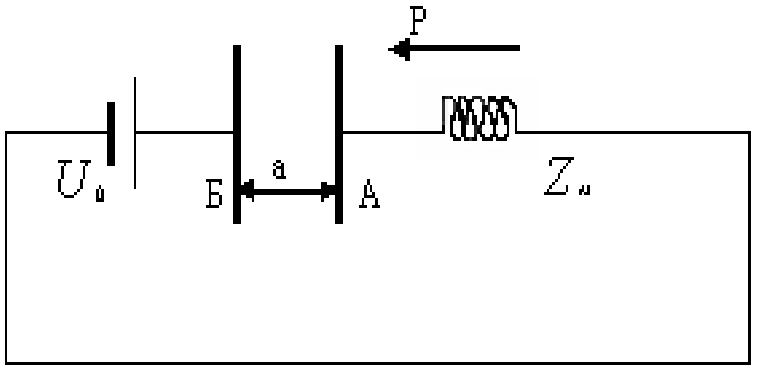
Технічні системи, що знаходяться в зоні дії небезпечних акустичних сигналів, нерідко є причиною витоку секретної інформації за межі контрольованої зони. Це відбувається за наявності в технічних системах елементів, що мають мікрофонні властивості. Такі елементи перетворюють акустичні коливання на електричні сигнали, що утворюють, канали ПЕМВ (побічні електромагнітні випромінювання).



Пристрій конденсаторного мікрофона

Електростатична система$_1$

Найпростішим перетворювачем цієї системи є конденсатор, одна пластина якого (А) рухлива, а інша (Б) закріплена нерухомо



Еквівалентна схема утворення електричної системи

Акустична чутливість у цьому випадку визначається за формулою

$$U_0 \frac{S}{w Z_m a}$$

де U0 - застосована до пластин напруга;

S – площа пластин;

a - зазор між пластинами Zm – опір пластин;

w - частота поля впливу

Електростатична система$_2$

Механічний опір одноконтурної механічної системи описується «механічним» законом Ома

$$Z_{\text{м}} = \frac{F}{V} =, r + j\left(wm - \frac{1}{wC_{\text{м}}}\right)$$

де r – активний опір (тертя), мехОм;

$C_{\text{М}}$ – гибкость, м/Ньютон.

m – маса рухомої пластини, кг;

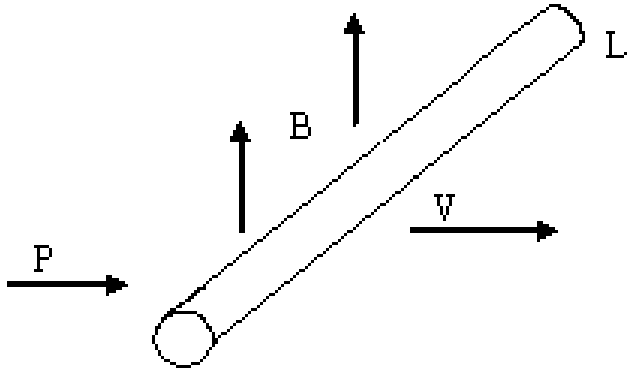
Для отримання ефекту перетворення в цій системі необхідно на пластини подати напругу. Прикладами пристроїв, що працюють за принципом електростатичних систем, є пластини реле.

Описана система також моделює поведінку монтажних проводів або електричних деталей плат, розташованих біля металевого корпусу технічного засобу.
Зменшити чутливість у такій системі можна шляхом збільшення зазору конденсатора, що утворився, зменшення площі його пластин і збільшення механічного опору системи за допомогою заливання провідників на платі спеціальним компаундом і жорсткого кріплення самої плати на металевому підставі.

Електродинамічна система

При русі провідника довжиною L в постійному магнітному полі з індукцією B зі швидкістю V у провіднику з'являється індукція е.р.с. сигналу

$$U_{\text{ист}} = BLV$$



Індукція ЕРС у провіднику

Враховуючи, що коливальна швидкість дорівнює чинній на провідник силі, поділеній на механічний опір

$$V = \frac{F}{Z_{\text{м}}}$$

і що сила визначається добутком тиску на площу провідника

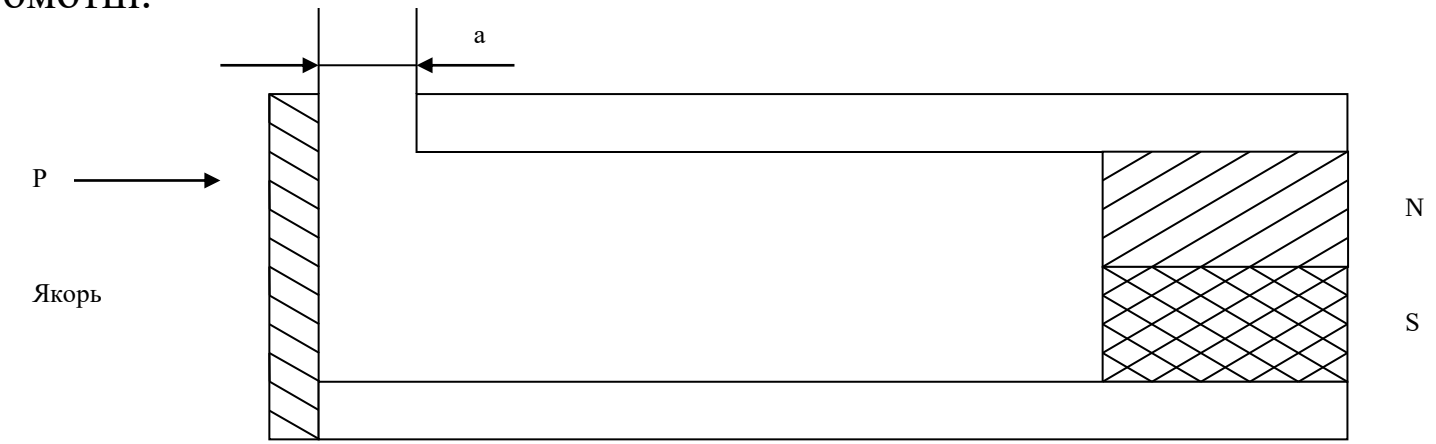
$$F = PS$$

Отримаємо рівняння для визначення акустичної чутливості у такій системі

$$\eta = \frac{BLS}{Z_{\text{м}}}$$

Електромагнітна система$_1$

Принцип перетворення полягає в індукуванні е.р.с. сигналу в обмотці електромагнітної системи за зміни магнітного потоку. Магнітний ланцюг перетворювача містить постійний магніт NS з полюсним наконечниками і гнучку пластину (якір) з феромагнітного матеріалу, один кінець якої закріплений на полюсному наконечнику, якщо якір буде приведений в коливальний рух під дією сили, це призведе до зміни зазору і відповідно до зміни магнітного потоку і появи е.р.с. в обмотці.



Зміна магнітного потоку та поява е.р.с. в обмотці системи

Електромагнітна система$_2$

Рівняння чутливості має вигляд $$\eta = \frac{\Phi \mu_0 Ssw}{a^2 Z_м}$$

де s – площа полюсного наконечника з боку зазору;
S – площа якоря;
Φ – магніторушійна сила постійного магніту.

Прикладами перетворювачів електромагнітної системи є електромагнітні реле, електричні дзвінки, електромагнітні телефонні капсулі та ін. В описаних системах нерідко неможливо зменшити акустичну чутливість при збереженні необхідних робочих параметрів. Слід враховувати і те, що в пристроях, що працюють за цим принципом при подачі в обмотку постійного струму зменшується зазор в a^2 разів збільшується акустична чутливість. Реально шляхом подачі постійного струму в обмотку деяких реле вдається приблизно на порядок збільшувати їхню чутливість до звукового поля. Цей ефект слід враховувати при визначенні необхідного згасання захисту.

Донецький національний технічний університет



Тема 5. Розвідка та добування інформації. Лекція 15. Радіоелектронна розвідка.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.

Лекційні питання

- Загальні положення
- Основні вимоги
- Класифікація РЕР
- Радіорозвідка
- Радіотехнічна розвідка
- Радіолокаційна розвідка

Загальні положення

Радіотехнічна розвідка

- **Радіоелектронна розвідка (РЕР; англ. Electronic signals intelligence (ELINT))** — вид технічної розвідки.
- Добування розвідувальних відомостей про противника (об’єкт) шляхом перехоплення і аналізу випромінювань його радіоелектронних засобів з застосуванням спеціальних технічних пристроїв.
- Як правило, термін «радіоелектронна розвідка» використовується для позначення розвідки засобів зв’язку і радіотехнічної розвідки у випадках, коли немає необхідності поділяти ці два види розвідки, або для підкреслення їх єдності.

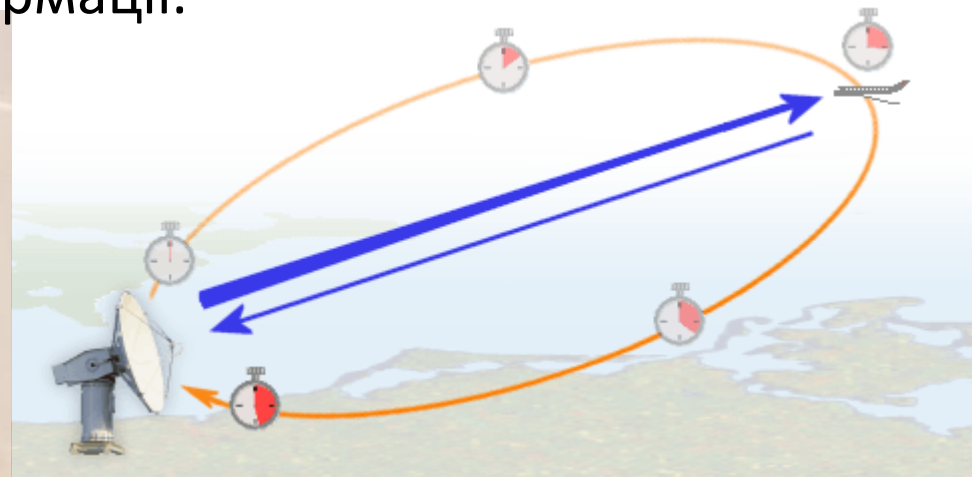


Радіо

- **РА́ДІО (від лат. radio — випромінюю)** — загальна назва методів безпровідного передавання та отримання інформації за допомогою електромагнітних хвиль радіочастотного діапазону. Передавання інформації здійснюють у системах радіозв'язку, радіомовлення, телебачення, радіокерування, активної радіолокації тощо. У системах пасивної радіолокації, пеленгації і подібних здійснюють тільки отримання інформації.

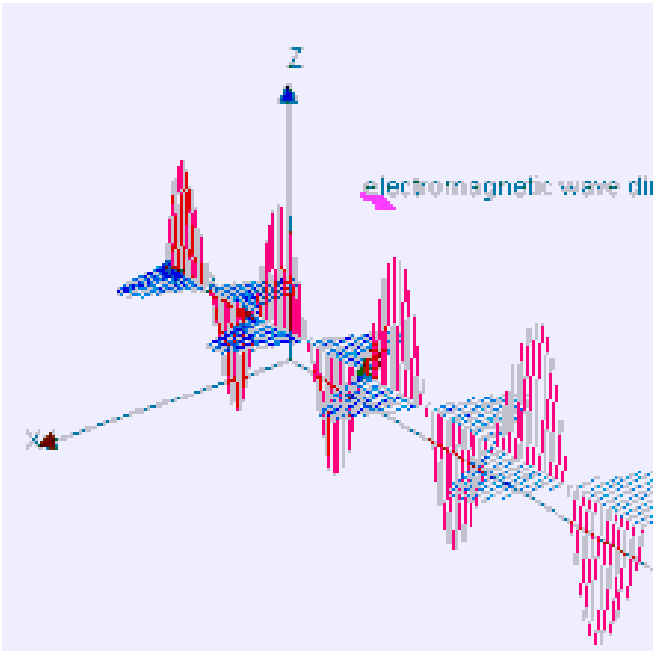






Електромагнітна хвиля$_1$

- **ЕЛЕКТРОМАГНІ́ТНА ХВИ́ЛЯ** — процес розповсюдження електромагнітної взаємодії в просторі у вигляді змінних зв'язаних між собою електричного та магнітного полів.
- Прикладами електромагнітних хвиль є світло, радіохвилі, рентгенівські промені, гамма промені.
- Загальні властивості електромагнітних хвиль вивчаються в розділі фізики, що називається класичною електродинамікою, специфічні — в інших розділах фізики, таких як радіофізика, оптика, спектроскопія, атомна фізика, ядерна фізика тощо.



Періодична зміна електричних та магнітних складових в електромагнітній хвилі

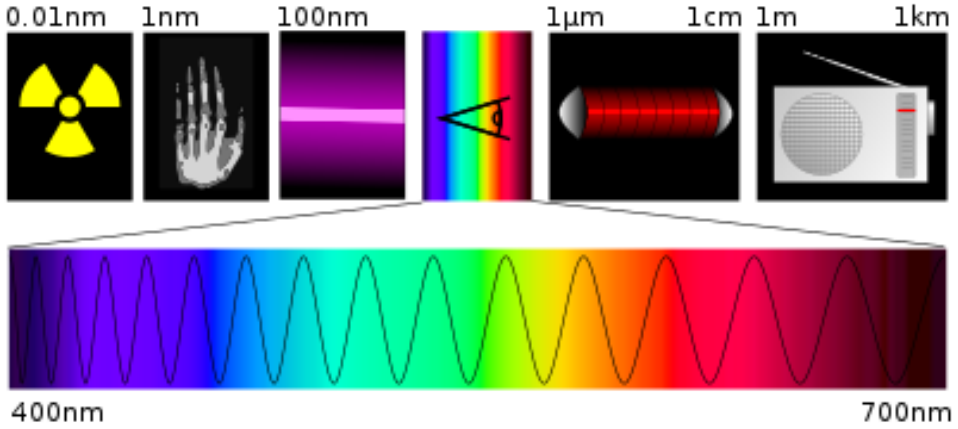
Електромагнітна хвиля$_2$

- У вакуумі ЕЛЕКТРОМАГНІТНА ХВИЛЯ розповсюджується зі швидкістю, яка називається швидкістю світла. Швидкість світла є фундаментальною фізичною константою, яка позначається латинською літерою c. Згідно з основним постулатом теорії відносності швидкість світла є максимально можливою швидкістю передачі інформації чи руху тіла. Ця швидкість становить 299 792 458 м/с.

Електромагнітна хвиля$_3$

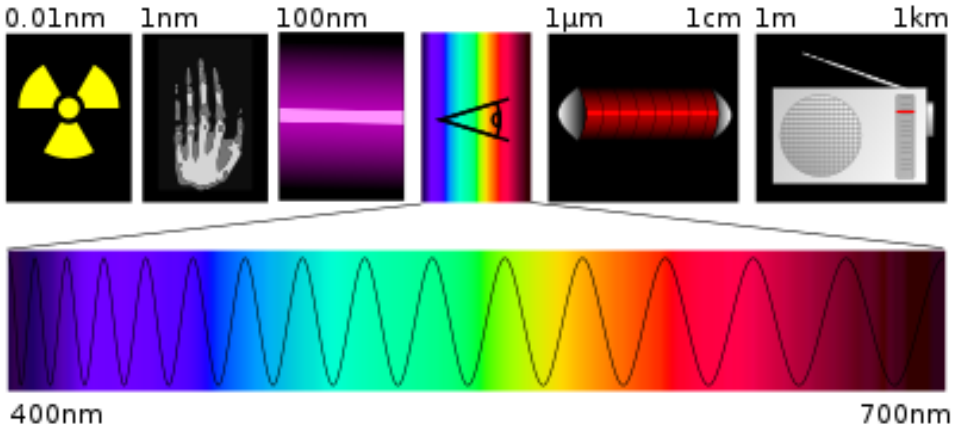
Шкала електромагнітних хвиль

Довжина, м	*Частота, Гц*	*Найменування*
10^{6}–10^{4}	$3\cdot10^{2}$–$3\cdot10^{4}$	Наддовгі
10^{4}–10^{3}	$3\cdot10^{4}$–$3\cdot10^{5}$	Довгі (радіохвилі)
10^{3}–10^{2}	$3\cdot10^{5}$–$3\cdot10^{6}$	Середні (радіохвилі)
10^{2}–10^{1}	$3\cdot10^{6}$–$3\cdot10^{7}$	Короткі (радіохвилі)
10^{1}–10^{-1}	$3\cdot10^{7}$–$3\cdot10^{9}$	Ультракороткі
10^{-1}–10^{-2}	$3\cdot10^{9}$–$3\cdot10^{10}$	Телебачення (НВЧ)
10^{-2}–10^{-3}	$3\cdot10^{10}$–$3\cdot10^{11}$	Радіолокація (НВЧ)
10^{-3}–10^{-6}	$3\cdot10^{11}$–$3\cdot10^{14}$	Інфрачервоне випромінювання
10^{-6}–10^{-7}	$3\cdot10^{14}$–$3\cdot10^{15}$	Видиме світло
10^{-7}–10^{-9}	$3\cdot10^{15}$–$3\cdot10^{17}$	Ультрафіолетове випромінювання
10^{-9}–10^{-12}	$3\cdot10^{17}$–$3\cdot10^{20}$	Рентгенівське випромінювання (м'яке)
10^{-12}–10^{-14}	$3\cdot10^{20}$–$3\cdot10^{22}$	Гамма-випромінювання (жорстке)
$\leq10^{-14}$	$\geq3\cdot10^{22}$	Космічні промені



Електромагнітна хвиля$_4$

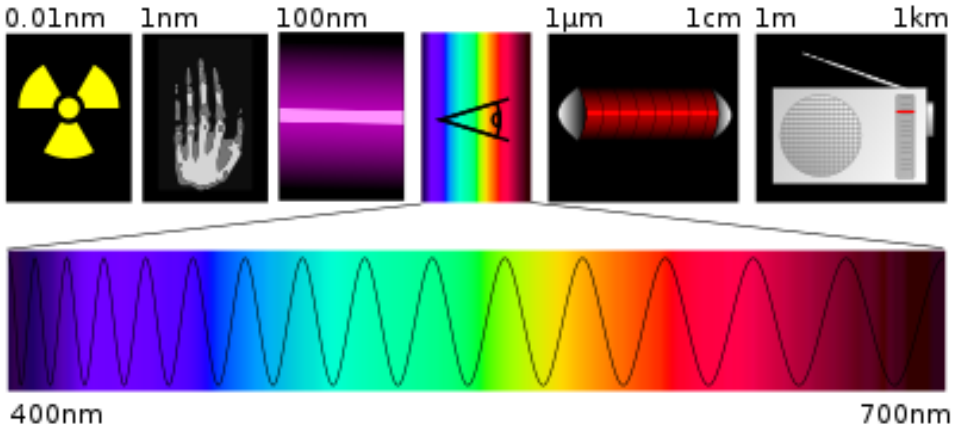
- В залежності від частоти чи довжини хвилі (ці величини пов'язані між собою), електромагнітні хвилі відносять до різних діапазонів. Хвилі в різних діапазонах різним чином взаємодіють з фізичними тілами.
- ДІАПАЗОНИ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ:
  - Електромагнітні хвилі з найменшою частотою (або найбільшою довжиною хвилі) належать до радіодіапазону. Радіодіапазон використовується для передачі сигналів на віддаль за допомогою радіо, телебачення, мобільних телефонів. У радіодіапазоні працює радіолокація. Радіодіапазон розділяється на метровий, дециметровий, сантиметровий, міліметровий, в залежності від довжини електромагнітної хвилі.



Спектральні діапазони з виділеним видимим світлом

Електромагнітна хвиля$_5$

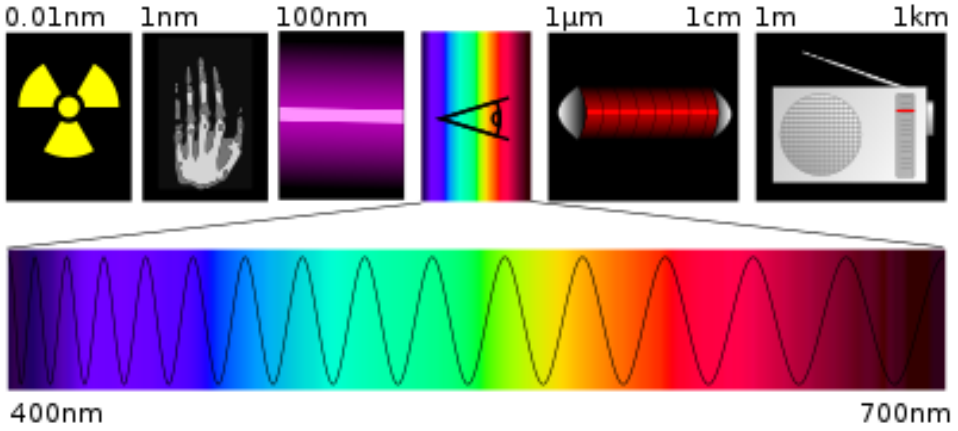
- Електромагнітні хвилі з вищою частотою належать до інфрачервоного діапазону. В інфрачервоному діапазоні лежить теплове випромінювання тіла. Реєстрація цього випромінювання лежить в основі роботи приладів нічного бачення. Інфрачервоні хвилі застосовуються також для вивчення теплових коливань у тілах і допомагають встановити атомну структуру твердих тіл, газів та рідин.



Спектральні діапазони з виділеним видимим світлом

Електромагнітна хвиля$_6$

- Електромагнітне випромінювання з довжиною хвилі від 400 нм до 760 нм належать до діапазону видимого світла. В залежності від частоти й довжини хвилі видиме світло розрізняється за кольорами.
- Хвилі з довжиною меншою за 400 нм називаються ультрафіолетовими. Людське око їх не розрізняє, хоча їхні властивості не дуже відрізняються від властивостей хвиль видимого діапазону.
- Більша частота, а, отже, й енергія квантів такого світла призводить до більш руйнівної дії ультрафіолетових хвиль на біологічні об'єкти. Земна поверхня захищена від шкідливої дії ультрафіолетових хвиль озоновим шаром. Для додаткового захисту природа наділила людей темною шкірою. Проте ультрафіолетові промені потрібні людині для продукування вітаміну D. Саме тому люди в північних широтах, де інтенсивність ультрафіолетових хвиль менша, втратили темне забарвлення шкіри.

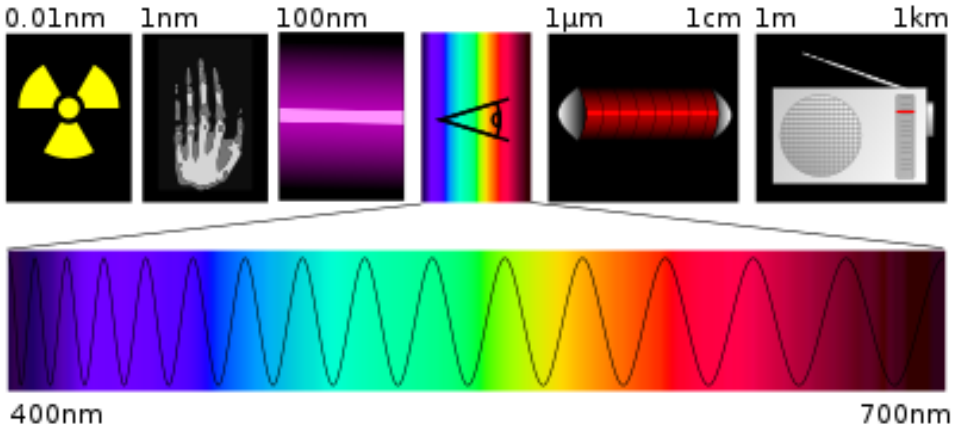


Спектральні діапазони з виділеним видимим світлом

Електромагнітна хвиля[7]

- Електромагнітні хвилі ще вищої частоти належать до рентгенівського діапазону. Вони називаються так тому, що їх відкрив Вільгельм Рентген, вивчаючи випромінювання, яке утворюється при гальмуванні електронів.
- В закордонній літературі такі хвилі заведено називати X-променями, поважаючи бажання Рентгена, щоб промені не називали його іменем. Рентгенівські хвилі слабо взаємодіють із речовиною, сильніше поглинаються середовищем із більшою густиною.
- Цей факт використовується в медицині для рентгенівської флюорографії. Рентгенівські хвилі застосовуються також для елементного аналізу та вивчення структури кристалічних тіл.

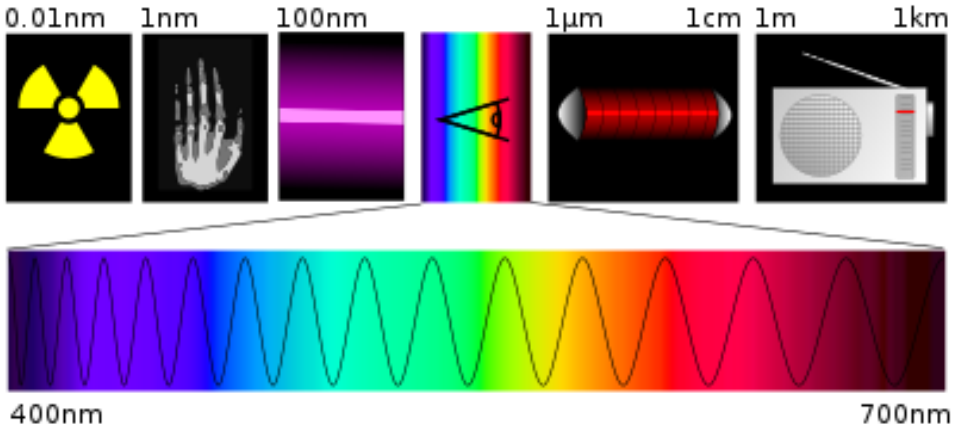




Спектральні діапазони з виділеним видимим світлом

Електромагнітна хвиля$_8$

- Найвищу частоту й найменшу довжину мають γ-промені. Такі промені утворюються внаслідок ядерних реакцій і реакцій між елементарними частинками. γ-промені мають велику руйнівну дію на біологічні об'єкти. Проте вони використовуються у фізиці для вивчення різних характеристик атомного ядра.



Спектральні діапазони з виділеним видимим світлом

Основні вимоги

Особливості РЕР

- Радіоелектронна розвідка в порівнянні з іншими видами розвідувальної діяльності має низку особливостей:
  - діє без безпосереднього контакту з об'єктами розвідки;
  - охоплює великі відстані та простір, межі яких визначаються особливостями поширення радіохвиль різних частот;
  - може вестись безперервно в різний час року і доби та при будь-якій погоді;
  - забезпечує високу достовірність інформації, оскільки вона виходить безпосередньо від противника;
  - здатна отримувати велику кількість інформації різного характеру та змісту;
  - забезпечує отримання інформації в найкоротші терміни, як правило в реальному масштабі часу;
  - малоуразлива і в багатьох випадках недосяжна для противника;
  - діє приховано; противник, зазвичай, не в змозі встановити факт ведення розвідки.



Основні вимоги до РЕР

- Основними вимогами, що пред'являються до радіоелектронної розвідки, є:
  - цілеспрямованість;
  - безперервність;
  - активність;
  - оперативність;
  - прихованість;
  - достовірність;
  - точність.
- **Цілеспрямованість** розвідки полягає в суворій відповідності поставленим завданням, і досягається правильним визначенням завдань, районів та об'єктів розвідки; комплексним веденням розвідки за єдиним планом, розподілом її зусиль по важливих напрямках (районам, об'єктам); зосередженням зусиль розвідки на виконання головних завдань.



Безперервність

- **Безперервність** полягає у веденні її у всіх видах бойових дій, вдень та вночі, в будь-яких умовах місцевості та погоди. Досягається ретельною організацією та підготовкою до бойового чергування, своєчасною постановкою завдань та систематичним контролем за веденням розвідки; передачею розвідувальних відомостей на зміну підрозділів.



Активність

- **Активність** РЕР полягає в наполегливому прагненні добути необхідні розвідувальні відомості про противника. Це досягається вмілим та своєчасним застосуванням засобів радіоперехоплення, нових прийомів та способів ведення розвідки, заснованих на правильному розумінні завдань та обстановки, знанні організації військ противника, його техніки та тактичних прийомів ведення бою.



Оперативність

- **Оперативність** полягає у своєчасному добуванні, обробці, аналізі та доведенні розвідувальних відомостей про об'єкти противника до командування. Досягається передбаченням розвитку обстановки, своєчасним плануванням розвідки та постановкою розвідувальних завдань виконавцям; скороченням витрат часу на збір, обробку та доведення розвідувальної інформації.



Прихованість

- **Прихованість** полягає в дотриманні умов, що виключають можливість виявлення противником засобів РЕР, і досягається ретельним маскуванням, дотриманням дисципліни при веденні розвідки.



Достовірність

- **Достовірність** полягає у виявленні та правильній оцінці істинних, демонстративних та помилкових об'єктів і дій противника. Досягається отриманням розвідувальної інформації від різних джерел, ретельним її аналізом, перевіркою та за необхідності проведенням дорозвідки.



Точність

- **Точність** визначення координат розвідуваних об'єктів полягає у встановленні їх координат з помилками, що не перевищують необхідний рівень та забезпечують ефективне застосування засобів ураження, і досягається застосуванням сучасних засобів пеленгування, створенням пеленгаторної бази.



Класифікація PEP

КТЗ РЕР

- Технічну основу радіоелектронної розвідки складають:
  - пасивні пристрої пошуку, перехоплення та аналізу радіовипромінювань та пеленгування джерел електромагнітних випромінювань;
  - активні радіолокаційні та лазерні засоби спостереження, виявлення та розпізнавання;
  - оптико-електронні прилади та інші прилади реєстрації фізичних полів об'єктів.
- У комплекс технічних засобів радіоелектронної розвідки входять:
  - приймальні антени спрямованої та ненаправленої дії з антено-фідерними пристроями;
  - радіоприймачі, у тому числі панорамні;
  - радіопеленгатори;
  - аналізатори спектру прийнятих сигналів;
  - пристрої для автоматичного відліку змін пеленгу та частоти, стандарти частоти і часу;
  - вихідні пристрої для прийому сигналів телефонних та телеграфних ущільнених каналів радіозв'язку, демодулятори;
  - кінцеві пристрої слухового прийому (телефони, динаміки);
  - засоби реєстрації (індикації) сигналів;
  - прилади розшифровки, обробки та зберігання прийнятої інформації, у тому числі ЕОМ;
  - засоби управління, зв'язку та передачі добутої інформації.

Стратегічна РЕР

- Радіоелектронна розвідка є найважливішою частиною державної та воєнної розвідки різних країн і являє собою основний, а в багатьох випадках, єдиний спосіб добування розвідувальної інформації.
- За різними оцінками засобами РЕР добувається 80-90 % первинної інформації.
- Радіоелектронна розвідка класифікується за кількома ознаками.
- ЗА ЦІЛЬОВИМ ПРИЗНАЧЕННЯМ І ХАРАКТЕРОМ ІНФОРМАЦІЇ, ЩО ДОБУВАЄТЬСЯ:
  - **Стратегічна радіоелектронна розвідка** ведеться в інтересах урядових органів та вищого військового командування з метою добування всебічної інформації про розвідуванні країні через випромінювання радіоелектронних засобів різних відомств і служб.
    - Здійснюється радіотехнічними підрозділами центральних органів розвідки держави (частини і підрозділи спеціальної технічної розвідки, серед іншого на них покладається перехоплення і дешифрування каналів урядового зв'язку, зв'язку дипломатичних установ тощо) і воєнної розвідки (радіотехнічні частини і з'єднання особливого призначення, що добувають інформацію необхідну для підготовки Збройних Сил і ресурсів держави до війни, прийняття рішення про початок військових дій та вмілого ведення стратегічних операцій).



Тактична РЕР

- **Тактична радіоелектронна розвідка** притаманна воєнній розвідці і є одним з видів бойового забезпечення військ інформацією шляхом безперервного спостереження за електромагнітним випромінюванням численних військових пристроїв та систем противника різного призначення.
- Вона в змозі добувати важливі відомості для ведення бойових дій силами з'єднань, частин та підрозділів.



Види РЕР

Радіорозвідка - Communication Intelligence (COMINT)



Радіотехнічна розвідка - Electromagnetic Intelligence (ELINT)



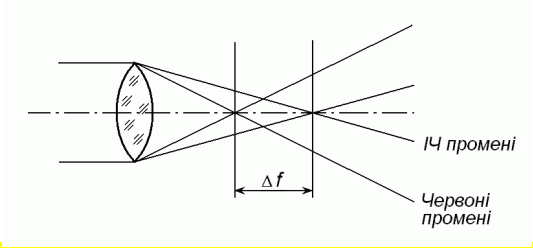
Радіолокаційна розвідка - Radar Intelligence (RADINT)



Телевізійна розвідка – Television Intelligence (TELINT)



Розвідка за допомогою пристроїв інфрачервоної техніки
-Infrared Sets Reconnaissance



Радіорозвідка

Радіорозвідка

- РАДІОРОЗВІДКА – найстаріший вид радіоелектронної розвідки.
  - Вона спрямована проти різних видів радіозв'язку.
  - Основний зміст радіорозвідки - виявлення та перехоплення відкритих, засекречених, кодованих передач зв'язкових радіостанцій, пеленгування їх сигналів, аналіз та обробка інформації, що видобувається з метою розкриття її змісту та визначення місцезнаходження джерел випромінювання.
  - Відомості радіорозвідки про ворожі станції, системи їх побудови та зміст переданих повідомлень дозволяють виявляти плани і задуми противника, склад і розташування його угруповань, встановити місцезнаходження їх штабів і командних пунктів управління, місце розміщення баз і стартових майданчиків ракетної зброї та інших.





Засоби радіорозвідки$_1$

Засоби радіорозвідки дозволяють виявляти противника абсолютно непомітно, просто "слухаючи" радіопростір

Український малогабаритний комплекс радіорозвідки Plastun бачить ворожі об'єкти за 15 км



Plastun-RP3000 дозволяє пеленгувати системи зв'язку, виявляти сигнали, зокрема із псевдовипадковим перелаштуванням робочої частоти (ППРЧ). Це обладнання також визначає місцеположення та відображення координат джерела радіовипромінювання в режимі реального часу з метою створення та актуалізації мапи радіоелектронної обстановки. Крім того, комплекс забезпечує обмін даними по захищеному каналу зв'язку в режимі реального часу для узгодження інформації про розташування та характеристики виявлених джерел радіовипромінювання.

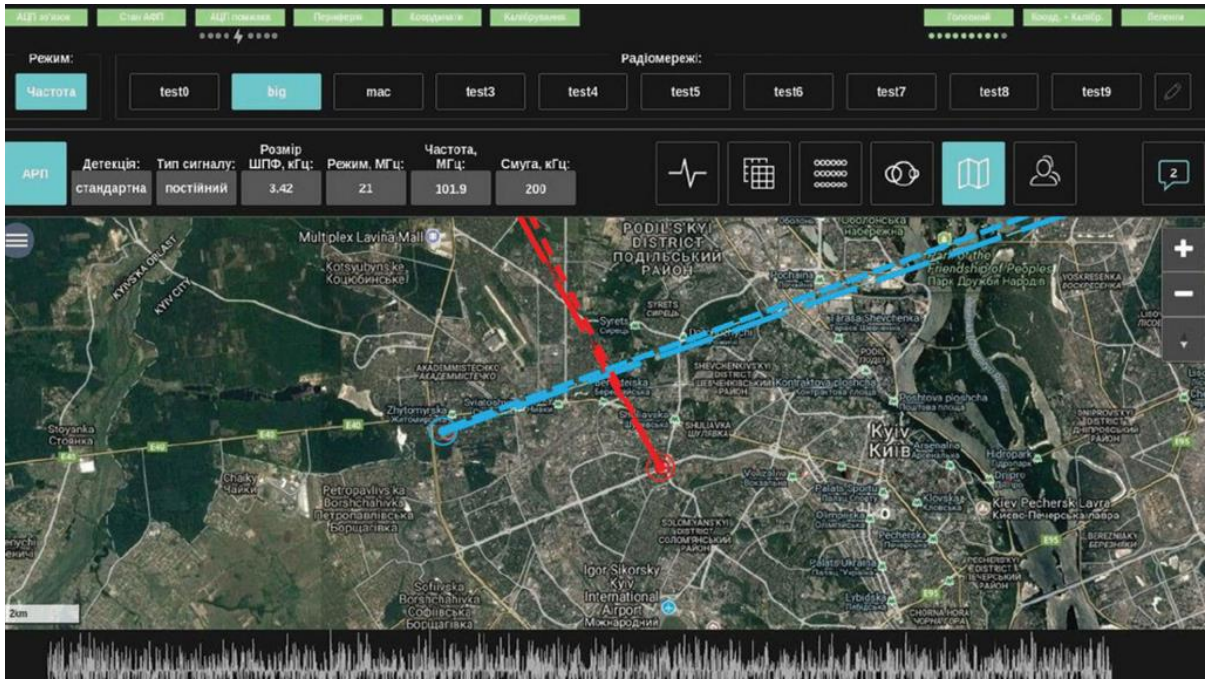
Засоби радіорозвідки$_2$



Власне програмне забезпечення дозволяє візуалізувати дані, які надходять до оператора.

Зокрема, у вкладці динаміки в режимі частоти із відображенням спектрограми відбувається пошук сигналів в робочому діапазоні та аналіз обстановки в радіоефірі в режимі реального часу. Оператор має можливість здійснювати контроль ефіру в усій смузі миттєвого огляду 20 МГц — без додаткових переключень чи налаштувань.

Засоби радіорозвідки$_3$



На мапі із відображенням місцеположення двох напівкомплектів Plastun-RP3000 і їх направленнями пеленгу відображається вся необхідна інформація для роботи оператора. Під час створення, редагування мапи радіоелектронної обстановки оператор має змогу не зупиняти процес виявлення та пеленгації джерел радіовипромінювання чи радіомереж.

Радіотехнічна розвідка

Радіотехнічна розвідка

- **РАДІОТЕХНІЧНА РОЗВІДКА** - вид радіоелектронної розвідки з виявлення та розпізнавання радіолокаційних станцій (РЛС), радіонавігаційних та радіотелекодових систем, використовує методи радіоприймання, пеленгування та аналізу радіосигналу.
- Засоби радіотехнічної розвідки дозволяють:
  - встановити несучу частоту радіопередавачів;
  - визначити координати джерел випромінювання;
  - виміряти параметри імпульсного сигналу (частоту повторення, тривалість та інші параметри);
  - встановити вид модуляції сигналу (амплітудна, частотна, фазова, імпульсна);
  - визначити структуру бічних пелюсток випромінювання радіохвиль;
  - виміряти поляризацію радіохвиль;
  - встановити швидкість сканування антен та метод огляду простору РЛС;
  - проаналізувати та записати інформацію.



Кольчуга$_1$

- «Кольчуга» — українська автоматизована станція радіотехнічної розвідки.
- За способом дії — пасивний радар. Завдяки відсутності активних випромінювань, «Кольчуга» не може бути виявлена засобами радіоелектроної розвідки.
- Станцію виробляв донецький завод ”Топаз”, але з початком російсько-української війни у 2014 році виробництво було перенесене до Науково-виробничого комплексу «Іскра (Запоріжжя). (Відео)
- https://www.youtube.com/watch?v=2vAhJ9l7PeE



Кольчуга$_2$

Пасивна система моніторингу радіоелектронного середовища та супроводу повітряних цілей

«KOLCHUGA RDF-360»

TARGET



до 700 км. ◄ радіо сигнал



ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ

Пасивне виявлення та ідентифікація цілей
Моніторинг повітряного, наземного и надводного середовища
Супровод повітряних та надводних цілей в пасивному режимі
Мобільний та стаціонарний варіант системи
Склад: 4станції(1 центральна, 3 бічні)

ДАЛЬНЯ РАДІОТЕХНІЧНА РОЗВІДКА

Дальність виявлення цілей:	до 700км
Діапазон частот:	0,13-12ГГц
Миттєва смуга огляду:	0,5ГГц
Сектор огляду:	360°
Цілі:	наземні, надводні, повітряні

ОСНОВНІ ТТХ СИСТЕМИ

Діапазон частот:	0,13-18ГГц
Кількість цілей що супроводжуються в реальному масштабі часу:	200
Місткість бази даних:	100 000 экземплярів
Супровід цілей:	по 3 координатах
Обробка сигналів:	РЛС, відповідочів системы «свій-чужий» (режими 1,2,3 (АС),4,S,навигаційної системи ТАКАН

ПАСИВНИЙ СУПРОВОД ПОВІТРЯНИХ ЦІЛЕЙ

Дальність виявлення цілей:	до 450км(пряма видимість)
Діапазон частот:	8-18ГГц
Діапазон частот 1.025-1.15ГГц	сигнали системи «свій-чужий»
Сектор огляду:	360°
Миттєва смуга огляду:	3,5ГГц
Типи цілей:	повітряні (також малопомітні цілі «Stealth»)

Радіолокаційна розвідка

Фізичні основи радіолокації

- Принцип функціонування первинного радіолокатора є простим для розуміння. Однак, теорія може виявитися дещо складнішою. Знання теорії важливе для розуміння принципів роботи вузлів і підсистем радіолокатора. Під час створення і в ході функціонування радіолокатора використовуються знання з багатьох дисциплін: від будівництва та важкого машинобудування до електротехніки та високочастотної техніки.
- Також використовуються методи обробки сигналів та інформації. Деякі фізичні закони при цьому становлять особливий інтерес.
- Вимірювання радіолокатором дальності до цілі стає можливим завдяки деяким особливостям розповсюдження радіохвиль.

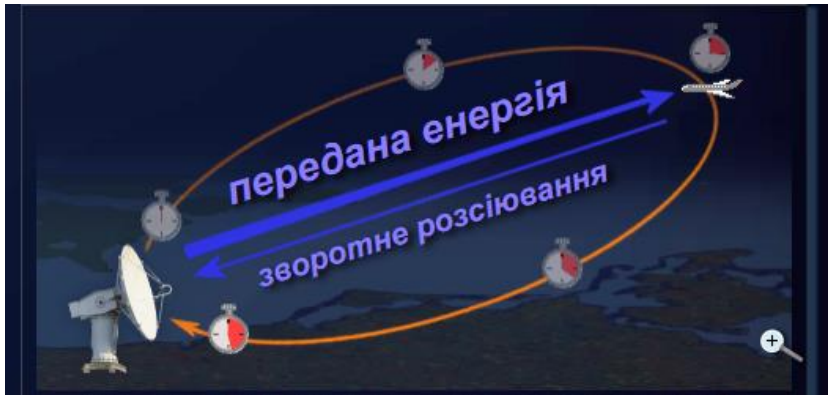


Рисунок 1: Принцип дії радіолокатора: вимірювання часу пробігу мікрохвильового імпульсу

Відбиття електромагнітних хвиль

- Електромагнітні хвилі відбиваються, коли на шляху їх розповсюдження трапляється провідна поверхня. Якщо відбита хвиля може бути прийнята в точці, звідки відбувається випромінення, це свідчить про наявність перешкоди у напрямку випромінювання.
- Електромагнітні хвилі розповсюджуються з постійною швидкістю, яка приблизно дорівнює швидкості світла,
  - 300 000 км/с, або
  - 186 000 миль/с, або
  - 162 000 морських миль/с.
- Постійність швидкості дає змогу визначити дальність до відбиваючого об’єкту (літак, корабель, автомобіль) шляхом вимірювання часу затримки відбитого сигналу відносно моменту випромінення.

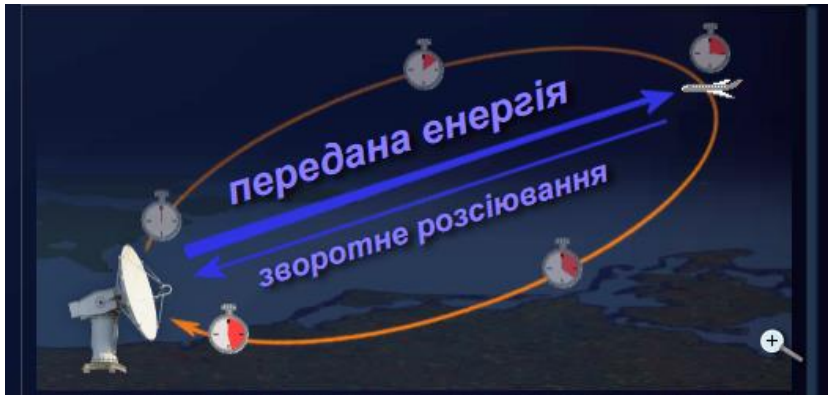


Рисунок 1: Принцип дії радіолокатора: вимірювання часу пробігу мікрохвильового імпульсу

Випромінювання електромагнітних хвиль

- Електромагнітна хвиля розповсюджується у вільному просторі по прямолінійній траєкторії, і ця властивість, у більшості випадків, змінюється несуттєво під впливом атмосферних та погодних умов.
- За допомогою спеціальних радіолокаційних антен, електромагнітна хвиля може бути випромінена у потрібному напрямку.
- Завдяки цьому стає можливим вимірювання напрямку (азимут та /або кут місця) на відбиваючий об’єкт.

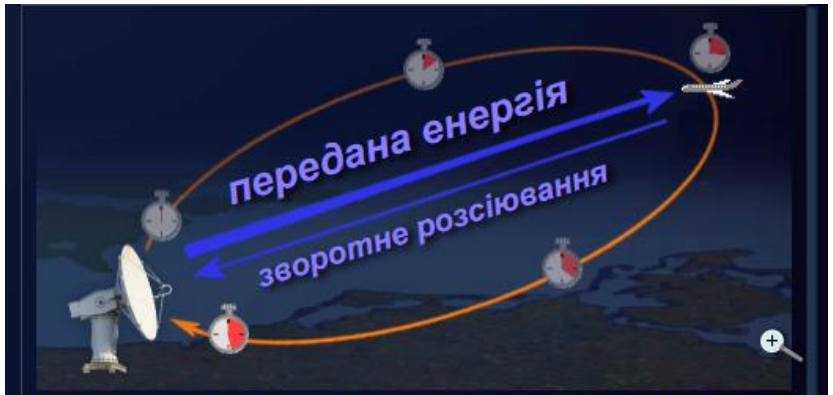
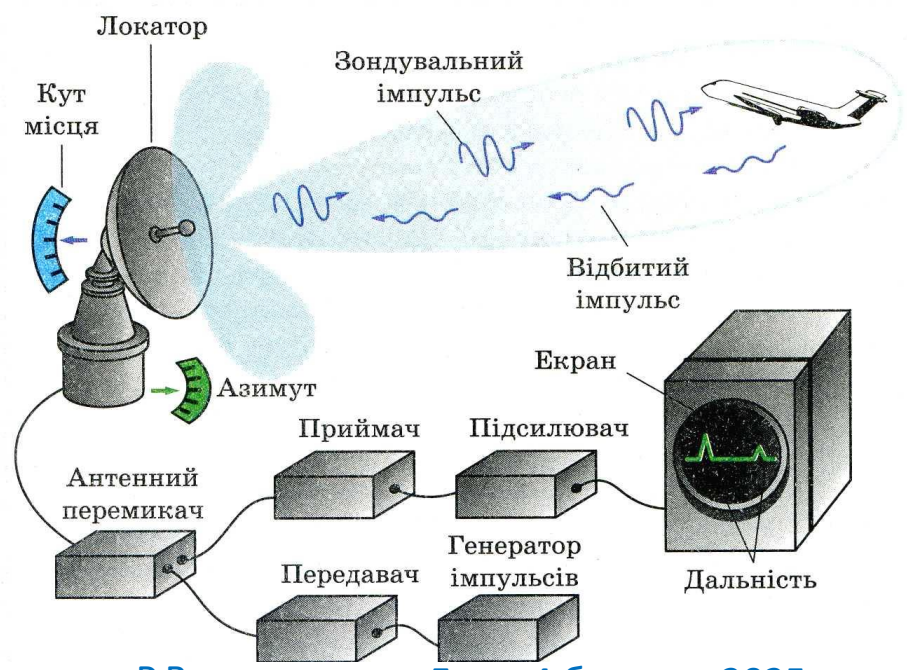


Рисунок 1: Принцип дії радіолокатора: вимірювання часу пробігу мікрохвильового імпульсу

Координати в просторі

- Якщо ціль точкова, то її положення у просторі повністю визначається трьома координатами. У сферичній системі координат це похила дальність Д, азимут ά і кут місця β. Початок координат О збігається з точкою стояння (розташування) РЛС.



Похила дальність цілі

- Оскільки розповсюдження радіохвиль відбувається із постійною відомою швидкістю (дорівнює швидкості світла, C0), то дальність до цілі може бути визначена по часу затримки прийнятого сигналу відносно зондувального. Виміряна дальність від радіолокатора до цілі зветься похилою дальністю цілі.
- **Похила дальність цілі** — це відстань по прямій (по лінії візування) від антени радіолокатора до опромінюваного об’єкту.

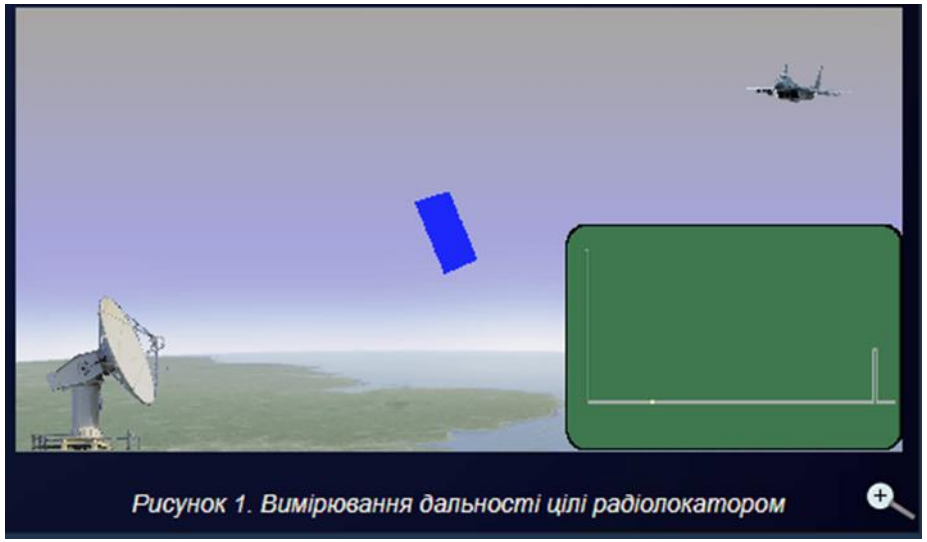


Рисунок 1. Вимірювання дальності цілі радіолокатором

Горизонтальна дальність

- В той же час, горизонтальна дальність (проекція похилої дальності на земну поверхню), для обчислення потребує інформації про висоту або кут місця цілі. Оскільки під час виявлення цілі електромагнітна хвиля проходить шлях до цілі та назад, то час проходження сигналу поділяється на два і, таким чином розраховується час руху імпульсу в один бік. Виходячи із зазначеного, формула для визначення похилої дальності цілі має вигляд:

$$R = \frac{c_0 \cdot t}{2}$$

c_0 — швидкість світла = $3 \cdot 10^8$ м/с;

t — виміряне значення часу проходження імпульсу [с];

R — відстань від антени до цілі [м].

Відстань зазвичай вимірюється в кілометрах або морських милях (*1 м. миля = 1,852 км*).

Азимут

- **Азимутом** цілі називають кут між напрямком на північ та горизонтальною проекцією напрямку «радіолокатор — ціль». Цей кут відраховується в горизонтальній площині від напрямку на північ за годинниковою стрілкою (Рисунок 1). Також азимут може відраховуватися від центральної вісі літака або корабля, з якого ведеться вимірювання (так званий відносний азимут).
- Азимут цілі вимірюється за напрямком променю (головного променю) антени в момент прийому відбитого від цілі сигналу. Направленість антени (характеризується значенням коефіцієнту направленої дії) — це спроможність антени фокусувати енергію в заданому напрямку. Антена з високим коефіцієнтом направленної дії зветься направленою. За положенням направленої антени в момент приймання відбитого імпульсу, можливо визначити азимут та кут місця цілі. Точність вимірювання кутових координат залежить від направлених властивостей антени.

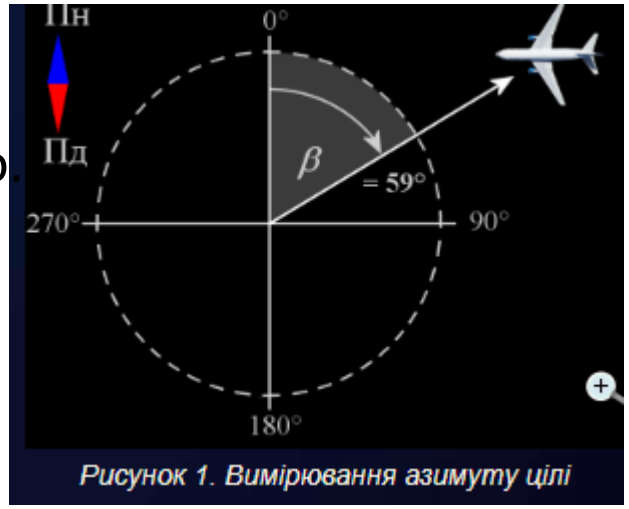


Рисунок 1. Вимірювання азимуту цілі

Вимірювання азимуту цілі

- Антени більшості радіолокаторів проектуються таким чином, щоби сформувати промінь в заданому напрямку. Таким чином, змінюючи кутове положення антени, можливо переміщувати промінь у просторі.
- Як можна бачити на Рисунку 2, форма променю така, що амплітуда сигналу відлуння змінюється під час проходження променю по цілі. В реальних радіолокаторах антена рухається постійно, а точка максимуму відбитого сигналу відслідковується спеціальним обладнанням або візуально оператором — це і буде момент, коли промінь «вказує» прямо на ціль. Радіолокатори слідкування (супроводження) або керування озброєнням зазвичай вирішують завдання пошуку максимальної амплітуди сигналу відлуння, після чого виконується утримання променю в цьому напрямку вручну або за допомогою автоматичних систем слідкування.
- Для вимірювання азимуту цілі, необхідно мати інформацію про напрямок на північ в точці встановлення антени радіолокатора. Для отримання такої інформації виконується операція, яка зветься орієнтуванням радіолокатора. У випадку із застарілими радіолокаторами для цього використовували компас, або орієнтири на місцевості, координати яких відомі. В сучасних системах для цього використовують інформацію від супутникових навігаційних систем (наприклад, GPS).

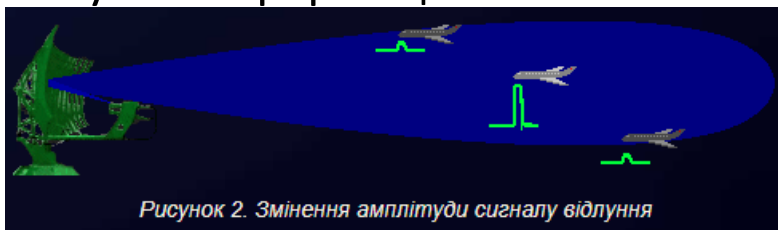


Рисунок 2. Змінення амплітуди сигналу відлуння

Кут місця цілі

- Для визначення просторового положення цілі в радіолокації використовуються різноманітні системи координат, основною з яких є місцева (локальна) полярна система координат (Рисунок 1). Центр цієї системи координат знаходиться в точці стояння радіолокатора та суміщений з електричним (геометричним) центром його антени. Вісь відліку знаходиться в горизонтальній площині та орієнтована вздовж напрямку на північ (на рисунку позначена «Пн»). Координатами в такій системі є азимут β, дальність D та кут місця ε цілі.
- **Кут місця цілі** — це кут між горизонтальною площиною та напрямком на ціль. Очевидно, що кут місця цілі відраховується у вертикальній площині. Він має додатні значення для цілей, що знаходяться вище площини горизонту, та від'ємні — для цілей нижче площини горизонту. Від'ємні значення кута місця можуть виникати, наприклад, коли радіолокатор розміщений на височині (пагорб, штучна гірка, узбережжя і тому подібне).

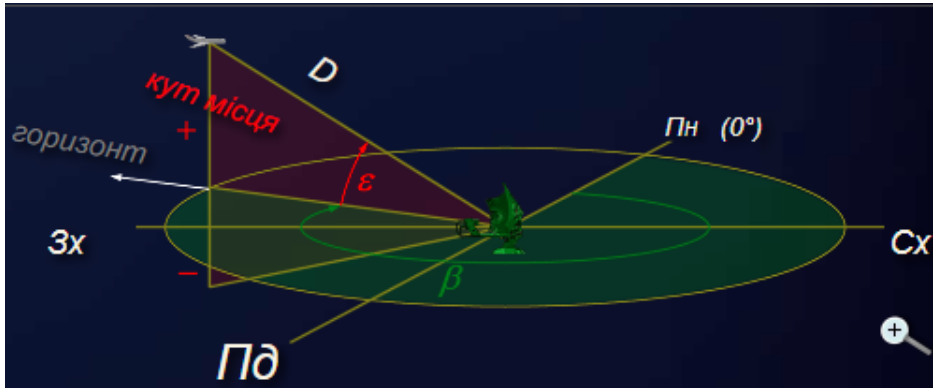


Рисунок 1. Координати, що вимірюються радіолокаційною станцією, (наприклад, β= 280° ; ε= 30°; D=…)

Вимірювання кута місця цілі

- Для вимірювання кута місця застосовують механічне або електронне сканування у вертикальній площині. Антена повинна мати в цій площині вузьку (іноді кажуть «голкоподібну») діаграму направленості. Значення кута місця променю антени в момент виявлення відбитого сигналу вважається виміряним значенням кута місця цілі.
- Для вимірювання кута місця цілі були розроблені спеціалізовані радіолокатори – радіолокаційні висотоміри. Результати їхньої роботи доповнюють дані, отримані за допомогою двокоординатних радіолокаторів (дальномірів), у сукупності забезпечуючи вимірювання повних координат цілі. Такий варіант побудови радіолокаційних комплексів (наприклад, 3D-комплекс від компанії Altimus-tech) застосовується і нині, поступово поступаючись місцем трикоординатним радіолокаторам, які використовують антенні решітки з електронним скануванням голкоподібного променю.



Роздільна здатність$_1$

- **Роздільна здатність** — це один з основних параметрів радіолокатора, що характеризує його здатність розрізняти (розділяти) цілі, що знаходяться поряд одна з одною, за дальністю або азимутом (кутовою координатою). Це можливість роздільного виявлення та вимірювання координат одночасно спостережуваних цілей.
- Роздільна здатність з дальності — це кількісна міра здатності радіолокаційної системи розділяти дві або більше цілей, що знаходяться на одному азимуті, але на різних дальностях. Величина роздільної здатності з дальності залежить від тривалості випромінюваного зондувального імпульсу, типів та розмірів цілей, а також ефективності приймача та індикаторного пристрою. Основним визначальним чинником є тривалість імпульсу. Якісно спроектований радіолокатор має розділяти цілі, віддалені одна від одної на відстань, яка відповідає половині тривалості зондувального імпульсу. Отже, теоретичну величину роздільної здатності з дальності можливо оцінити за допомогою співвідношення:

$$S_r \geq \frac{c_0 \cdot \tau}{2}$$

S_r — роздільна здатність з дальності;
c_0 — швидкість світла;
τ — тривалість зондувальних імпульсів.

Роздільна здатність$_2$

- На Рисунках 2 та 3 пояснюється поняття «роздільна здатність» на прикладі зондувального імпульсу тривалістю в одну мікросекунду (1 мкс). Нескладно показати, що просторовий розмір такого імпульсу дорівнюватиме 300 м. 300 м.
- Якщо відстань між двома літаками замала, то радіолокатор замість двох «бачить» лише одну ціль, як показано на Рисунку 2.
- В іншому прикладі, коли відстань між літаками достатньо велика (Рисунок 3), бачимо розділення обох цілей:

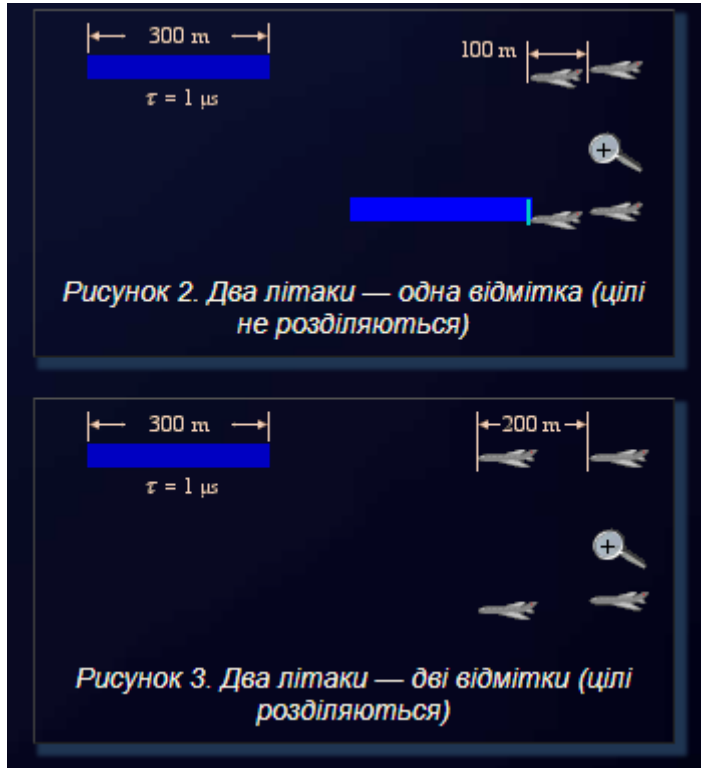


Рисунок 2. Два літаки — одна відмітка (цілі не розділяються)

Рисунок 3. Два літаки — дві відмітки (цілі розділяються)

Мінімальна дальність дії радіолокатора

- При використанні роздільних антен для випромінювання зондувального сигналу та приймання відбитого від цілі сигналу, мінімальна дальність дії імпульсного радіолокатора практично дорівнює нулю.
- Однак, у разі використання для випромінювання і приймання однієї й тієї самої антени (моностатичний локатор) передатчик та приймач радіолокатора можуть працювати тільки почергово. Це пояснюється тим, що радіолокаційний приймач, який є високочутливим пристроєм, під час впливу на нього потужного зондувального сигналу може вийти з ладу. Таким чином, на час випромінювання зондувального сигналу приймач закривається, а дальність, пропорційну цьому часу, називають мінімальною дальністю дії радіолокатора. Ця дальність визначає розміри так званої «сліпої» або «мертвої» зони.
- Крім цього, після закінчення випромінювання потрібен деякий час для відновлення антенного перемикача (до якого також відносять і прилади захисту приймача), що також впливає на розмір «сліпої» зони. Ціль, що знаходиться в цій зоні, не буде виявлена радіолокатором. Тому мінімальна дальність дії є однією з важливих характеристик радіолокатора.
- Виходячи з наведених вище міркувань, легко записати формулу для визначення мінімальної дальності дії радіолокатора:

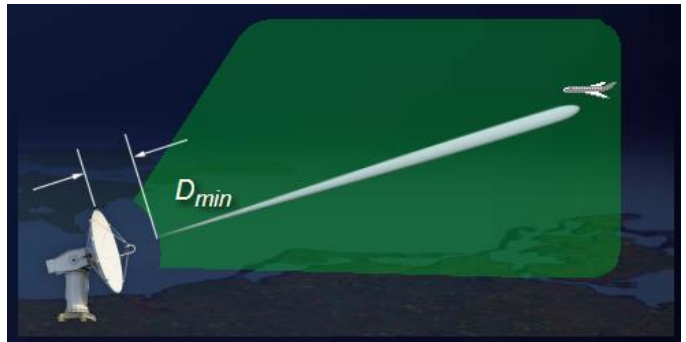


Рисунок 1. До пояснення мінімальної дальності дії радіолокатора

$$D_{\min} = \frac{c_0 \cdot (\tau + t_{\text{відн.}})}{2}$$

c_0 — швидкість розповсюдження електромагнітної хвилі;

τ — тривалість зондувального сигналу;

$t_{відн.}$ — час відновлення антенного перемикача (наприклад, для газорозрядного приладу це тривалість процесу деіонізації).

Приклад. РЛС «МАЛАХІТ»

- Завадозахищена РЛС метрового діапазону з цифровою обробкою та автоматичною передачею інформації РЛС «МАЛАХІТ» призначена для:
  - автоматичного виявлення, визначення поточних координат (азимуту, дальності, курсу, швидкості та висоти при поєднанні з ПРВ) та параметрів траєкторії руху;
  - автоматичної передачі даних за супроводжуваними цілями на КП, а також споживачам радіолокаційної інформації при використанні у складі підрозділів радіолокаційної розвідки РТВ та ЗРВ в умовах інтенсивних відображень від підстилаючої поверхні та наземних предметів, дії організованих активних, пасивних та комбінованих перешкод;
  - виявлення та супроводу цілей з малими ЕПР, що використовують технології Стелс;
  - виявлення та супроводження цілей на морській акваторії.



Донецький національний технічний університет



Тема 5. Розвідка та добування інформації. Лекція 16. Кібернетична розвідка.

Предмет: МтаЗТЗІ
Розділ: Кібербезпека
Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.



Лекційні питання

- Загальні положення
- Засоби і способи кіберрозвідки
- Канали НСД

Загальні положення

Кіберрозвідка$_1$

КІБЕРРОЗВІДКА - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.



Кіберрозвідка$_2$

У більш широкому сенсі під кіберрозвідкою будемо сприймати таке визначення:

Кібернетична розвідка – процес добування усіма наявними технічними засобами розвідки (космічної, повітряної, радіоелектронної, мережевої, програмно-комп'ютерної, розвідки систем управління тощо) й засобами розвідки з відкритих джерел (*OSINT*- розвідка) інформації наявної в кіберпросторі про протиборчу сторону та подальша її обробка, що здійснюються за єдиним задумом і планом з метою викриття процесів управління, які протікають в кібернетичних системах під час їх функціонування та формування вихідних даних для здійснення заходів кібернетичного захисту та кібернетичного впливу на технічні, соціальні та соціотехнічні кібернетичні системи.



Основні функції кібернетичної розвідки

- Основні функції наступні:
  - постійний пошук і добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, що становлять інтерес з використанням усіх наявних технічних засобів розвідки й засобів розвідки з відкритих джерел інформації з кіберпростору;
  - обробка, систематизація, класифікація, узагальнення та аналіз добутої розвідувальної інформації;
  - підготовка розвідувальної інформації на підставі проведеного аналізу для прийняття обґрунтованих управлінських рішень;
  - формуванні вихідних даних для здійснення заходів кібернетичного захисту власних кібернетичних систем та здійснення кібернетичного впливу на кібернетичні системи протиборчої сторони;
  - прогнозування можливих проявів кібернетичних загроз та їх наслідків.

Особливості кіберрозвідки

- Основні особливості кіберрозвідки наступні:
  - порівняно з іншими видами розвідки роль кібернетичної розвідки постійно зростає. При правильному підході до організації кібернетичної розвідки, а також раціональному застосуванні сил та засобів її забезпечення у мирний час можливо добувати від 35% до 95% інформації про об’єкти або суб’єкти, що становлять інтерес;
  - добуваюча та обробляюча складові процесу кібернетичної розвідки мають взаємозалежний тісний зв’язок;
  - підвищується роль знань на заключному етапі процесу кібернетичної розвідки, який на відміну від інших видів розвідки не завершується підготовкою розвідувальних даних для визначених органів. Заключний етап кібернетичної розвідки полягає у приведенні розвідувальних даних у вищий ступінь готовності до їх застосування у процесі прийняття управлінських рішень – у вигляді набутих знань;
  - під час кібернетичної розвідки роль, місце та функції людини як на етапі добування, так і на етапі обробки змінюються за рахунок зменшення об’єму працевитрат;
  - сутність кібернетичної розвідки в основному зводиться на здійснення діяльності, спрямованої на досягнення або утримання переваги в кіберпросторі над протиборчою стороною;
  - складність територіальної та державної ідентифікації належності суб’єкта або об’єкта кібернетичної розвідки, що суттєво ускладнює процес добування розвідувальної інформації та забезпечення її достовірності.

Вимоги та фази кіберрозвідки

СИСТЕМНІ ВИМОГИ ДО КІБЕРНЕТИЧНОЇ РОЗВІДКИ

- підсистеми кібернетичної розвідки повинні мати розвинену інфраструктуру, що дозволить здійснювати постійний моніторинг процесів управління різної природи в системах управління різного цільового призначення та ієрархічної складності з метою досягнення синергетичного ефекту;
- підсистеми кібернетичної розвідки мають бути максимально автоматизованими, а звітні результати повинні подаватися у стандартизованій формі, яка доступна усім підсистемам;
- система кібернетичної розвідки повинна мати централізований банк даних для збереження розвідувальної інформації та добутих знань.

Кібернетична розвідка включає *три основні фази*

- організацію кіберрозвідки;
- ведення кіберрозвідки;
- інформаційну роботу.

Фази кіберрозвідки

Організація кіберрозвідки передбачає визначення цілей і завдань розвідки, виділення необхідних сил і засобів, планування її заходів, постановку завдань виконавцям, організацію їх підготовки та інші питання

Ведення кіберрозвідки має безпосередній зв'язок з добуванням розвідувальної інформації.

Інформаційна робота являє собою збір, обробку розвідувальної інформації, її узагальнення та доведення до зацікавлених осіб.

Форми кіберрозвідки



Рис. 3.1. Форми кіберрозвідки та зв’язок між ними

Методи отримання інформації

Методи отримання інформації

Легальна кіберрозвідка

– це вид діяльності, що ґрунтується на легальних способах добування розвідувальної інформації про процеси управління в кібернетичних системах й здійснюється в кіберпросторі уповноваженими органами з питань кібербезпеки.

Нелегальна кіберрозвідка

Нелегальна кіберрозвідка здійснюється в кіберпросторі й ґрунтується на нелегальних способах збору розвідувальної інформації та, в основному, стосується добування розвідувальної інформації з обмеженим доступом, що охороняється державою або її власником.

Легальні методи

- електронно-обчислювальні машини (ЕОМ), у тому числі (ПЕОМ);
- участь у науково-технічних конференціях;
- аналіз суспільно-політичних, наукових та технічних видань;
- відвідування виставок;
- дослідження повідомлень електронних ЗМІ (телебачення, радіо, World Wide Web) та ін.













Нелегальні методи

- викрадення зразків продукції та (або) технологічного обладнання;
- викрадення документів;
- копіювання документів;
- впровадження агентів на об'єкт противника;
- впровадження агентів в структури противника;
- знімання інформації по технічних каналах;
- проникнення в автоматизовані системи (АС) противника, що використовуються для обробки інформації, та ін.









Характеристики розвідки

- Основні характеристики розвідки наступні:
  - розвідка має номінальний характер щодо підвищення достовірності видобутої інформації;
  - розвідка діє ешелоновано, що дозволяє проводити детальну розвідку;
  - розвідка має координований характер;
  - розвідка має глобальний характер;
  - розвідка спрямована насамперед на особливо важливі об'єкти (наприклад, військові, політичні).

Види інформації

Розподіл інформації щодо важливості та за ступенем захищеності :

- таємна;
- конфендецийна;
- відкрита;





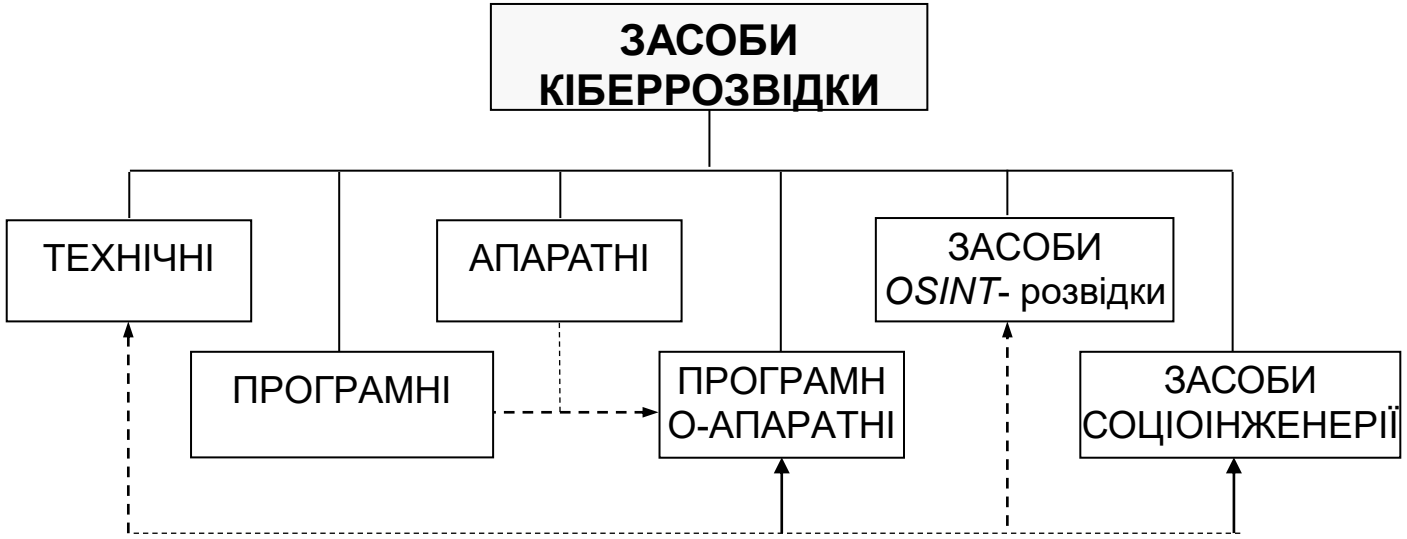


Засоби і способи кіберрозвідки

Класифікація засобів кіберрозвідки$_1$

Засоби кібернетичної розвідки поділяються на такі *основні типи:*

- технічні засоби;
- програмні засоби;
- апаратні засоби;
- програмно-апаратні засоби;
- засоби кіберрозвідки з відкритих джерел (OSINT- засоби);
- засоби соціальної інженерії.



Основні типи засобів кіберрозвідки та зв’язків між ними

Засоби кіберрозвідки$_1$

Технічні засоби кіберрозвідки – це сукупність розвідувальної апаратури (апаратів, машин та виготовлених з їх використанням спеціалізованого обладнання або технічних засобів, інструментів, речовин тощо), що призначені для несанкціонованого одержання розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони шляхом контролю кіберпростору й окремих його складових.

Програмні засоби кіберрозвідки – це сукупність спеціалізованих програмних модулів, які створені з метою добування розвідувальної інформації з кіберпростору про процеси управління в кібернетичних системах протиборчої сторони.

Апаратні засоби кіберрозвідки – це сукупність спеціалізованих апаратних засобів, що забезпечують добування розвідувальної інформації шляхом дослідження апаратури, обладнання, модулів їх аналізу та випробування тощо, задіяних в управлінні кібернетичними системами протиборчої сторони з метою виявлення їх технічних характеристик та потенційних можливостей.

Програмно-апаратні засоби являють собою сукупність програмних та апаратних спеціалізованих засобів, призначення та функції яких випливають з основного призначення та функцій їх складових.

Засоби кіберрозвідки$_2$

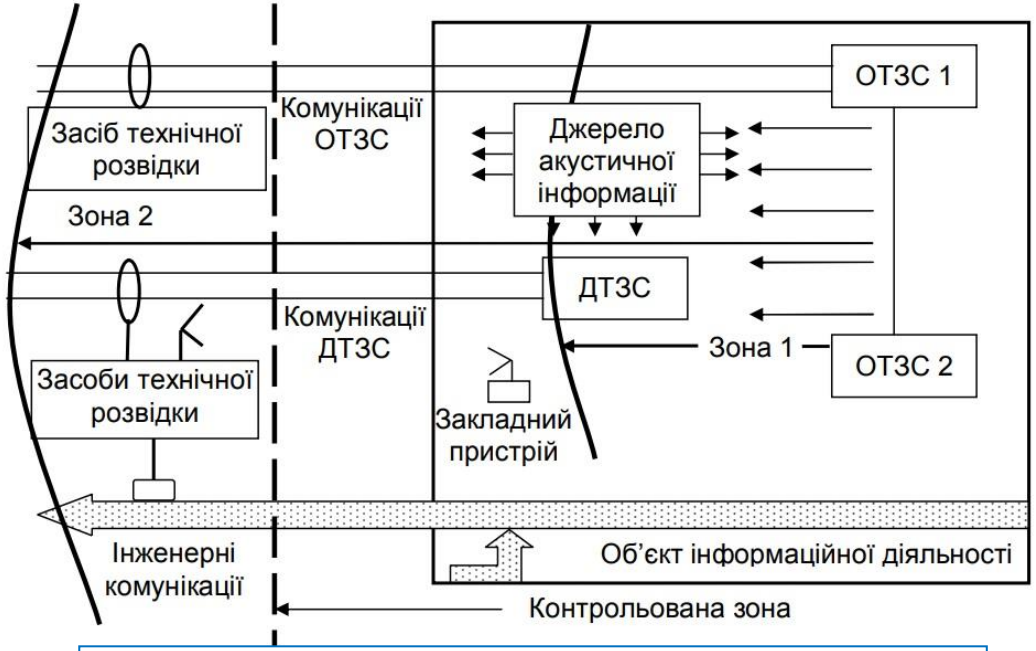
Засоби OSINT- розвідки – це сукупність, технічних, програмних, апаратних, програмно-апаратних та інших засобів, що використовуються підрозділами кібернетичної розвідки для добування розвідувальної інформації з відкритих та відносно відкритих джерел кіберпростору про процеси управління, що протікають у кібернетичних системах протиборчої сторони.

Засоби соціальної інженерії – засоби добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, орієнтовані на її отримання від суб'єкта кібернетично розвідки. Саме соціальна інженерія вважається фахівцями одним із найбільш перспективних способів ведення кібернетичної розвідки. Окрім інформації про процеси управління в кібернетичних системах за допомогою методів соціального інжинірингу вдається одержувати несанкціонований доступ до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншу конфіденційні дані про об'єкт або суб'єкт розвідки – людину (або групу людей), використовуючи її (їх) слабкість або некомпетентність, непрофесіоналізм або недбалість та керуючи її (їх) діями. Соціальний інжиніринг може практикуватись як самостійно, без застосування описаних вище засобів, так і з їх використанням.

Канали НСД

Технічний канал витоку інформації

Під **ТЕХНІЧНИМ КАНАЛОМ ВИТОКУ ІНФОРМАЦІЇ (ТКВІ)** розуміють сукупність об’єкту розвідки, технічного засобу розвідки (ТЗР), за допомогою якого отримується інформація про цей об’єкт, та фізичне середовище, де розповсюджується інформаційний сигнал та завада. За суттю під ТКВІ розуміють **спосіб отримання за допомогою ТЗР розвідувальної інформації** про об’єкт розвідки. При цьому форма подання інформації може бути довільна.



Схематична можливість витоку інформації

Канали несанкціонованого отримання інформації

— канали та шляхи витоку інформації з інформаційної системи; паразитний (небажаний) ланцюжок носіїв інформації, один або кілька з яких є (можуть бути) правопорушником або його спеціальною апаратурою.

КАНАЛИ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Непрямі канали

не вимагають безпосереднього доступу до технічних засобів інформаційної системи

Прямі канали

вимагають доступу до апаратного забезпечення і даних інформаційної системи

Приклади непрямих каналів

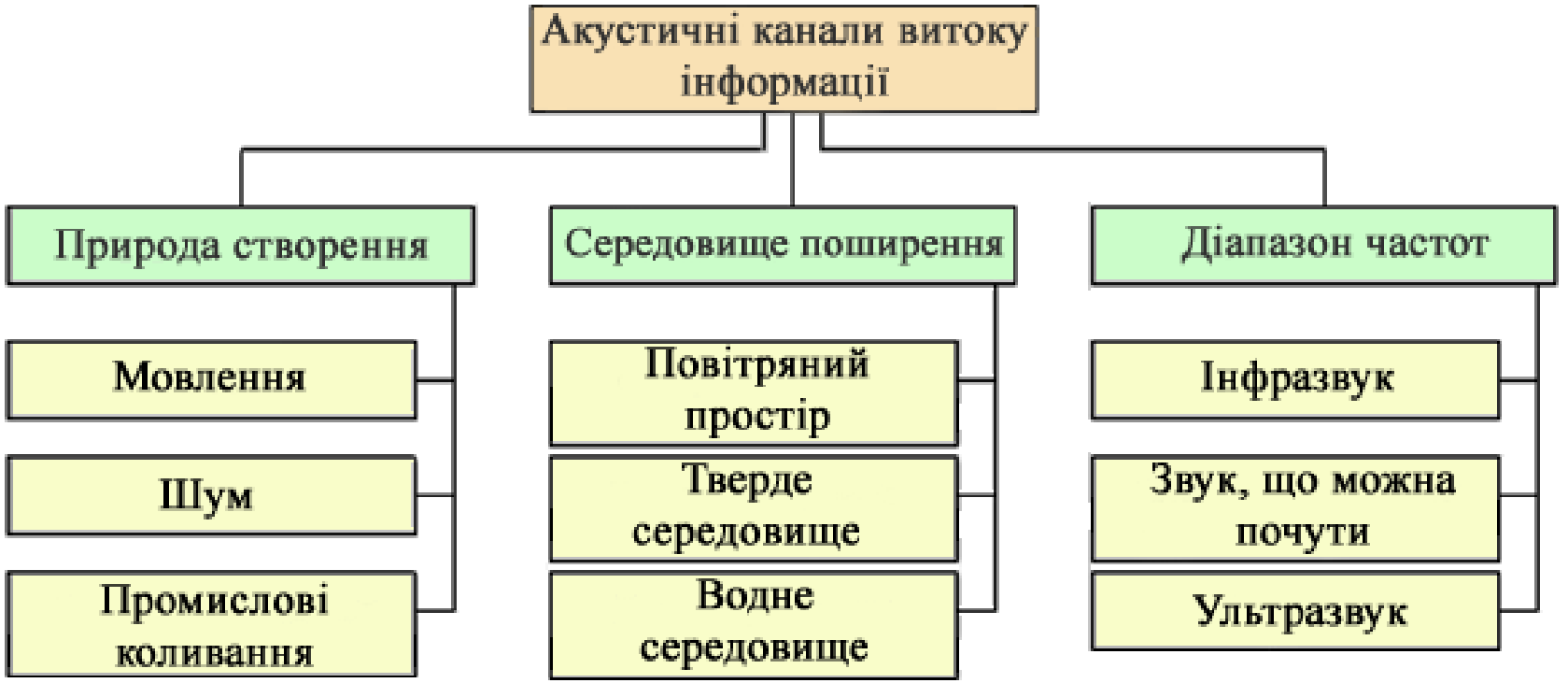
Крадіжка або втрата носіїв інформації, дослідження не знищеного сміття;
Дистанційне фотографування, прослуховування;
Перехоплення електромагнітних випромінювань.

Приклади прямих каналів

Інсайдери (людський фактор).
Витік інформації внаслідок недотримання комерційної таємниці;
Пряме копіювання.

Класифікація ТКВІ

АКУСТИЧНІ — запис звуку, підслуховування і прослуховування



В акустичних каналах витоку інформації середовищем поширення мовних сигналів є повітря

Акустичні ТКВІ$_1$

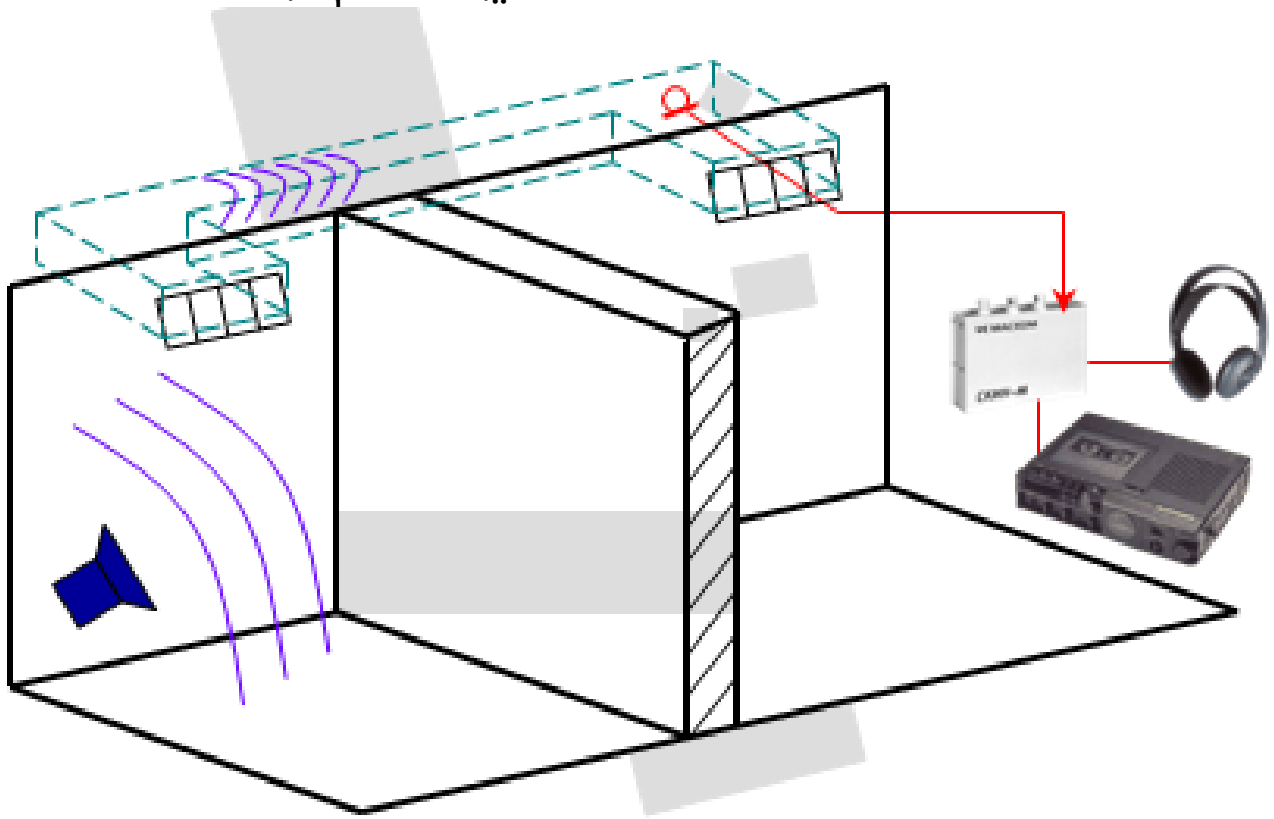
АКУСТИЧНІ канали витоку інформації

Шляхи витоку акустичної інформації за межі огороджувальних конструкцій :

- за рахунок «мембранного ефекту». Так званий «мембранний ефект» обумовлений коливанням тонких (відносно довжини) і, як правило відносно легких, елементів огороджувальних конструкцій (віконного скла, фанерних, гіпсокартонних, пластикових перегородок тощо), здатних прогинатися під дією звуку;
- через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань;
- за рахунок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні. У даному випадку частина енергії акустичних коливань (частина відбивається), падаючи на поверхню огороджувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення речовини. Подолавши огороджувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

Акустичні ТКВІ$_2$

АКУСТИЧНІ канали витоку

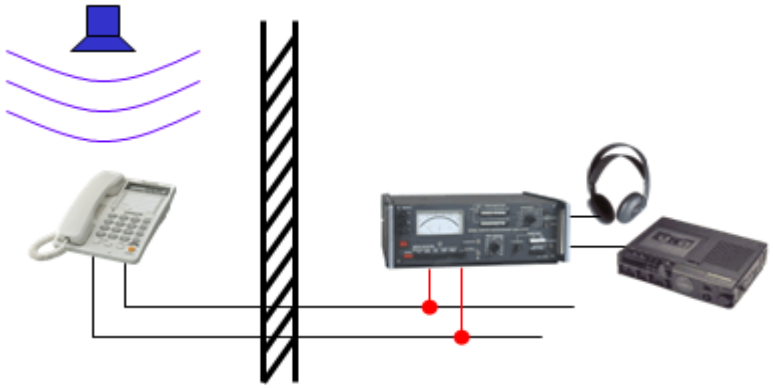


Приклад витоку акустичної інформації

Акустоелектричні ТКВІ

АКУСТОЕЛЕКТРИЧНІ — отримання інформації через звукові хвилі з подальшою передачею її через мережі електроживлення

Шляхи утворення акустоелектричних каналів витоку інформації
- Акустоелектричні перетворення у мережі електроживлення;
- Акустоелектричні перетворення у мережі часофікації;
- Акустоелектричні перетворення у системі пожежної сигналізації;
- Акустоелектричні перетворення у мережі радіомовлення;
- Акустоелектричні перетворення у телефонній мережі;
- Акустоелектричні перетворення у системі охоронної сигналізації





Віброакустичні ТКВІ

ВІБРОАКУСТИЧНІ — сигнали, що виникають за допомогою перетворення інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються

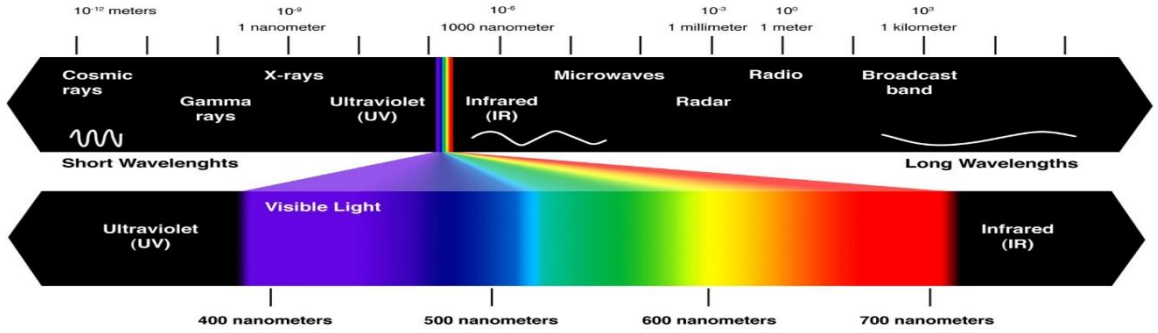
Звукова хвиля, поширюючись по повітрю, впливає своєї кінетичної енергією наелементи будівельних конструкцій і предмети, що знаходяться в контрольованому приміщенні. Далі звукова хвиля поширюється в матеріалі, з якого виконані конструкції і предмети з загасанням, зумовленим властивістю матеріалу. Зрозуміло, що чим щільніше матеріал, тим далі і з меншими втратами пройде звуковий сигнал. Так як стіни приміщення мають кінцеву товщину, звукова хвиля, з певною амплітудою дійде до зовнішньої сторони стіниЦе означає, що із зовнішнього боку стін контрольованого приміщення ми можемо зареєструвати мікроколивання, створювані джерелом звуку усередині приміщення.

Оптичні ТКВІ

ОПТИЧНІ — візуальні методи, фотографування, відеозйомка, спостереження

В оптичному каналі отримання інформації можливо шляхом:
· візуального спостереження;
· фото-відеозйомки;
· використання видимого та інфрачервоного діапазонів для передачі інформації від приховано встановлених мікрофонів та інших датчиків;

Як середовища поширення в оптичному каналі витоку інформації виступають:
· безповітряний простір;
· атмосфера;
· оптичні світловоди



Visible spectrum

Електромагнітні ТКВІ

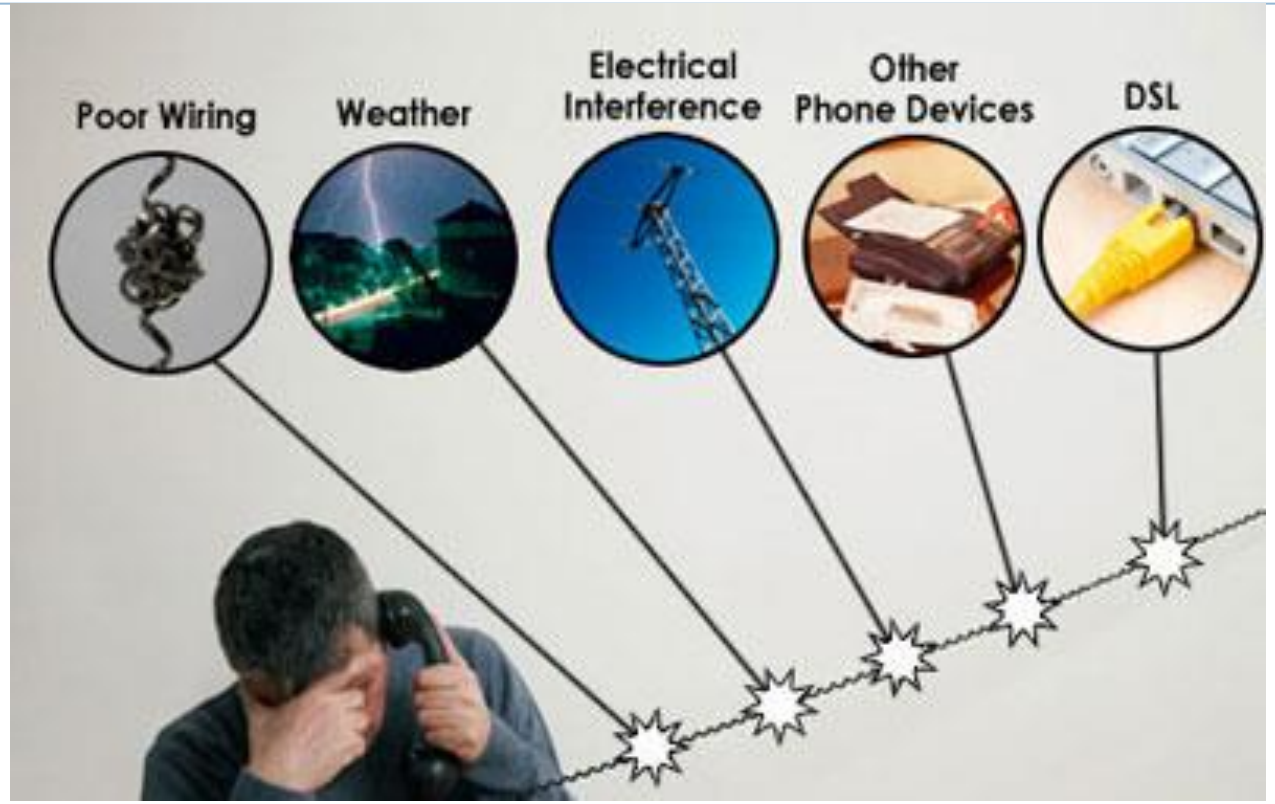
ЕЛЕКТРОМАГНІТНІ — копіювання полів шляхом зняття індуктивних наводок

Модульовані інформаційним сигналом високочастотні електромагнітні випромінювання передавачів засобів зв'язку можуть перехоплюватися портативними засобами радіорозвідки і при необхідності передаватися в центр обробки для їх розкодування. Такий канал перехоплення інформації широко використовується для прослуховування телефонних розмов.



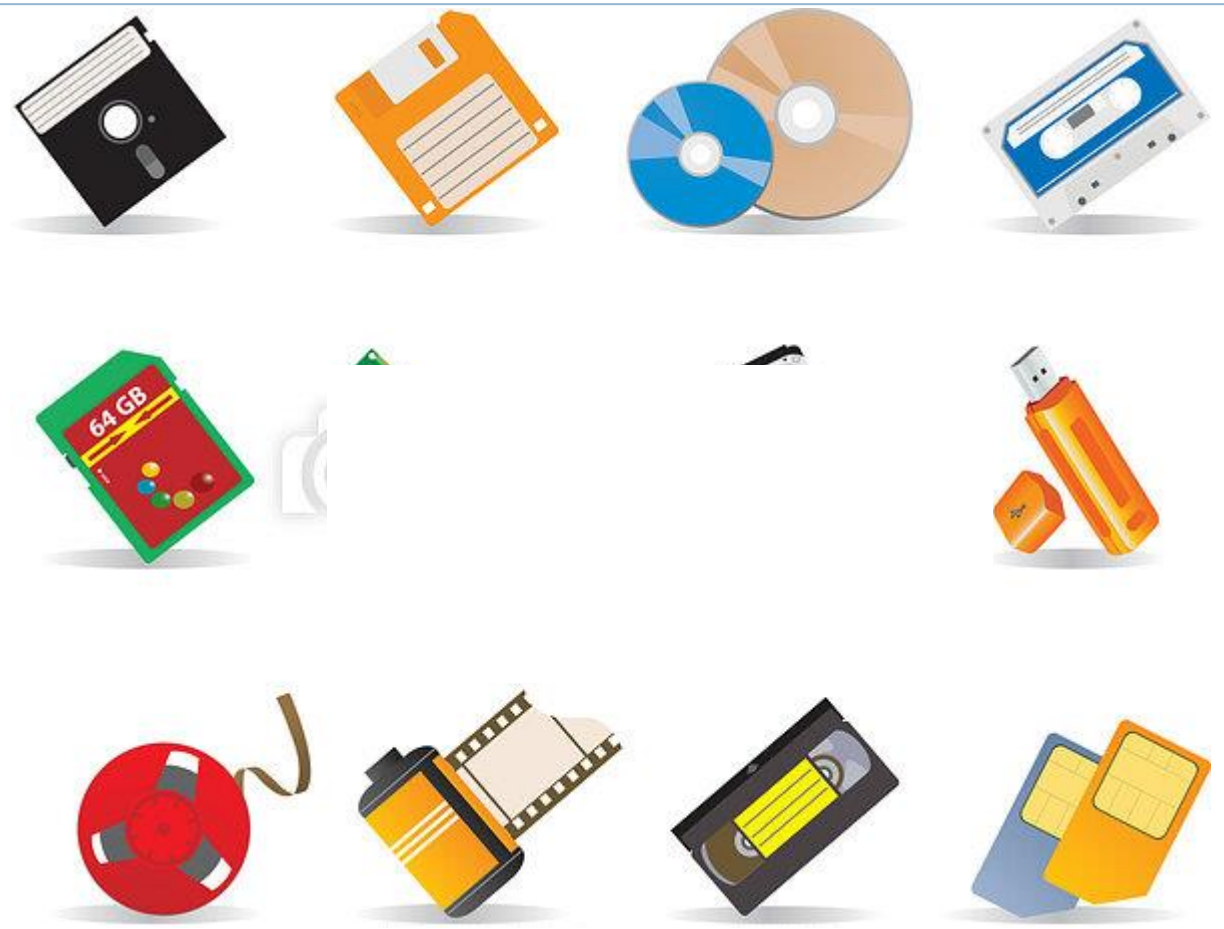
Радіовипромінювання

РАДІОВИПРОМІНЮВАННЯ або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом



Матеріальні ТКВІ

МАТЕРІАЛЬНІ — інформація на папері або інших фізичних носіях інформації



Класифікація каналів розповсюдження інформації

Канали розповсюдження інформації – це засіб обміну інформацією між суб'єктами ділових та особистих відносин

Неформальні
• особисте спілкування (зустрічі, переговори, листування, телефонні переговори, обмін факсимільними повідомленнями та повідомленнями електронної пошти тощо); • виставки, семінари, конференції та інші масові заходи; • засоби масової інформації (друк, газети, радіо, телебачення, електронні форуми, групи новин)

Формальні
• ділові зустрічі, наради, переговори та ін.; • обмін офіційними діловими та науковими документами; • засоби передачі офіційної інформації (пошта, телеграф, телефон, електронна пошта, World Wide Web та ін.)

Класифікація каналів розповсюдження інформації

Каналами поширення інформації також можуть бути:

- поширення в країні та за кордоном офіційних видань про зареєстровані винаходи;
- обмін науково-технічною літературою (книги, журнали), здійснюваний бібліотеками та іншими організаціями з міжбібліотечного обміну, як у країні, і із зарубіжними організаціями;
- вивезення за кордон книг та журналів науково-технічного та економічного характеру громадянами, які виїжджають у службові відрядження
- публікації фахівцями та науковцями наукових та технічних матеріалів у закордонних виданнях, у тому числі у World Wide Web;
- особисте листування фахівців і вчених з тематики, що їх цікавить, із закордонними колегами, особливо електронною поштою;
- розсилання науково-технічних бюлетенів до електронних груп новин, обговорення тем, що цікавлять, у дискусійних групах, форумах Internet тощо.

Систематизований перелік способів НСД

Протиправне навмисне оволодіння секретною та (або) конфіденційною інформацією особами, які не мають права доступу до відомостей, що охороняються

Знищення (псування, руйнування)	Підключення до каналів та ліній зв'язку та передачі даних	Негласне ознайомлення із відомостями та документами	Підслуховування розмов різними шляхами та способами
Ініціативна співпраця	Схиляння до співпраці	Підробка (модифікація)	Візуальне спостереження
Випитування	Перехоплення	Копіювання	Викрадення
Фотографування			Збір та аналітична обробка

Список рекомендованих джерел для самопідготовки

Список рекомендованих джерел для самопідготовки$_1$

1. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.
2. Дорогий Я.Ю., Нікітенко А.О. Методи та засоби технічного захисту інформації. Практикум : ел. навч. посіб. для студентів всіх форм навчання галузі знань 12 Інформаційні технології / авт. Я.Ю. Дорогий, А.О. Нікітенко. – Луцьк : ДонНТУ, 2024. – 240 с.
3. ДСТУ 3396.0-96.
4. ДСТУ 3396.1-96.
5. ДСТУ 3396.2-97.
6. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Список рекомендованих джерел для самопідготовки$_2$

7. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»
8. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи»
9. 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».
10. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення».
11. ТПКО-95 Тимчасове положення з категоріювання ОІД.
12. ДБН А.2.2-2-96 ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.
13. Положення про державний контроль за станом технічного захисту інформації від 16.05.2007 №87.