

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA – технологій факультету № 6

**МЕТОДИЧНІ МАТЕРІАЛИ
ДО ПРАКТИЧНИХ ЗАНЯТЬ**

з навчальної дисципліни " Методи та засоби захисту інформації "
вибіркових компонент
освітньої програми першого рівня вищої освіти

125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО

Вченою радою факультету № 6
Протокол від 25.08.2023 № 7

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій
факультету № 6 (*протокол від 15.08.2023 № 8*)

Розробник: доцент кафедри кібербезпеки та DATA – технологій факультету № 6
Харківського національного університету внутрішніх справ, к.т.н. доцент Тулупов В.В.

Рецензенти:

професор кафедри протидії кіберзлочинності Харківського національного університету
внутрішніх справ, к.т.н. доцент Носов В.В.

завідувач кафедри проектування та експлуатації електронних апаратів Харківського
національного університету радіоелектроніки, к.т.н. доцент Хорошайло Ю.Є.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Література	Вид контролю
	Всього	з них:					
		лекції	Практичні заняття	Лабораторні	Самостійна робота		
Семестр № 5							
ТЕМА № 1. Цілі, задачі та організація технічної розвідки	8	4			4	1-5, 27-31	екзамен
ТЕМА № 2. Концепція інженерно-технічного захисту інформації	10	2	4		4	1-5, 27-45	
ТЕМА № 3. Характеристика захищеної інформації	14	2	2		10	1- 8, 12, 13, 27-45	
ТЕМА № 4. Електромагнітні випромінювання та наведення	16	2	2	4	8	1-8, 12, 13, 27-52	
ТЕМА № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ)	14	2	2	2	8	1-8, 12, 13, 27-45	
ТЕМА № 6. Технічні канали витоку акустичної інформації	12	2	2	2	6	1-8, 12, 13, 27-52	
ТЕМА № 7. Технічні канали витоку інформації, що обробляється ТЗПІ	20	4	4	4	8	1-8,12, 13, 27-51	
ТЕМА № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами	14	2	2	2	8	1-8, 9,12, 13, 27-45	
ТЕМА № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами	12	2	2		8	1-8, 12, 13, 27-51	
ТЕМА № 10. Методи та засоби технічного захисту акустичної інформації	16	2	2	4	8	1-5, 7, 8, 12, 13,	
ТЕМА № 11. Методи пошуку електронних пристроїв перехоплення інформації. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації	18	4	2	4	8	1-5, 7, 8, 12, 13, 16,18,27-56	
ТЕМА № 12. Засоби пошуку електронних пристроїв перехоплення інформації. Класифікація засобів радіовиявлення. Індикаторні засоби радіомоніторингу Інтерсептори.	24	4	4	8	8	1-8, 12-15, 16,18,27-56	
Всього за семестр :	180	30	28	32	90		

Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Література	Вид контролю
	Всього	з них:					
		лекції	Практичні заняття	Лабораторні	Самостійна робота		
Семестр № 5							
ТЕМА № 1. Цілі, задачі та організація технічної розвідки	12				12	1-5, 27-31	екзамен
ТЕМА № 2. Концепція інженерно-технічного захисту інформації	12				12	1-5, 27-45	
ТЕМА № 3. Характеристика захищеної інформації	12				12	1- 8, 12, 13, 27-45	
ТЕМА № 4. Електромагнітні випромінювання та наведення	12				12	1-8, 12, 13, 27-52	
ТЕМА № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ)	20	2	2	2	14	1-8, 12, 13, 27-45	
ТЕМА № 6. Технічні канали витоку акустичної інформації	12				12	1-8, 12, 13, 27-52	
ТЕМА № 7. Технічні канали витоку інформації, що обробляється ТЗПІ	12				12	1-8,12, 13, 27-51	
ТЕМА № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами	22	4	2	2	14	1-8, 9,12, 13, 27-45	
ТЕМА № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами	12				12	1-8, 12, 13, 27-51	
ТЕМА № 10. Методи та засоби технічного захисту акустичної інформації	20	2	2	2	14	1-5,7, 8, 12, 13,	
ТЕМА № 11. Методи пошуку електронних пристроїв перехоплення інформації. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації.	22	4	2	2	14	1-5, 7, 8, 12, 13, 16,18,27-56	
ТЕМА № 12. Засоби пошуку електронних пристроїв перехоплення інформації. Класифікація засобів радіовиявлення. Індикаторні засоби радіомоніторингу. Інтерсептори.	12				12	1-8, 12-15, 16,18,27-56	
Всього за семестр :	180	12	8	8	152		

2. Методичні вказівки до практичних занять:

Тема № 2-3. Практичне заняття № 1 на тему: Складові структури захисту інформації

Навчальна мета заняття: проаналізувати основні складові структури захисту інформації.

Кількість годин: 4 год.

Навчальні питання:

1. Системний підхід до інженерно-технічного захисту інформації
 - 1.1. Цілі, завдання та ресурси системи захисту інформації
 - 1.2. Основні положення системного підходу до інженерно-технічного захисту інформації
2. Державна політика і система ТЗІ в Україні.
3. Структура системи захисту інформації.

Література:

Основна

1. Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
2. Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
3. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.
5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
6. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

7. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
8. Шепета О. В. Адміністративно-правові засади технічного захисту інформації : монографія / Акад. наук вищ. освіти України, Global organization of allied leadership, Acad. of open society security. К. : О. С. Ліпкан, 2012. 295 с.
9. Носов В. В., Манжай А. В. Організація та забезпечення безпеки інформації : навчальний посібник. Харків : ХНУВС, 2007. 216 с.

Нормативно-правові акти

10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.
11. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL:

- <https://zakon.rada.gov.ua/laws/show/3855-12>.
12. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2939-17>.
 13. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>.
 14. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 № 222-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/222-19>.
 15. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05.04.2007 № 877-V // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/877-16>.
 16. Про акредитацію органів з оцінки відповідності : Закон України від 17.05.2001 № 2407-III // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2407-14>.
 17. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1229/99>.
 18. Про затвердження Концепції технічного захисту інформації в Україні : постанова Кабінету Міністрів України від 08.10.1997 № 1126 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF>.
 19. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF>.
 20. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>.
 21. Про деякі питання захисту інформації, охорона якої забезпечується державою : постанова Кабінету Міністрів України від 13.03.2002 № 281 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.
 22. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.
 23. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. ДБН А.2.2-96. Видання інформаційне. К. : Держкоммістобудування України, 1996. 18 с.
 24. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 23.12.2020 № 383 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/download/nakaz-vid-23122020-383-pro-zatverdjennya-zvodu-2020-87459.html>

Інформаційні ресурси в Інтернеті

25. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws>.
26. Фонд нормативних документів у сфері технічного та криптографічного захисту

інформації // Державна служба спеціального зв'язку та захисту інформації України :
офіційний вебсайт. URL:
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=89734.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Організація захисту інформації забезпечується правовими, організаційними і інженерно-технічними заходами. Організаційні інженерно-технічні заходи складають зміст технічного захисту інформації. Правові заходи інформації є базисом, на який спирається організаційні та інженерно-технічні заходи по захисту інформації.

II. Основна частина

1. Системний підхід до інженерно-технічного захисту інформації

Слабоформалізовані завдання, до яких ставиться більшість завдань інженерно-технічного захисту, характеризуються наступними основними особливостями:

- наявністю великої кількості факторів, що впливають на ефективність рішення завдання;
- відсутністю кількісних достовірних вихідних даних про цих факторів;
- відсутністю формальних (математичних) методів одержання оптимальних результатів рішення слабоформалізованих завдань по сукупності вихідних даних.

Ці особливості виключають можливість формального одержання оптимального результату рішення завдання. Але навіть формальний апарат при недостовірних вихідних даних не гарантує одержання точного результату.

Слабоформалізовані завдання вирішуються в основному евристичними методами. Однак ці методи не забезпечують одержання оптимального результату, а визначають область раціональних рішень, тобто тих, які з певними допусками відповідають постановці завдання. Як правило, завдання має кілька раціональних рішень, які в просторі результатів утворюють область, усередині якої розташоване оптимальне рішення.

Евристичні методи реалізують на підсвідомому рівні¹ знання й досвід фахівців. Евристичні методи рішення слабоформалізованих завдань часто забезпечують більш точні результати, чим формальні на основі грубих математичних моделей або при недостовірних і недостатніх вихідних даних.

Але можливості евристичних методів мають обмеження, обумовлені числом факторів, що враховують при рішенні завдання, впливу.

Якщо число факторів впливу велике, що має місце при рішенні завдань інженерно-технічного захисту інформації, то точність евристичних методів значна. У загальному випадку завдання інженерно-технічного захисту інформації характеризуються більшою кількістю й різноманіттям факторів, що впливають на результат рішення, причому цей вплив часто не вдається однозначно виявити й строго описати. До них, у першу чергу, ставляться завдання, результати рішення яких залежать від людей, тобто організація ефективного захисту інформації залежить винятково фахівців із захисту інформації.

1.1 Основні положення системного підходу до інженерно-технічного захисту інформації

¹ Підсвідомий рівень на сучасному етапі розвитку біологічної й психологічної наук поки являє собою «чорний ящик», алгоритм роботи якого невідомий. Фахівці із психоаналізу намагаються по окремих проявах несвідомого на свідомому рівні виявити психічні хвороби пацієнтів, причини яких криються в неусвідомлюваних психічних травмах у попередні роки.

Рішення будь-яких завдань виробляється на основі моделей досліджуваних об'єктів і процесів. Розв'язуване завдання або проблема являє собою різницю між реальним об'єктом або процесом і тим, що треба одержати. Найбільш універсальною моделлю об'єкта або процесу є подання його у вигляді системи.

Системний підхід – це дослідження об'єкта або процесу за допомогою моделі, називаною системою.

Цей підхід передбачає найвищий рівень опису об'єкта дослідження – системний. Найнижчим рівнем є рівень опису параметрів об'єкта – параметричний. Між ними існують розташовуються структурний і функціональний рівні.

Сутність системного підходу полягає в наступному:

- сукупність сил і засобів, що забезпечують рішення завдання, представляється в виді моделі, називаною системою;

- система описується сукупністю параметрів;

- будь-яка система розглядається як підсистема більше складної системи, що впливає

- на структуру й функціонування розглянутої;

- будь-яка система має ієрархічну структуру, елементами й зв'язками якої не можна зневажати без достатніх заснований;

- при аналізі системи необхідний облік зовнішніх і внутрішніх факторів, що впливають,

- прийняття рішень на основі частини з них без розгляду інших може

- привести до невірних результатів;

- властивості системи перевищують суму властивостей її елементів за рахунок якісно нових властивостей, відсутніх у її елементів – системних властивостей.

Сукупність елементів утворює систему, коли в них з'являються загальні цілі.

Якщо представити мети елементів у вигляді векторів, то вектори цілей елементів простої сукупності (набору елементів) орієнтовані довільно. При додаванні векторів результуючий вектор набору елементів не буде істотно відрізнятися от векторів елементів. Однак якщо вектори цілей елементів орієнтовані в одному напрямку, те результуючий вектор буде істотно відрізнятися от векторів елементів. У цьому випадку набір елементів трансформується в систему з додатковими можливостями.

Найважливішим відмінністю системи от набору елементів є те, що система має властивості, відсутніми в її елементів. Традиційний несистемний підхід припускає, що властивості об'єкта або суб'єкта є сукупність властивостей його частин.

Ефективність реалізації системного підходу на практиці залежить от уміння фахівця виявляти й об'єктивно аналізувати все різноманіття факторів і зв'язків досить складного об'єкта дослідження, яким є, наприклад, організація як об'єкт захисту.

Стосовно до інженерно-технічного захисту інформації передбачають:

- чітку постановку завдання, що включає визначення тематичних питань інформації і її джерел як об'єктів захисту, виявлення погроз цієї інформації й формулювання цілей і завдань захисту інформації;

- розробку принципів і шляхів рішення завдання;

- розробку методів рішення завдань;

- створення програмного, технічного й методичного забезпечення рішення завдання.

Системний аналіз передбачає застосування комплексу методів, методик і процедур, що дозволяють виробити в результаті аналізу моделі системи раціональні рекомендації з рішення проблем системи. Математичним забезпеченням системного аналізу є апарат дослідження операцій. Дослідження операцій являє собою комплекс наукових методів для рішення завдань ефективного керування організаційними системами, у яких основним елементом є людина. При рішенні слабоформалізованих завдань методами системного аналізу в більшості випадків вдається знайти тільки область раціональних рішень,

усередині якої перебуває найкращий (оптимальний) для конкретних вихідних даних результат.

Системний підхід і системний аналіз становлять основу теорії систем.²

Відповідно до вимог системного підходу сукупність взаємозалежних елементів, функціонування яких спрямовано на забезпечення безпеки інформації, утворює систему захисту інформації. Такими елементами є люди, інженерні конструкції й технічні засоби, що забезпечують захист інформації не залежно від їхньої приналежності до інших систем. Ядро системи захисту утворюють сили й засоби, основними функціями яких є забезпечення інформаційної безпеки. Однак вони становлять лише частину сил і засобів системи захисту інформації. Наприклад, у систему захисту інформації входять не тільки структурні підрозділи (служба безпеки, відділ режиму й таємності, 1-й відділ і ін.), призначені для захисту інформації, але всі співробітники організації, зобов'язані в повній мірі своєї відповідальності забезпечувати захист інформації. Отже, вони також є елементами системи захисту інформації організації. І якщо який-небудь співробітник організації порушить правила обігу із секретними документами, то можливий величезний збиток, незважаючи на бездоганну роботу інших елементів системи захисту.

Для системи захисту інформації дуже важко точно вказати місця входів і виходів у системі. Входами будь-якої системи є сили й впливи, що змінюють стан системи. Такими силами й впливами є загрози інформації. Загрози можуть бути внутрішніми й зовнішніми, у тому числі такі як слабка правова дисципліна співробітників, неякісна експлуатація засобів обробки інформації або наявність у приміщенні радіо й електричних приладів, побічні фізичні процеси в яких сприяють несанкціонованому поширенню інформації.

Джерелами загроз можуть бути зловмисники, технічні засоби усередині організації, співробітники організації, внутрішні й зовнішні поля, стихійні сили й т.д.

Виходи системи являють собою реакцію системи на входи. Виходами системи є заходи щодо захисту інформації. Однак локалізувати в просторі виходи системи так само складно, як і входи. Заходи щодо захисту інформації також включають різноманітні способи й засоби, у тому числі документи, що визначають доступ співробітників до інформації у конкретному структурному підрозділі організації.

Отже, *система захисту інформації являє собою модель системи, що поєднує сили й засоби організації, що забезпечують захист інформації.*

Вона описується параметрами, які показані на рис. 1.1.

2 Теорія систем зародилася в 30-і роки. У роки Другої світової війни корпорація «Ренд корпорешен» розробила методологію системних досліджень, а в 50-і роки теорія систем сформувалася як самостійний напрям. В 50-і роки в США було організовано «Суспільство досліджень в області загальної теорії систем». Його організаторами є фахівці з математичних проблем в області системотехніки й психології Л. Берталанфі, Р. Жерар і А. Рапопорт, К. Боулдинг. З 1956 р. «Суспільство ...» видає за редакцією Берталанфі й Рапорту щорічники «General System». В 1959 р. при Кейсовском технологічному інституті (США) створений «Центр системних досліджень». Корпорація «International Business Mashines Corporation» в 1963 р. організувала Інститут системних досліджень.

Створенню й розвитку теорії систем сприяли й праці росіян учених В. И. Вернадского, А. А. Богданова, Л. С. Виготського, Г. С. Поспелова, Н. П. Бусленко, В. Н. Садовського, Н. П. Федоренко й других. З 1969 року в Росії видається щорічник «Системні дослідження», у 1976 році заснований у Москві науково-дослідний інститут системних досліджень РАН (НДІСД).



1.1. Параметри системи захисту інформації

До параметрів системи відносяться:

- цілі й завдання (конкретизовані в просторі й у часі мети);
- входи й виходи системи;
- обмеження, які необхідний урахувати при побудові (модернізації, оптимізації) системи;
- процеси усередині системи, що забезпечують перетворення входів у виходи.

Цілі являють собою очікувані результат функціонування системи захисту інформації, а завдання те, що треба зробити для того, щоб система могла забезпечити досягнення поставлених цілей. Можливість рішення завдань залежить от ресурсу, що виділяється на захист інформації. Ресурс містить у собі людей, які вирішують завдання захисту інформації, фінансові, технічні й інші засоби, що витрачають на захисті інформації. Входами системи захисту інформації є загрози інформації, а виходами – цілі, які треба застосувати для запобігання загроз або знизивши їх до припустимого рівня. Заходи, дії й технології, що визначають цілі захисту від загрозам, утворюють процес.

Тому для слабоформалізованих завдань немає методів їхнього точного рішення, тобто процес являє собою вибір загроз на вході системи для вибору раціональних варіантів захисту, що задовольняють значенням використовуваних показників ефективності захисту.

Отже, процес вибору повинен включати також показники ефективності, по яких виробляється вибір мер з безлічі відомих. При відсутності формальних методів рішення слабоформалізованих завдань у загальному випадку можна забезпечити лише вибір раціональних рішень, що задовольняють певним вимогам і утворюють області рішень, усередині якої перебуває оптимальне рішення.

Рішення проблеми захисту інформації з погляду системного підходу можна сформулювати як трансформацію існуючої системи, що не забезпечує необхідний рівень захищеності, у систему із заданим рівнем безпеки інформації.

1.2. Цілі, завдання та ресурси системи захисту інформації

Формулювання цілей і завдань захисту інформації, як будь-якої іншої діяльності, представляє початковий етап забезпечення безпеки інформації.

У той же час фахівці в області системного аналізу вважають, що от чіткості й конкретності цілей і постановок завдань багато в чому залежить успіх у їхньому досягненні й рішенні.

Цілі захисту інформації такі:

- запобігання витоку, розкрадання, перекручування, підробки інформації;
- запобігання погроз безпеки особистості, суспільства, держави;
- запобігання несанкціонованих дій по знищенню, модифікації, копіюванню, блокуванню інформації, запобігання других форм незаконного втручання в інформаційні ресурси й інформаційні системи, забезпечення правового режиму як об'єкта власності;
- захист конституційних прав громадян по збереженню особистої таємниці, конфіденційності персональних даних, наявних в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;

– забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві й застосуванні інформаційних систем, технології й засобів їхнього забезпечення.

У загальному виді *ціль захисту інформації визначається як забезпечення безпеки інформації, що містить державну або інші таємниці*. Але така постановка цілі містить невизначені поняття: інформація й безпека.

Основною ціллю захисту інформації є забезпечення заданого рівня її безпеки.

Під заданим рівнем безпеки інформації розуміється такий стан захищеності інформації от загроз, при якому забезпечується припустимий ризик її знищення, зміни й розкрадання.

При цьому під знищенням інформації розуміється не тільки її фізичне знищення, але й стійке блокування санкціонованого доступу до інформації. Блокування інформації прямої загрози її безпеки не створює.

Загроза може бути реалізована з різною ймовірністю. Ймовірність реалізації загрози безпеки інформації визначає ризик її власника. Допустимість ризику означає, що збиток у результаті реалізації загроз не приведе до серйозних наслідків для власника інформації. Збиток може виявлятися в різноманітних формах: неотримання прибутку, очікуваної от інформації при її матеріалізації в із продукції або прийнятті більше обґрунтованого рішення; додаткові витрати на заміну зразків військової техніки, характеристики якої стали відомі ймовірному супротивникові тощо.

Ризик власника інформації залежить от рівня інженерно-технічного захисту інформації, що визначається ресурсами системи. Ресурс може бути визначений у вигляді кількості людей, приваблюваних до захисту інформації, у вигляді інженерних конструкцій і технічних засобів, застосовуваних для захисту, грошових сум для оплати праці людей, будівництва, розробки й покупки технічних засобів, їх експлуатаційних і інших витрат. Найбільш загальною формою подання ресурсу є грошова мера. Ресурс, що виділяється на захист інформації, може мати разовий і постійний характер. Разовий ресурс витрачається на закупівлю, установку й налагодження дорогої техніки, постійний – на заробітну плату співробітникам служби безпеки й підтримка певного рівня безпеки, шляхом експлуатації технічних засобів і контролю ефективності захисту. Середній ресурс оцінюється величиною коштів, виділюваних або витрачають у середньому в рік, як відношення витрат за певний період на тривалість цього періоду в літах. При побудові або модернізації системи захисту необхідні більші разові витрати на створення або закупівлю технічних засобів захисту за досить великий час їхнього застосування {5-10 років) окупаються.

Чим більший ресурс для організації захисту інформації, тим більш високий рівень безпеки інформації.

Завдання інженерно-технічного захисту, як будь-які інші завдання, – не мікроцілі, а чіткий і конкретний опис того, що треба зробити для досягнення мети.

Сформулювати завдання можна тільки тоді, коли визначена інформація. У постановці завдання вказується необхідність визначення раціональних мер для конкретної інформації з урахуванням наявного ресурсу.

2. Державна політика і система ТЗІ в Україні

Нормативними документами в сфері ТЗІ визначенні основні загрози безпеки інформації в Україні:

- діяльність інших держав, направлена на отримання переваги в внутрішньополітичній, економічній, військовій і інших сферах;
- недосконалість організації в Україні міжнародних виставок апаратури різного призначення (особливо рухомих) і заходів екологічного моніторингу, які можуть використовуватися для отримання інформації розвідувального характеру;
- діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, направлена на отримання переваги в політичній боротьбі і конкуренції;

- злочинна діяльність, направлена на протизаконне отримання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним або фізичним особам;
- використання інформаційної системи низького рівня, які приводять до залучення небездоганих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ і засобів ТЗІ;
- недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також кваліфікація технічного персоналу.

Система ТЗІ визначається як:

- суб'єктами, об'єднаних цілями і задачами інформації організаційними і інженерно-технічними заходами;
- нормативно-правової бази;
- матеріально-технічної бази.

Обов'язковість використання інженерно-технічних заходів для захисту інформації:

- інформації, яка складає державну та іншу передбачену законом таємницю;
- конфіденційної інформації, що є власністю держави;
- відкритої інформації, важливої для держави, незалежно від того, де вказана інформації циркулює;
- відкритої інформації, важливої для особистості та суспільства, якщо ця інформація циркулює в державних органах, підприємств, установ, організаціях;
- виконання на свій розсуд суб'єктами інформаційних відносин потреб відносно технічного захисту;
- конфіденційної інформації, яка не належить державі і відкритої інформації, яка важлива для особи і суспільства, якщо інформація циркулює не в межах державних органів, підприємств, установ і організацій;
- покладання відповідальності за формування і реалізацію державної політики у сфері ТЗІ за спеціально уповноважений центральний орган виконавчої влади;
- ієрархічна побудова організаційної структури системи ТЗІ і керівництво їх діяльності у межах повноважень, визначених нормативно-правовими актами;
- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
- координації дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації і системами інформаційної і національної безпеки;
- фінансове забезпечення системи ТЗІ за рахунок державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів і інших джерел.

3. Структура системи захисту інформації

Систему захисту інформації (СЗІ) для конкретних об'єктів (інформаційних систем) можна представити у вигляді:

- основ побудови системи захисту інформації;
- напрямків по захисту інформації;
- етапів побудови СЗІ.

Основою побудови системи захисту інформації є:

- 1) Законодавча, нормативно-правова, наукова і методична база забезпечення захисту інформації.
- 2) Структура і задачі органів (підрозділів), що забезпечують безпеку інформаційних технологій.
- 3) Організаційно-технічні і режимні заходи і методи захисту інформації.
- 4) Програмно-технічні способи і засоби, що використовуються для захисту інформації.

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури ІС і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

- 1) Захист об'єктів інформаційних систем.
- 2) Захист процесів, процедур і програм обробки інформації.
- 3) Захист каналів зв'язку.
- 4) Пригнічення побічних електромагнітних наведень.
- 5) Управління системою захисту.

Етапи побудови СЗІ необхідно пройти в рівній кількості для всіх і кожного окремо напрямків(з врахуванням всіх основ).

У загальному випадку можна виділити наступні етапи побудови СЗІ:

- визначення інформаційних ресурсів (ІР), які підлягають захисту;
- виявлення всієї кількості загроз безпеки ІР, які підлягають захисту;
- проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;
- розробка проекту (плану) системи захисту інформації, знижуючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз.
- реалізація проекту (плану) захисту інформації;
- визначення якості реалізації системи захисту;
- здійснення контролю функціонування і управління системою захисту.

Проходження етапів необхідно в тій чи іншій мірі здійснювати безперервно і по замкнутому циклу, з проведенням відповідного аналізу стану СЗІ та уточнюючою вимогою до неї після кожного кроку.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Якими факторами обумовлюється розвиток ТЗІ в Україні?
2. Які основні загрози безпеки інформації в Україні?
3. Що являє собою система ТЗІ і на яких принципах реалізується державна політика в сфері ТЗІ?
4. Хто виступає суб'єктом системи ТЗІ України?
5. Назвіть основні етапи побудови СЗІ.

Тема № 4. Практичне заняття № 2 на тему: Побічні електромагнітні випромінювання та наведення технічних засобів.

Навчальна мета заняття: ознайомитися із технічними каналами витоку інформації яка обробляється ТЗПІ.

Кількість годин – 2 год.

Навчальні питання:

1. Побічні електромагнітні випромінювання та наведення
 - 1.1. Побічні перетворення акустичних сигналів в електричні сигнали
 - 1.2. Паразитні зв'язки та наведення
2. Низькочастотні і високочастотні випромінювання технічних засобів
3. Електромагнітні випромінювання розподілених джерел
4. Витік інформації ланцюгами електроживлення
5. Витік інформації ланцюгами заземлення

Рекомендована література:

Основна

1. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
2. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.

3. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
4. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

5. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.

Нормативно-правові акти

6. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>.
7. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.
8. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.
11. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. ДБН А.2.2-96. Видання інформаційне. К. : Держкоммістобудування України, 1996. 18 с.

Інформаційні ресурси в Інтернеті

9. Перелік нормативно-методичних документів в галузі захисту інформації // Облікові документи для секретного діловодства / ТОВ «НІКС» : офіційний вебсайт. URL: <https://sites.google.com/a/nics.com.ua/price/>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Фізичну основу випадкових небезпечних сигналів, виникаючих під час роботи у виділеному приміщенні радіозасобів та електричних приладів, складають *побічні електромагнітні випромінювання і наведення (ПЕМВН)*.

II. Основна частина

1. Побічні електромагнітні випромінювання та наведення

Процеси і явища, утворюючі ПЕМВН, за способами виникнення можна розділити на 4 види:

- не передбачені функціями радіозасобів і електричних приладів перетворення зовнішніх акустичних сигналів в електричні сигнали;
- паразитні зв'язки та наведення;
- побічні низькочастотні випромінювання;
- побічні високочастотні випромінювання.

1.1. Побічні перетворення акустичних сигналів в електричні сигнали

Перетворювачі зовнішніх акустичних сигналів в електричні сигнали називаються акустоелектричними перетворювачами. До акустоелектричних перетворювачів відносяться фізичні пристрої, елементи, деталі та матеріали, здатні під дією змінного

тиску акустичної хвилі створювати еквівалентні електричні сигнали або змінювати свої параметри.

Класифікація акустoeлектричних перетворювачів по фізичних процесах, що створює небезпечні сигнали, приведені на рис. 1.1.



рис. 1.1. Класифікація акустико-електричних перетворювачів

На виході активних акустoeлектричних перетворювачів під дією акустичної хвилі виникають електричні сигнали. У пасивних акустoeлектричних перетворювачів тієї ж дії, акустичні хвилі викликають лише зміни параметрів перетворювачів.

За способами формування електричного сигналу активні акустoeлектричні перетворювачі можуть бути електродинамічними, електромагнітними і п'єзoeлектричними.

Небезпечні сигнали в електродинамічних акустoeлектричних перетворювачах виникають відповідно до закону електромагнітної індукції при переміщенні проводу в магнітному полі під дією акустичної хвилі (рис. 1.2)

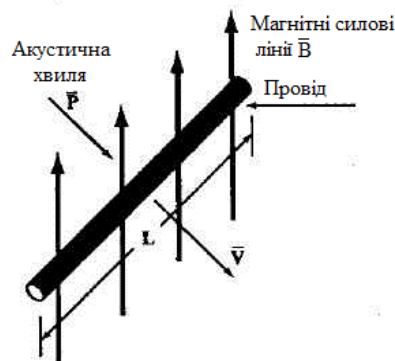


рис. 1.2. Принцип роботи електродинамічного акустико-електричного перетворювача

Якщо провід довжиною L під дією акустичної хвилі зі звуковим тиском P переміщається зі швидкістю v в магнітному полі з індукцією B , то в ньому за умови перпендикулярності силових магнітних ліній проводу і швидкості його переміщення, виникає ЕРС величиною

$E = LBv$. Так як $v = PS / ZMC$ (P – звуковий тиск, S – площа дроту, на яку тисне акустична хвиля, ZMC – величина механічного опору руху проводу), то $E = LBSP / ZMC$.

Найбільшою чутливістю володіють електродинамічні акустoeлектричні перетворювачі у вигляді динамічних головок гучномовців (див. рис. 1.3).

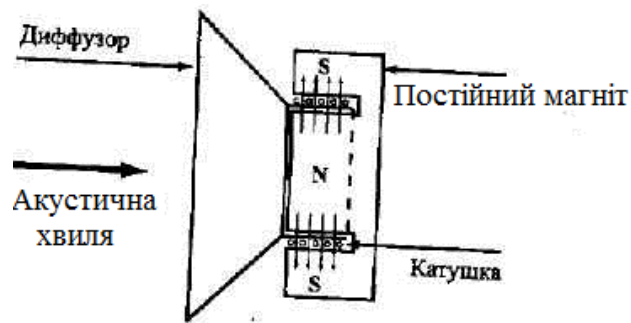


рис. 1.3. Схема електродинамічного гучномовця

Сутність перетворення полягає в наступному. Під тиском акустичної хвилі, поєднана з дифузorzом катушка, у вигляді картонного циліндра з намотаною на ньому тонкого дроту, переміщується в магнітному полі, створюваному постійним магнітом циліндричної форми. Відповідно до закону електромагнітної індукції в проводах катушки виникає електрорушійна сила (ЕРС), величина якої пропорційна гучності звуку.

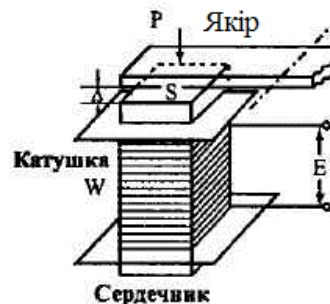


Рис. 1.4. схема електромагнітного акустoeлектричного перетворювача

Аналогічний ефект виникає в електромагнітних акустoeлектричних перетворювачах. До них відносяться електромагніти електромеханічних дзвінків і капсулів телефонних апаратів, крокові двигуни вторинних годин, кнопкові сповіщувачі ручного виклику пожежної служби об'єкту, що охороняється і т.д.

Для електромагнітного акустoeлектричного перетворювача напруга E на кінцях дроту, намотаного на катушці, пропорційна кількості витків W , площі s і відносній магнітній проникності сердечника, і пропорціонально відстані D між полюсом сердечника і рухомого якоря.

Перелік побутових радіо - та електроприладів, у яких виникають подібні процеси і які встановлюються в службових і житлових приміщеннях, досить великий. До них відносяться: телефонні апарати з електромеханічними дзвінками, вторинний електричний годинник системи єдиного часу підприємства або організації, вентилятори та ін. Рівні небезпечних сигналів у цих ланцюгах залежать від конструкції конкретного типу засобів та їх значення, мають значний розкид. Наприклад, небезпечні сигнали, створювані дзвінковим ланцюгом телефонного апарату, можуть досягати значень часток і одиниць мВ.

Активними акустoeлектричними перетворювачами являються також деякі кристалічні речовини (кварц, сегнетова сіль, титанат тощо), які широко використовуються в радіоапаратурі для стабілізації частоти і фільтрації сигналів, як акустичних випромінювачів сигналів виклику в сучасних телефонних апаратах замість електромеханічних дзвінків. На поверхні цих речовин при механічній деформації їх кристалічної решітки виникають електричні заряди.

У пасивних акустоелектричних перетворювачах акустична хвиля змінює параметри елементів схем засобів, у результаті чого змінюються параметри циркулюючих в цих схемах електричних сигналів. У більшості випадках під дією акустичної хвилі змінюються параметри індуктивностей і ємностей електричних ланцюгів. Відповідно до цього акустоелектричні перетворювачі називаються *індуктивними і ємнісними*.

Різновидом індуктивного є *магнітострикційний акустоелектричний перетворювач*³.

До найбільш поширених випадкових акустоелектричних перетворювачів відносяться:

- динаміки пристроїв телефонних апаратів;
- динамічні головки гучномовців, електромагнітні капсулі телефонних трубок, електричні двигуни, системи єдиного часу і побутових електроприборів;
- котушки контурів, дроселів, трансформаторів, проводи монтажних джгутів, пластини (електроди) конденсаторів;
- п'єзоелектричні речовини (віброакустичні випромінювачі акустичних генераторів перешкод);
- феромагнітні матеріали у вигляді сердечників трансформаторів і дроселів.

Загроза інформації від акустоелектричного перетворювача залежить, насамперед, від його чутливості. *Чутливість акустоелектричного перетворювача* характеризується відношенням величини електричного сигналу на його виході або зміни падаючого на нього напруги до сили звукового тиску на поверхню чутливого елемента перетворювача на частоті $f = 1000$ кГц і вимірюється в В/Па або мВ/Па. Очевидно, що *чим вище чутливість випадкового акустоелектричного перетворювача, тим більше потенційна загроза від нього для безпеки акустичної інформації*.

Небезпечні сигнали, утворені акустоелектричними перетворювачами, можуть:

- поширюватися по проводах, що виходять за межі контрольованої зони;
- випромінюватися в ефір;
- модулювати інші, більш потужні електричні сигнали, до яких можливий доступ зловмисників.

Технічну основу для реалізації першої загрози створюють, наприклад, непрацюючий гучномовець міської ретрансляційної мережі і ланцюг дзвінка телефонних апаратів, застарілих, але широко ще застосовуваних типів (ТА-68м, ТА-72М, ТАН-70-2, ТАН-76-3, ТА-1146, ТА-1162, ТА-1164 та ін.) Головка гучномовця безпосередньо підключається до кабелю (двожильного проводу) при прийомі першої програми міської ретрансляційної мережі через узгоджувальний трансформатор, який підвищує амплітуду небезпечних сигналів до 30-40 мВ. Сигнал такої амплітуди може поширюватися проводами ретрансляційної мережі на значні відстані, достатні для зняття інформації зловмисником за межами території організації. Однак, якщо в радіотрансляційній мережі йде передача мови або музики, то сигнали цієї передачі, які мають суттєво більшу (в 100-200 разів) амплітуду і співпадаючий діапазон частот, пригнічують небезпечні сигнали. Тому працюючі гучномовці, може бути, і заважають роботі людей, але виключають витік інформації з приміщень через акустоелектричні перетворювачі в гучномовцях.

Інша ситуація з акустоелектричними перетворювачами в телефонних апаратах. Телефонні лінії постійно підключені до джерела струму напругою близько 60 В. Хоча

3 Магнітострикція проявляється у зміні магнітних властивостей феромагнітних речовин (електротехнічної сталі та її сплавів) при їх деформації (розтягу, стиску, згинанні, крученні). Таке явище називається Вілларі ефектом або зворотнім магнітострикції, відкритим італійським фізиком Е. Вілларі в 1865 р. Цей ефект обумовлений зміною під дією механічного напруження доменної структури феромагнетика. Пряма магніто-реакція полягає в зміні геометричних розмірів і об'єму феромагнітного тіла при переміщенні його в магнітне поле. В результаті зворотної магнітострикції під дією акустичної хвилі змінюється магнітна проникність сердечників контурів, дроселів, трансформаторів радіоелектротехнічних пристроїв, що призводить до еквівалентної зміни значень індуктивностей ланцюга і модуляції.

небезпечні сигнали на виході дзвінкової мережі складають одиниці і частки мВ, їх не важко відокремити за допомогою фільтра від значно більш високої напруги постійного струму в телефонній лінії. Постійний струм фільтр не пропускає, а небезпечні сигнали з мовної інформації від акустoeлектричних перетворювачів з частотами в звуковому діапазоні проходять через фільтр з малим послабленням, а потім посилюються до необхідного значення.

Небезпечними сигналами на виході акустoeлектричних перетворювачів, що мають навіть дуже малі значення, не можна нехтувати. По-перше, чутливість сучасних радіоприймачів і підсилювачів електричних сигналів перевищує в десятки і сотні разів рівні найбільш поширених небезпечних сигналів, а, по-друге, малопотужні небезпечні сигнали можуть модулювати більш потужні електричні сигнали і поля, і таким чином збільшувати дальність розповсюдження небезпечних сигналів.

Наприклад, якщо небезпечні сигнали потрапляють в ланцюзі генераторів (гетеродинів) будь-якому радіо - або телевізійному приймачу, то вони модулюють гармонійні коливання цих операторів по амплітуді або частоті і поширюються за межами приміщення вже у вигляді електромагнітної хвилі. Також поля небезпечних сигналів на виході акустoeлектричних перетворень, які самі по собі через малу напруженість не несуть великої загрози безпеки інформації, можуть наводити в колах поруч розташованих радіoeлектронних засобів електричних сигналів з аналогічним ефектом.

1.2. Паразитні зв'язки та наведення

У будь-якому радіoeлектронному засобі або електричному приборі поруч із струмопроводами (проводами, провідниками друкованих плат), передбаченими їх схемами, виникають численні побічні шляхи, по яких поширюються електричні сигнали, в тому числі небезпечні сигнали акустoeлектричних перетворювачів. Ці шляхи створюються в результаті паразитних зв'язків та наведень. Першопричиною їх є поля, створювані електричними зарядами і струмами в ланцюгах радіoeлектронних засобів та приладів.

Однак незважаючи на вжиті заходи щодо зниження рівня паразитних зв'язків та Відомі *три види паразитних зв'язків*:

- ємнісний;
- індуктивний;
- гальванічний.

Ємнісний зв'язок утворюється в результаті впливу електричного поля, індуктивний – впливу магнітного поля, гальванічний зв'язок – через загально активний опір. Модель ємнісного паразитного зв'язку представлена на рис.1.5.

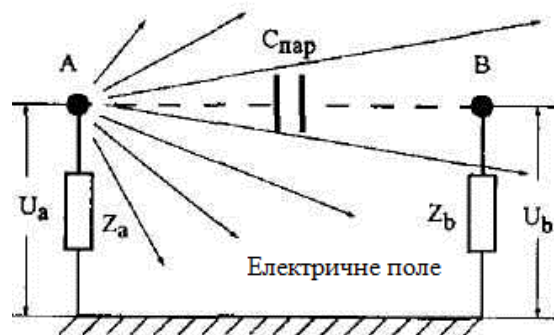


Рис. 1.5. паразитний ємнісний зв'язок

На цьому малюнку U_a – потенціал заряду точки А відносно корпусу, що створює електричне поле. В результаті впливу цього поля в точці В виникає заряд протилежного знаку. Величина потенціал заряду (наведеної напруги) U_b точки В відносно корпусу визначається відношенням ємнісного опору C , і опору Z_b :

$$U_b = U_a \frac{Z_b}{Z_b + Z_n},$$

де $Z_n = 1 / j\omega C_n$ – ємнісний опір між точками А і В, ω – кругова частота зміни потенціалу заряду точки А. Ємність С являється паразитною і створює ємнісний паразитний зв'язок між точками А і В.

Відношення називається $\beta_c = U_b / U_a = \frac{Z_b}{Z_b + Z_n}$ – ємнісного зв'язку. У більш реальних випадках β_c менше 1. Отже, коефіцієнт паразитного ємнісного зв'язку пропорційний величині паразитної ємності і частоті коливання електричного поля.

Ємнісний паразитний зв'язок виникає між будь-якими елементами схеми: проводами, радіoeлементами схеми і корпусом (шасі). Величина паразитної ємності на одиницю довжини проводів, паралельно розташованих на віддалені b один від одного, визначається по формулі:

$$C_n = \frac{\pi \epsilon_a}{\ln \left[\frac{2b}{d} + \sqrt{\left(\frac{b}{d} \right)^2 - 1} \right]},$$

Де d – діаметр проводів; ϵ_a – абсолютне значення діелектричної постійної.

З цієї формули випливає, що величина ємності пропорційна діелектричній проникності середовища, діаметру проводів і обернено пропорційна відстані між проводами. Так як між поруч розташованими основними і допоміжними засобами існує паразитний ємнісний зв'язок, що сприяє передачі сигналів і захищається інформацією від ОТЗС до ДТЗС, то для визначення величини наведення треба знати їх паразитні ємності. Ці ємності називаються власними ємностями радіoeлектронного засобу та електричного приладу. Обчислити власну ємність можна тільки для найпростіших конфігурацій типу штир, куля, диск. Наприклад, для штиря довжиною L паразитна ємність становить $C_n \sim 0,1l$, для диска $C_n \sim 0,35D$, кулі – $C_n \sim 0,56 D$, де D – діаметр кулі і диска. Для реальних радіoeлектронних засобів складної конфігурації власна ємність C_n визначається експериментально шляхом розміщення засобів в однорідному електричному полі і виміром наведеної напруги на його виході U_v . Попередньо змінюється наведене еталонне напруга U_n в найпростішому пристрої (диску, кулі та ін.) з відомою (еталонною) власною ємністю C_{ne} , вміщеному в це поле. На основі отриманих даних власна ємність досліджуваного засобу визначається методом заміщення, відповідно до якого $C_m = C_{ne} * U_v / U_n$.

Взаємна індуктивність замкнутих ланцюгів залежить від взаємного розташування і конфігурації провідників. Вона тим більша, чим більша частина магнітного поля струму в одного ланцюга пронизує провідники іншого ланцюга.

Слід розрізняти взаємну індуктивність між провідниками різних ланцюгів від індуктивності провідника. Індуктивність характеризує властивість провідника перешкоджати проходити через нього струму, яке обумовлено явищем самоіндукції. Вона виникає, коли силові лінії змінного магнітного поля пронизують провідники, по яких протікає струм, що створює це магнітне поле.

Гальванічний паразитний зв'язок ще називають зв'язком через загальний опір, що входить до складу декількох кіл. Такими загальними опорами можуть бути опір сполучних проводів і пристроїв живлення і управління. Наприклад, вузли та блоки комп'ютера, що здійснює обробку інформації, з'єднані з напругою +5 В блоку живлення. Для установки «0» тригерів дискретних пристроїв на відповідні їх входи подається одночасно відповідний сигнал управління.

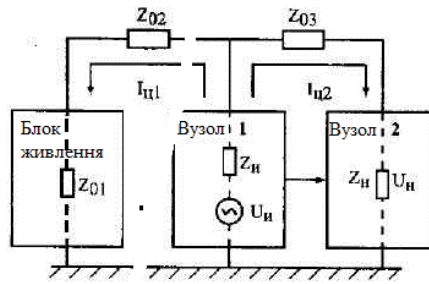


Рис. 1.7. паразитний гальванічний зв'язок

Відповідно до нього, до блоку живлення через загальні опори Z_{01} , Z_{02} , і Z_{03} підключені вузол 1 і вузол 2 радіоелектронного засобу. Сигнал напругою U_i 1-го вузла створює струми $I_{н1}$ і $I_{н2}$, в результаті яких на еквівалентному опорі Z_i 2-го вузла виникає напруга наведення U_i . Ця рівність $B_i = U_m / U_i$ називається коефіцієнтом паразитного гальванічного зв'язку.

Якщо побічні поля та електричні струми є носіями, що захищаються, то паразитні наведення і зв'язки можуть призводити до витоку інформації. Отже, паразитні зв'язки та наведення представляють собою побічні фізичні процеси і явища, які можуть призводити до витоку інформації, що захищається.

Можливість витоку інформації через паразитні зв'язки та наведення носить ймовірнісний характер і залежить від багатьох факторів, у тому числі від конфігурації, розмірів (відносно періоду коливань струмів, що протікають) і взаємного положення випромінюючих та приймаючих струмопровідних елементів засобів. І на відміну від передбачених для зв'язку функціональних антен, конструкція і характеристики яких визначаються при створенні радіопередавальних і радіоприймальних засобів, ці елементи можна назвати випадковими антенами.

Випадковими антенами можуть бути монтажні дроти, з'єднувальні кабелі, доріжки печатних плат, радіодеталі, металеві корпуси засобів та приладів та інші елементи засобів. Параметри випадкових антен істотно гірші функціональних. Але через невеликі відстані між передаючими і прийомними випадковими антенами (в радіоелектронному засобі або одному приміщенні) вони створюють загрози витоку інформації.

Випадкові антени мають складну і часто невизначену поділену конфігурацію, досить точно розрахувати значення їх електричних параметрів, що збігаються з вимірюваними, дуже складно. Тому реальну випадкову антену замінюють її моделями у вигляді дротяної антени – відрізання дроту (вібратора) і рамки.

У ближній зоні вібратор створює переважно електричне поле. Властивості дротяної антени перетворити електричний сигнал в поле (радіосигнал) і навпаки характеризуються параметром антени, названим діючою висотою вимірюваним в м. Чинна висота передавальної антени представляє собою параметр, що зв'язує напруженість електричного поля, створюваного антеною в напрямку головного випромінювання, з рівнем сигналу в самій антені. Діюча висота приймальної антени дорівнює відношенню ЕРС в приймальній антені до напруженості викликає її електричне поле: $Hd == U_i / E$. При цьому передбачається, що приймальна антена орієнтована в просторі відповідно до поляризації електромагнітних полів і прийом здійснюється з напрямку максимального рівня поля. Так як відношення напруженостей електричної і магнітної складових електромагнітного поля біля складових антени дорівнює хвильовому опору середовища ($Z_a = E_a / H_a$), то $H_i = U_i / H Z_i$.

Коефіцієнт підсилення випадкової антени у вигляді замкнутого ланцюга (рамки) оцінюється за допомогою параметра, названого діючою довжиною антени $L = U / H$. За аналогією зі способами визначення власної ємності кожна діюча висота (довжина) випадкової антени знаходиться методом заміщення.

Паразитні зв'язки можуть викликати витік інформації по проводах і створювати умови для виникнення побічних електромагнітних випромінювань. За рахунок паразитних

зв'язків виникають небезпечні сигнали в проводах кабелів різних ліній і ланцюгів, у тому числі в ланцюгах заземлення та електроживлення, а також виникають паразитні коливання в підсилювачах, дискретних пристроях та ін.

Серйозну загрозу безпеці інформації створюють наведення сигналів ОТЗС на дротах та кабелях, що виходять за межі контролюючої зони. Коли струм проходить по провідникам першого ланцюга, навколо них створиться магнітне поле, силові лінії якого пронизують провідники другого ланцюга. В результаті цього по ланцюгу потече крім основного ще й перехідний струм, що створює перешкоду основному. Захищеність від взаємних перешкод оцінюється так званим перехідним загасанням $Z = 10 \lg P_{c1} / P_{i2}$, де P_{c1} і P_{i2} – потужність сигналів в 1-го ланцюга і наведення від них у 2-го ланцюга. Для надійного захисту інформації перехідне загасання повинно бути не менше величини $10 \lg P_{c1} / P_{i2}$, де P_{c1} і P_{i2} – потужність сигналу з інформацією та чутливість приймача зловмисника, перехоплює наведений сигнал. Так як кабелі в будівлі укладаються в спеціальних колодязях і нішах, то між кабелями за рахунок їх досить близького і паралельного на великій відстані розташування виникають досить великі паразитні зв'язки між кабелями внутрішньої і міської АТС, інших інформаційних ліній зв'язку, ланцюгами електроживлення та заземлення. Так як співробітники організації при розмові по телефонам внутрішньої АТС частіше допускають порушення режиму таємності (конфіденційності), ніж під час розмови по міській АТС, то при регулярному підслуховуванні розмов по внутрішній АТС можна добути цінну інформацію.

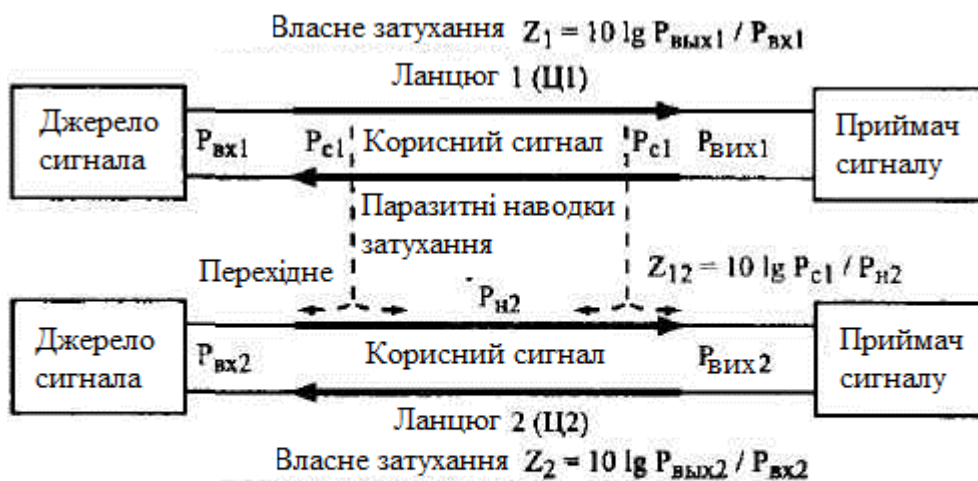


рис. 1.8. паразитні наведення

Сучасна архітектура службових приміщень передбачає створення між міжповерховими перекриттями і стелею (підлогою) вільного простору для прокладки різних кабелів (електроживлення, внутрішньої і міської АТС, трансляції, оперативного та диспетчерського зв'язку, мереж передачі даних та ін.) Це створює додаткові можливості для виникнення між проводами кабелів паразитних зв'язків та появи небезпечних сигналів, що поширюються за межі контрольованої зони.

2. Низькочастотні і високочастотні випромінювання технічних засобів

Велику загрозу безпеці інформації створюють також побічні випромінювання радіо-та електротехнічними засобами електромагнітних полів, які містять захищену інформацію. Джерелами випромінювань можуть бути ланцюги, що містять статичні або динамічні заряди (електричний струм), в інформаційні параметри яких тим чи іншим способом записується захищена інформація. Носії інформації, що захищається у вигляді

статичних або динамічних зарядів можуть потрапляти в ці ланцюги безпосередньо, якщо ці ланцюги беруть участь в обробці, передачі і зберіганні інформації що захищається або самі елементи кіл мають властивості акустоелектричних перетворювачів, або опосередковано, коли небезпечні сигнали проникають в випромінюючі ланцюги через паразитні зв'язки.

Вид випромінювання і характер поширення електромагнітного поля в просторі залежить від частоти коливань поля та виду випромінювача. Розрізняють низькочастотні і високочастотні небезпечні випромінювання.

Під *низькочастотними випромінюваннями* розуміють випромінювання електромагнітних полів, частоти яких відповідають звуковому діапазону. Джерелами таких випромінювань є пристрої і ланцюги звукопідсилювальної апаратури (мікрофони, підсилювачі потужності, аудіомагнітофон, гучномовці та їх погоджуючі трансформатори, кабелі між мікрофонами і підсилювачами, підсилювачами і гучномовцями, ланцюги, що містять випадкові акустоелектричні перетворювачі, телефонні апарати і кабелі внутрішньої АТС та ін.)

Найбільшу загрозу створюють засоби звукофіксації приміщень для озвучування акустичної інформації, яка містить державну або комерційну таємницю. Ці засоби включають мікрофони, підсилювачі потужності, гучномовці, встановлюються на стінах великих приміщень (залів для нарад, конференц-залів) або в спинки крісел, а також з'єднувальні кабелі. Причому часто підсилювачі потужності розміщуються в технічному приміщенні, віддаленому на значній відстані від конференц-зали.

По проводам кабелів звукопідсилювальної апаратури протікають великі струми, складові частки і одиниці ампер. Ці струми створюють потужні магнітні нулі, які, по-перше, можуть поширюватися за межі виділеного приміщення, будівлі і навіть організації, а по-друге, наводити ЕРС в будь-яких струмопровідних конструкціях, у тому числі в колах електроживлення і металевій арматурі будівель.

До *високочастотних небезпечних випромінювань* відносяться електромагнітні поля, що випромінюються ланцюгами радіоелектронних засобів, по яких поширюються високочастотні (вище звукового діапазону) сигнали з секретною (конфіденційною) інформацією. Можна стверджувати, що якщо не прийняті спеціальні допоміжні заходи, то джерелами подібних небезпечних побічних ВЧ-випромінювань можуть бути будь-які ланцюга радіо- і електричних засобів. До основних джерел побічних випромінювань з потужністю, достатньої для поширення електромагнітного поля за межі контрольованої зони, наприклад приміщення, відносяться:

- гетеродина радіо - і телевізійних приймачів;
- генератори підмагнічування і стирання аудіо - і відеомагнітофонів;
- підсилювачі й логічні елементи в режимі паразитної генерації;
- електронно-променеві трубки засобів відображення інформації, що захищається (моніторів, телевізорів);
- елементи ВЧ-нав'язування;
- монітори, клавіатура, принтери та інші пристрої комп'ютерів, в яких циркулюють сигнали в паралельному коді.

До випромінюючих елементів ВЧ-нав'язування відносяться радіо - і механічні елементи, які забезпечують модуляцію підводяться до них зовнішніх електричних і радіосигналів. До таких елементів відносяться:

- нелінійні елементи, на які одночасно надходять низькочастотний електричний сигнал захищається інформацією (небезпечний сигнал) і високочастотний гармонійний сигнал;
- струмопровідні механічні конструкції, що змінюють свій розмір і перевідбивається зовнішнє електромагнітне поле.

3. Електромагнітні випромінювання розподілених джерел

Основними розподіленими джерелами магнітного, електричного та електромагнітного полів є симетричні і несиметричні кабелі. Характер випромінювання полів для симетричних і несиметричних кабелів істотно розрізняється.

До несиметричним відносяться кабелі, проводи яких мають різні електричні параметри або по провідникам протікають різні струми. Приклади несиметричного кабелю – коаксіальні телевізійні кабелі та стрічкові кабелі для з'єднання пристроїв комп'ютера. В коаксіальному кабелі струми протікають по центральному проводу та екрану, що мають різні електричні параметри. Провідники стрічкових кабелів мають однакові електричні параметри, але по інформаційним та корпусним провідникам протікають різні струми.

Розподілені джерела випромінювань створюють електромагнітні випромінювання несиметричних і симетричних кабелів. Несиметричний кабель утворює магнітну рамку, утворену інформаційним проводом і землею. Випромінювання симетричного кабелю створюються за рахунок асиметрії кабелю відносно точки вимірювання і землі.

4. Витік інформації ланцюгами електроживлення

До ланцюгів, які мають вихід за межі контрольованої зони і в які можуть проникнути небезпечні сигнали через паразитні зв'язку будь-яких видів, відносяться, перш за все, ланцюги електроживлення. Тому запобігання витоку інформації з цих ланцюгів є одним із завдань інженерно-технічного захисту інформації.

Ланцюги електроживлення забезпечують передачу електричної енергії у вигляді змінного електричного струму напругою 380/220 В і частотою 50 Гц від зовнішніх джерел (підстанцій) переважній більшості встановлюються в приміщеннях радіо-і електричних приладів (технічних засобів і систем – ТСС).

Типове вторинне джерело живлення (блок живлення) складається з наступних послідовно з'єднуються вузлів:

- мережевого трансформатора з коефіцієнтом трансформації n ;
- випрямляча;
- фільтра блоку живлення;
- стабілізатора;
- пристрої для захисту блоку живлення від короткого замикання.

Трансформатор перетворює напругу 220В в напругу живлення вузла (блоку) радіоелектронного засобу. Для отримання постійної напруги змінний струм випрямляється і з метою зменшення пульсацій фільтрується. Параметри фільтра визначають з умови забезпечення допустимого коефіцієнта пульсацій напруги живлення порядку 1-2% вихідних каскадів РЕЗ, струми в яких складають більшу частину струмів через еквіваленту навантаження з провідністю G_M .

5. Витік інформації ланцюгами заземлення

Так як ланцюги заземлення виходять за межі приміщення і будівлі, то поширюються по ним небезпечні сигнали створюють загрози міститься в них інформації. Ланцюги заземлення в загальному випадку створюються для виконання таких функцій:

- виключення можливості ураження електричним струмом персоналу, який обслуговує технічні засоби (захисна функція);
- встановлення опорного (загального) «нуля» для вимірювань рівнів вимірюваних сигналів (базова функція);
- екранування електричного поля (екранує функція);
- забезпечення шляхів для протікання зворотних (обернених) живлячих і сигнальних струмів (поворотна функція).

При заземленні використовуються два поняття: «земля» і «маса». Під масою розуміються схемотехнічні конструкції (шина, дріт опорного потенціалу, корпус, нульова точка, нейтрал), по відношенню до яких вимірюються потенціали сигналів схеми. «Маса» і «земля», як правило, але не завжди, гальванічно пов'язані один з одним, а їх потенціали

можуть відрізнятись. Потенціал землі, так само як рівень океану, приймається за нульовий. Незалежно від виконуваної функції її ефективність тим вища, чим менше опір ланцюга заземлення, що включає шину заземлення і заземлювач.

Небезпечні сигнали в ланцюгах заземлення виникають з двох причин:

- наведення в ланцюгах заземлення РЕЗ полями побічних електромагнітних випромінювань;

- протікання струму заземлення по контуру заземлення.

Чим вище частота сигналу, тим більше струм заземлення.

Небезпечний сигнал може бути «знятий» з ланцюга заземлення індуктивним способом або з опору, включеного послідовно в цей ланцюг. Так як завжди до однієї шини заземлення підлягає кілька радіоелектронних засобів, то протікають по ній струми являють собою суміш струмів різних джерел. Тому виділення в цій суміші небезпечних сигналів з визначеного приміщення можливо в принципі, але пов'язане з виконанням низки умов, у тому числі із забезпеченням відносини сигнал/перешкода, необхідним для виділення інформації з необхідною якістю. Перешкоди являють собою не тільки теплові шуми, але і сигнали інших радіоелектронних засобів.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Як і де утворюються паразитні випромінювання?
2. Який механізм утворення наводок? Де вони виникають?
3. В чому полягає небезпека паразитних випромінювань та наводок?
4. Дайте визначення технічних заходів із захисту об'єкту.
5. Які основні складові технічних заходів?
6. Який порядок проведення робіт з ТЗІ?
7. В чому полягає особливість використання беззаходових способів зняття інформації?
8. В чому полягає фізична сутність способу високочастотного нав'язування для зняття інформації?

Тема № 5-6. Практичне заняття № 3 на тему: Технічні канали витоку інформації.

Навчальна мета заняття: ознайомитися із технічними каналами витоку інформації яка обробляється ТЗПІ.

Кількість годин – 4 год.

Навчальні питання:

1. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ.

2. Класифікація методів та засобів захисту інформації від витоку технічними каналами.

Література:

Основна

1. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
2. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.
3. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
4. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

5. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з

дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.

Нормативно-правові акти

6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.
7. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>.
8. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.
9. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-2005: чинний від 2005-11-08. К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. 17 с. URL: <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350>.

Інформаційні ресурси в Інтернеті

10. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.
11. Відомості про засоби технічного захисту інформації, на які закінчився термін дії сертифікатів відповідності та експертних висновків // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Згідно з Державним стандартом України (ДСТУ 3396.2-96) «Технічний захист інформації. Терміни та визначення», *технічний канал витоку інформації* – сукупність носіїв інформації, середовища їх поширення та засобів технічної розвідки.

Канал витоку інформації – неконтрольований фізичний шлях від джерела інформації за межі організації чи кола осіб, що володіють охоронюваними відомостями, за допомогою якого можливо неправомірно оволодіння зловмисником інформацією.

II. Основна частина

1. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ

Для перехоплення, обробки й аналізу інформації в КВІ можуть використовуватися різноманітні технічні засоби (ТЗ), а також люди (порушники). Тоді існуючі КВІ в залежності від джерел і одержувачів інформації утворюють чотири основних типи каналів: «людина – людина», «людина – ТЗ», «ТЗ – ТЗ» і «ТЗ – людина».

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

Виходячи з фізичної природи утворення, технічні канали витоку інформації класифікують як:

- *візуально-оптичні канали* – це, як правило, візуальне спостереження: безпосереднє чи віддалене із застосуванням технічних засобів. Переносником інформації виступає світло, що випускається джерелом конфіденційної інформації, або відбите від нього у видимому, інфрачервоному чи ультрафіолетовому діапазонах;

- *віброакустичні канали*. В акустичних каналах переносником інформації (мова, шуми) виступає звук, що лежить у смузі ультразвуку (понад 20000 Гц), чутного та інфразвукового (до 16 Гц) діапазонів. Діапазон звукових частот, які чує людина, лежить у межах від 16 до 20000 Гц, а як таких, що містяться в людському мовленні, – від 100 до 6000 Гц. Середовищем поширення звуку є повітря, земля, вода, будівельні конструкції (цегла, залізобетон, металева арматура та ін.);

- *радіоелектронний канал*. Переносником інформації є або електромагнітні хвилі в радіочастотному діапазоні, або струм, що проходить через загальне джерело живлення або по колу заземлення;

- *матеріально-дійсними каналами витоку* виступають найрізноманітніші матеріали у твердому, рідкому чи газоподібному або корпускулярному (радіоактивні елементи) вигляді.

Технічні засоби прийому, обробки, зберігання й передачі інформації (ТЗПІ) – це технічні засоби, що безпосередньо обробляють конфіденційну інформацію. До таких засобів відносяться:

- електронно-обчислювальна техніка, режимні АТС;
- системи оперативно-командного й гучномовного зв'язка;
- системи звукопідсилення;
- звукового супроводу і звукозапису і т.д.

При виявленні технічних каналів витоку інформації ТЗПІ необхідно розглядати як систему, що включає основне (стаціонарне) устаткування, кінцеві пристрої, сполучні лінії (сукупність проводів і кабелів, що прокладаються між окремими ТЗПІ і їхніми елементами), розподільні й комутаційні пристрої, системи електроживлення, системи заземлення.

2. Класифікація методів та засобів захисту інформації від витоку технічними каналами

1. Організаційні методи захисту.
2. Технічні методи захисту.

Організаційний захід – це захід захисту інформації, проведення якого не вимагає застосування спеціально розроблених технічних засобів.

До основних організаційних і режимних заходів відносяться:

- залучення до проведення робіт по захисту інформації організацій, що мають ліцензію на діяльність в області захисту інформації, видану відповідними органами;
- категоріювання та атестація об'єктів ТЗПІ і виділених для проведення закритих заходів приміщень (далі виділених приміщень) по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідної міри секретності;
- використання на об'єкті сертифікованих ТЗПІ у ДТЗС;
- встановлення контрольованої зони навколо об'єкту;
- залучення до робіт по будівництву, конструкції об'єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

- організація контролю і обмеження доступу на об'єкти ТЗП і у виділені приміщення;
- введення територіальних, частотних, енергетичних, просторових і тимчасових обмежень в режимах використання технічних засобів, що підлягають захисту;
- відключення на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів, від ліній зв'язку і так далі.

Технічний захід – це захід по захисту інформації, який передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.

До технічних заходів з використанням пасивних засобів відносяться :

– **контроль і обмеження доступу на об'єкти ТЗП та у виділені приміщення:**

– встановлення на об'єктах ТЗП і у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу.

– **локалізація випромінювань :**

- екранування ТЗП та їх ліній з'єднання;
- заземлення ТЗП і екранів їх ліній з'єднання;
- звукоізоляція виділених приміщень.

– **розв'язування інформаційних сигналів:**

- встановлення спеціальних засобів захисту типу «Граніт» у допоміжних технічних засобах і системах, що мають «мікрофонний ефект» та вихід за межі контрольованої зони;
- встановлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання і каналізації що мають вихід за межі контрольованої зони;
- встановлення автономних або стабілізованих джерел електроживлення ТЗП;
- встановлення облаштувань гарантованого живлення ТЗП (наприклад, мотор-генераторів);

- встановлення в ланцюгах електроживлення ТЗП, а також в лініях освітлювальної і розеткової мереж виділених приміщень перешкодоподавляючих фільтрів типу Ф11.

До технічних заходів з використанням активних засобів відносяться:

– **просторове зашумлення:**

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних перешкод (при виявленні і визначенні частоти випромінювання заставного пристрою або побічних електромагнітних випромінювань) з використанням засобів створення прицільних перешкод;

- створення акустичних і вібраційних перешкод з використанням генераторів акустичного шуму;

- пригнічення диктофонів в режимі запису з використанням пригнічувачів диктофонів;

– **лінійне зашумлення:**

- лінійне зашумлення ліній електроживлення;

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

– **знищення закладних пристроїв**, підключених до лінії, з використанням спеціальних генераторів імпульсів (спалювачів «жучків»).

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Задачі контролю захищеності об'єкта від витоку технічними каналами.
2. В якому випадку пристрій об'єкта та сам об'єкт вважаються захищеними від витоку каналами ПЕМВ?
3. Види контролю захищеності об'єктів від розвідки (радіомоніторинг).
4. Який орган визначає склад нормативної та методичної документації для атестації конкретних об'єктів інформатизації?

Тема № 7, 8. Практичне заняття № 4 на тему: Методи та засоби захисту інформації, що оброблюється ТЗПІ, від витоку технічними каналами.

Навчальна мета заняття: ознайомитися з основними Методи та засоби захисту інформації, що оброблюється ТЗПІ, від витоку технічними каналами

Кількість годин – 6 год.

Навчальні питання:

План лекції

1. Методи та засоби захисту інформації, що оброблюється ТЗПІ, від витоку технічними каналами.

1.1 Екранування засобів ТЗПІ. Властивості та вимоги щодо засобів екранування.

1.2 Заземлення засобів ТЗПІ. Типові системи заземлення технічних засобів.

1.3 Особливості та вимоги до засобів фільтрування інформаційних сигналів.

Рекомендована література:

Основна

1. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.

2. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.

3. 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.

4. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.

5. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

6. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.

7. Романенко С. М., Дмитренко В. П., Карпуков Л. М. Поля і хвилі в задачах технічного захисту інформації : навч. посіб. для студентів ВНЗ, які навчаються за напрямом підгот. «Кібербезпека» / Запоріж. нац. техн. ун-т. Запоріжжя : ЗНТУ, 2016. 280 с.

Нормативно-правові акти

8. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>.

9. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.

10. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К.: Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.

12. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. ДБН А.2.2-96. Видання інформаційне. К.: Держкоммістобудування України, 1996. 18 с.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К.: Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с.

II. Основна частина

1. Методи та засоби захисту інформації, що оброблюється ТЗПІ, від витоків технічними каналами.

Захист інформації, що оброблюється ТЗПІ, здійснюється з використанням пасивних та активних методів та засобів.

Пасивні методи захисту направлені на:

- ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів, унеможливлених їх виділення засобами розвідки на шумовому фоні;
- ослаблення наведень побічних електромагнітних випромінювань ТЗПІ на сторонні провідники та з'єднувальні лінії ДТЗС, що виходять за межі зони що контролюється до рівнів, унеможливлених їх виділення засобами розвідки на шумовому фоні;
- виключення (ослаблення) просочування інформаційних сигналів ТЗПІ до мереж живлення що виходять за межі зони що контролюється до рівнів, унеможливлених їх виділення засобами розвідки на шумовому фоні;

Активні методи захисту спрямовані на:

- створення просторових маскуючих електромагнітних завад з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлених їх виділення засобами розвідки на шумовому фоні;
- створення маскуючих електромагнітних завад у сторонніх провідниках та з'єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлених їх виділення засобами розвідки на шумовому фоні;
- послаблення побічних електромагнітних випромінювань ТЗПІ та їх наведень у сторонні провідники здійснюється шляхом екранування та заземлення ТЗПІ та їх ліній заземлення.

Послаблення просочування інформаційних сигналів ТЗПІ до мереж електроживлення здійснюється шляхом фільтрації інформаційних сигналів.

1.1 Екранування засобів ТЗПІ. Властивості та вимоги щодо засобів екранування.

Основні вимоги, які пред'являються до системи заземлення, полягають у наступному:

- Система заземлення повинна включати загальний заземлювач, заземлюючий кабель, шини і дроти, що сполучають заземлювач з об'єктом;
- Опору заземлюючих провідників, а також земляних шин повинні бути мінімальними;

- Кожен заземлюється елемент повинен бути приєднаний до заземлювача або до заземлюючої магістралі за допомогою окремого відгалуження.

Вузли та елементи електронної апаратури створюють електромагнітні поля в ближній зоні та з'єднувальних лініях ТЗПІ та ДТЗС. Зниження рівня ПЕМВ здійснюється за рахунок їх екранування.

Відрізняють такі способи екранування:

- електростатичне екранування;
- магнітностатичне екранування;
- електромагнітне екранування.

Загалом характерні елементи конструкцій екранованих приміщень, які створюють склад ТЗПІ та ДТЗС, повинні проектуватись та будуватись з урахуванням єдиних вимог, які забезпечують мінімізацію випромінювань за межі приміщення та мінімізацію проникнення електричних сигналів дротами, які виходять за межі приміщення. Основні конструктивні елементи приміщень серверних та електронних архівів, які можна віднести до ТЗПІ і ДТЗС виглядають таким чином:

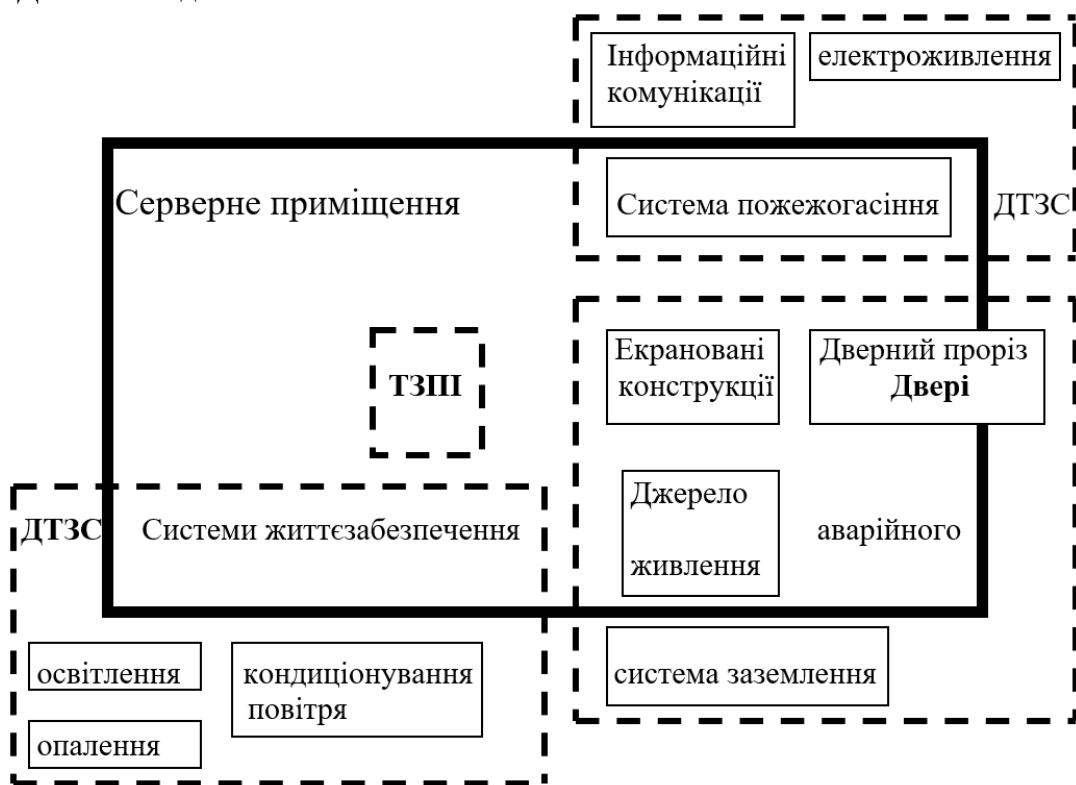


Рис. 1 – Схема приміщення серверної

Рекомендації та вимоги, щодо їх проектування при небезпеці витоку інформації за рахунок ПЕМВН, або втрати інформації за рахунок зовнішніх електромагнітних полів сформульовані в документах:

– НД ТЗІ ТР ЕОТ – 95 «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наведень»;

– НД ТЗІ ТР ТЗІ - ПЕМВН-95 «Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень».

Вводи комунікацій, трубопроводи, кабелі тощо – повинні мати мінімальні розміри. Необхідно надійно з'єднувати екрани провідних комунікацій з поверхнею екран-споруди.

2. Метод заземлення. Типові системи заземлення технічних засобів

Характеристики систем заземлення визначені в ГОСТ 464-79 «Заземления для стационарных установок проводной связи, радиорелейных станций,

радиотрансляционных узлов и антенн систем коллективного приема телевидения. Нормы сопротивления», у якому нормується опір заземлення у межах 1 Ом для систем колективного прийому телебачення більш як для 50 абонентів.

Використовуються декілька типів заземлення: одноточкові, багатоточкові і комбіновані (гібридні) схеми, а також послідовні та паралельні схеми, та їх комбінації.

Одноточкова паралельна схема цього недоліку не має. Але має інший недолік. Вона потребує великої кількості довгих заземлюючих дротів. Це призводить до зростання електричного опору системи заземлення. Крім того, тут можуть з'являтися небажані взаємні зв'язки, які створюють декілька ланцюгів заземлення для кожного пристрою. В результаті можуть з'являтися вирівнюючі струми і різниці потенціалів між пристроями.

Багатоточкова схема вільна від цих недоліків. Але тут треба приймати запобіжні заходи від створення замкнених електричних контурів.

Основні вимоги до систем заземлення:

- система має включати до себе загальний заземлювач, кабель заземлення, шини та дроти, які з'єднують заземлювач з об'єктом;
- опір системи заземлення має бути мінімальним;
- кожний елемент що заземлюється має підключатися до заземлювача або до заземлюючої магістралі за допомогою окремого відгалужувача. Послідовне підключення декількох елементів, що заземлюються, до одного провідника, забороняється;
- система має бути вільна від замкнених контурів;
- не треба використовувати загальний провідник для систем екрануючих заземлень, захисних заземлень та сигнальних кіл.
- контакти мають бути захищені від корозії та утворення оксидних плівок, а також від утворення гальванопар;
- можна використовувати в якості заземлення нульові фази електромереж, металеві конструкції будівель, екрани і захисні оболонки підземних кабелів, металеві труби систем опалення, водопостачання тощо.

Якщо якомога краще забезпечений електричний контакт між заземлювачем та ґрунтом, а магістраль заземлення має невелику довжину, то опір системи заземлення, в основному, складає опір ґрунту.

Нормований опір ґрунтів становить у середньому величини, що наводяться нижче:

Таблиця 1 Нормований опір ґрунтів

Характер ґрунту	Зведений опір ρ , Ом·м		
	середній	мінімальний	максимальний
Зола, попіл, садовий ґрунт	40	40	40
Глина, суглинок, сланець	70	55	150
Сухий пісок	2500	1000	4000
Вологий пісок	300	130	400
Бетон	500	40	1000
Гравій глинистий неоднорідний	300	250	350

З втратою води провідникові властивості зменшуються. Для більшості ґрунтів 30% води достатньо для забезпечення опору зменшеному у 20-30 разів.

При промерзанні ґрунту його опір різко зростає. Опір заземлення залежить і від конструкції заземлювача.

Зрошення ґрунту навкруги заземлювачів 2...5 відсотковим розчином солі знижує опір ґрунту у 5...10 разів.

Врахувати усі фактори щодо особливостей ґрунту неможливо. Тому зведений опір ґрунту контролюють, для чого його вимірюють 2 рази на рік, влітку та взимку.

Для прикладу наведені експериментальні дані для опору заземлення стрижневого заземлювача діаметром 15,9 мм, довжиною 1,5 м для різних ґрунтів:

Таблиця 2 Опір заземлення стрижневого заземлювач

Тип ґрунту	Опір заземлення R, Ом		
	середній	мінімальний	максимальний
Зола, шлак, соляні відходи	14	3,5	41
Глина, суглинок, сланець	24	2	98
Те ж саме, з домішкою піску	93	6	800
Гравій, пісок, каміння з невеликою кількістю глини або суглинка	554	35	2700

У разі підвищених вимог до заземлення використовують багатократне заземлення, створене з ряду одинарних симетрично розташованих заземлювачів, з'єднаних між собою. Магістралі заземлення слід прокладати на глибині не менш як 1,5 метри.

1.3 Особливості та вимоги до засобів фільтрування інформаційних сигналів

Фільтрація є одним з методів локалізації небезпечних сигналів, що циркулюють в технічних засобах та системах обробки інформації. Для фільтрації сигналів в мережах живлення ТЗП використовують розділяючі трансформатори і протизавадні фільтри.

Розділяючі трансформатори забезпечують розв'язування первинного та вторинного ланцюгів за сигналами наведень. До їх завдань відносяться:

- розділення за ланцюгами живлення джерел та рецепторів наведень;
- усунення асиметричних наведень;
- послаблення симетричних наведень в ланцюгу вторинних кіл, що виникають за рахунок асиметричних наведень в ланцюгах первинних кіл.

Засоби розв'язування та екранування в таких трансформаторах забезпечують максимальне значення опору між обмотками (приблизно 10000 МОм) при малому опорі між вторинною обмоткою та «землею», за рахунок великої ємності цього ланцюга.

Розділяючий трансформатор зі спеціальними засобами екранування і розв'язування забезпечує послаблення інформаційного сигналу наведень на навантаженні на 126 дБ при ємності між обмотками 0,005 пФ і на 140 дБ при ємності між обмотками 0,001 пФ.

Рівень симетричних наведень на виході трансформатора за рахунок асиметричних наведень на вході може бути послабленим на 40 дБ за рахунок спеціальних методів екранування.

Протизавадні фільтри розподілені на ФНЧ і ФВЧ, смугові і загороджувальні, тощо. Головне їх призначення – пропускати без послаблення сигнали з робочого діапазону частот при послабленні усіх складових за межами цього діапазону.

Розрізняють електричні фільтри за двома групами: для придушення міжсистемних завад (міжсистемні фільтри) та завад в мережах живлення в межах однієї системи (внутрішньо системні фільтри) [20].

До перших відносять фільтри, які забезпечують:

- вибірковість супергетеродинних приймачів за сусіднім каналом (налаштований фільтр разом з підсилювачем проміжної частоти);
- придушення дзеркального каналу та поза смугових завад у преселекторах супергетеродинних приймачів;
- придушення шкідливих частот (режекторні фільтри);
- захист входу радіоприймача від завад на частотах поза діапазону частот приймання приймача (фільтри верхніх або нижніх частот);
- придушення побічних частот радіопередавачів (фільтри з великою прохідною потужністю).

Зазвичай міжсистемні фільтри характеризуються однаковим вхідним та вихідним опором 50 або 72 Ом. Для фільтрів звукових частот опір фільтра становить 600 Ом, а для фільтрів ДМХ та ультрависоких частот – 300 Ом.

Внутрішньосистемні фільтри використовують для:

- придушення завад, які поширюються в мережах живлення загального користування;
- зниження рівня зв'язку на ВЧ між різними приладами;
- придушення широкосмугових завад, створюваних електроприладами, електродвигунами, імпульсними джерелами живлення, люмінесцентними лампами, пристроями запалювання авто двигунів, тощо;
- захист різних приладів, чутливих до завад (датчиків, сенсорів, лічильної техніки, відеотехніки, тощо).

Такі фільтри мають різний опір. Наприклад для систем електроживлення типовим є вихідний опір мережі 1 Ом. Крім того, опір джерела та навантаження залежить від частоти. При випробуваннях фільтра здійснюється його під'єднання до джерела випробовуючого сигналу та навантаження, зазвичай, з опором 50 Ом. При цьому визначаються характеристики фільтра, а головне, загасання сигналів в діапазоні частот. При підключенні до фільтра реальних джерела струму (опір якого для силових ліній 220 В складає 1...0,5 Ом) та навантаження (вхідний опір якого визначається його струмом споживання), умови роботи фільтра змінюються і характеристика загасання сигналів в діапазоні частот спотворюється.

Слід зазначити, що згідно "Тимчасових рекомендацій з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок ТР ЕОТ - 95" для забезпечення з технічного захисту інформації в АС і ЗОТ від витоку каналами ПЕМВН рекомендовано застосовувати завадозаглушувальні фільтри для технічного захисту інформації, що забезпечують захист від витоку інформації по електромережі.

Електромережні фільтри для екранованих центрів обробки даних (ЦОД), екранованих кімнат, серверних шаф, панелі електромережних фільтрів для вводу в екрановані приміщення. Фільтри 3А, 10А, 25А, 75А, 100А, 210А. Трифазні, однофазні. Телефонні фільтри на слабкий струм. Наприклад Фільтри торгової марки ЕМСБІ типу ФЗП110-2 ТУ У 31.1-31731859-001-2003 (рис. 2).



Рис. 2 – Фільтри торгової марки ЕМСБІ ФЗП-110-2

Фільтри торгової марки ЕМСБІ типу ФЗП110-2 ТУ У 31.1-31731859-001-2003 захищають інформацію в дуже широкому діапазоні частот – від звукових (10 кГц) до надвисоких (18 ГГц) від витоку колами електроживлення основних и допоміжних технічних засобів цифрової та аналогової обробки інформації (комп'ютери, модеми, принтери тощо).

Одночасно фільтри ФЗП110-2 ефективно захищають згадані засоби обробки інформації від «брудної» мережі електроживлення і від пачок високовольтних імпульсних перешкод наносекундного діапазону, які можуть поступати з мережі електроживлення з-за грозової діяльності, внаслідок аварій в мережі електроживлення або шляхом навмисного силового впливу (електромагнітний тероризм).

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Які заходи відносяться до активних методів захисту інформації.
2. Які заходи відносяться до пасивних методів захисту інформації.
3. У чому полягає поняття ослаблення інформаційних сигналів.
4. У чому полягає поняття ослаблення наведень побічних електромагнітних випромінювань ТЗП.
5. У чому полягає поняття послаблення просочування інформаційних сигналів ТЗП.
6. У чому полягає поняття створення маскуючих електромагнітних завад.
7. У чому полягає поняття послаблення побічних електромагнітних завад.
8. У чому полягає поняття творення просторових маскуючих електромагнітних завад.
9. Які існують основні вимоги до систем заземлення.
10. У чому полягає особливості фільтрування інформаційних сигналів.
11. Які існують вимоги до засобів фільтрування інформаційних сигналів.

Тема № 9. Практичне заняття № 5. Методи захисту акустично-оптичного каналу.

Навчальна мета заняття: ознайомитися з основними методами і засобами виявлення та пригнічування диктофонів

Кількість годин – 2 год.

Навчальні питання:

1. Принцип дії лазерної акустичної локаційної системи і методи захисту акустично-оптичного каналу.
2. Методи і засоби виявлення та пригнічування диктофонів диктофонів.

Література:

Основна

1. Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
2. Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
3. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.
5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
6. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

7. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
8. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
9. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. галузі знань 1601, 1701 «Інформаційна безпека» за спец. 7.17010201, 8.17010201 – Системи технічного захисту інформації, автоматизації її обробки / Голев Д. В., Кононович В. Г., Хомич С. В. ; за ред. чл.-кор. МАЗ В. Г. Кононовича ; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О. С. Попова, 2013. 217 с.
10. Носов В. В., Манжай А. В. Організація та забезпечення безпеки інформації : навчальний посібник. Харків : ХНУВС, 2007. 216 с.
11. Про інформацію : Закон України від 02.10.1992 № 2657-ХІІ // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>.
12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>.
13. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF>.
14. Про затвердження Правил забезпечення захисту інформації в

інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>.

15. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.

16. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.

Інформаційні ресурси в Інтернеті

17. Фонд нормативних документів у сфері технічного та криптографічного захисту інформації // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=89734.

18. Каталог обладнання для виявлення каналів витоку інформації // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/>.

19. Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/texnika-dlya-fizichnogo-oglyadu/>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

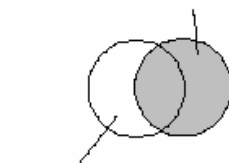
План проведення заняття:

I. Порядок проведення вступу до заняття.

1. Принцип дії ЛАЛС (лазерної акустичної локаційної системи) і методи захисту акустично-оптичного каналу

При відбитті лазерного променя від поверхні скла під впливом акустичного сигналу відбувається модуляція кута відбиття падаючого променя лазера та фази оптичного сигналу. У варіанті кутової модуляції променя кут відбиття змінюється згідно з амплітудою акустичної хвилі. Відбитий промінь приймається оптичним приймачем, світлочутливий елемент якого юстирується таким чином, щоб пляма відбитого променя при відсутності коливань скла освітлювала половину екрана фотоприймача. У цьому випадку зміни напрямку відбитого променя при коливаннях скла викликають відповідні зміни площі плями світла на світлочутливому елементі оптичного приймача, що призводить до амплітудної модуляції струму фотоприймача. На рис. 1 зображено взаємне положення світлочутливого елементу та відбитого променя при правильному налаштуванні.

зайчик лазерного променя



фотоприймач

Рис. 1

Другий варіант побудови ЛАЛС (лазерної акустичної локаційної системи) передбачає реалізацію в оптичному приймачі фазової демодуляції порівнянням фаз випромінюваного та відбитого променів. З цією метою вихідний промінь за допомогою напівпрозорого дзеркала розщеплюється на два променя. Один з них опромінює скло, другий прямує до приймача як опорного сигналу. В точці приймання внаслідок інтерференції опорного та відбитого променів на поверхні світлочутливого елементу виникає інтерференційна картина, інтенсивність освітлення якої відповідає різниці фаз променів (рис 2).

Цей варіант забезпечує більш високу чутливість системи, але складніший в реалізації.

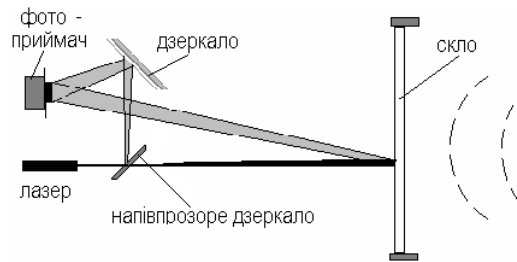


Рис. 2

До недоліків ЛАЛС можна віднести:

- складність установки (настроювання) системи при використанні ІК діапазону (промінь не видний);
- вартість самої системи і величина витрат на ефективний захист від ЛАЛС не на користь ЛАЛС.

Отже, системи лазерного прослуховування, незважаючи на їх високі потенційні можливості, мають обмежене реальне застосування, особливо розвідкою комерційних структур.

ЛАЛС найбільш ефективні для прослуховування розмов у приміщеннях невеликого розміру і в салонах автомашин. Дальність дії ЛАЛС без спеціальної обробки скла – 100-300 метрів. При покритті скла спеціальним матеріалом – до 500 метрів, а при встановленні на вікнах спеціальних спрямованих відбивачів (трипель-призм) – до 1000 м.

Модель розвідувального контакту при зніманні інформації з використанням ЛАЛС подана на рисунку 3..

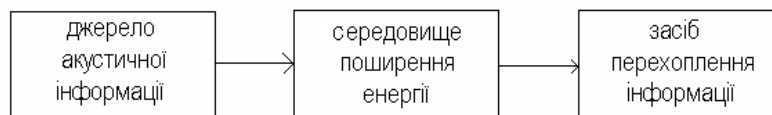


Рис. 3.

Із рисунка видно, що запобігти несанкціонованому доступу до конфіденційної інформації можна, впливаючи на джерело, на середовище поширення енергії та на засіб розвідки.

З урахуванням виділених областей розвідувального контакту способи захисту від прослуховування з використанням ЛАЛС можна розділити на три групи:

- організаційні;
- організаційно-технічні;
- технічні.

2. Методи і засоби виявлення та пригнічування диктофонів диктофонів.

Щоб запобігти несанкціонованому запису на диктофон, необхідно:

- виявити диктофон;
- порушити нормальну роботу диктофона.

Для виявлення диктофонів, що працюють в режимі запису, застосовуються так звані *детектори диктофонів*. Принцип їх дії оснований на виявленні слабкого магнітного поля, створюваного генератором підмагнічування або двигуном диктофону, що працює в режимі запису. Детектори диктофонів випускаються в переносному та стаціонарному варіантах. До переносних належать детектори «Сова», RM-100, TRD-800, а до стаціонарних – PTRD-14, PTRD-16 та ін.

У переносному варіанті блок аналізу детектора розміщується в кишені оператора, пошукова антена – в рукаві (звичайно прикріплюється на передпліччі), а давач сигналізації вібраторного типу – на поясі або в кишені. При виявленні випромінювань (перевищенні магнітного поля встановленого оператором порогового значення) включеного на запис диктофону прихований сигналізатор-вібратор починає вібрувати, сигналізуючи операторові про можливий запис розмови.

Для захисту виділених приміщень в основному використовуються детектори диктофонів, виконані в стаціонарних варіантах. На відміну від переносних детекторів, що мають один подавач сигналів, стаціонарні детектори диктофонів обладнані декількома подавачами, що дозволяє суттєво підвищити ймовірність виявлення диктофонів.

Стаціонарний варіант припускає встановлення антени в стіл для переговорів та в крісла (підлокітники). Блок аналізу та індикатор наявності диктофонів розміщується в столі керівника або у чергового (в цьому випадку створюється додатковий канал керування). При наявності у того, хто веде бесіду, диктофону в одязі або в речах (папка, портфель і т. ін.) у керівника приховано, спрацьовуватиме індикація цього факту.

Для виявлення непрацюючих диктофонів застосовуються нелінійні локатори. До типових представників пристроїв цього класу належить, наприклад, нелінійний локатор «Циклон-Рамка». Зона контролю локатора становить: по висоті – 2,2 м, по довжині – 1,5 м, по ширині – 1,5 м.

Порушити нормальну роботу диктофона можливо:

- методом енергетичного приховування, застосовуючи засоби електромагнітного та ультразвукового пригнічення;
- засобами нуліфікації (несанкціоноване пошкодження або стирання запису).

Поряд із засобами виявлення портативних диктофонів на практиці використовуються і *засоби електромагнітного та ультразвукового пригнічення*. З цією метою використовуються пристрої типу електромагнітного пригнічування і пристрої ультразвукового пригнічування типу «Завіса».

Принцип дії пристроїв електромагнітного пригнічування («Рубіж», «Шумотрон», «Буран», «УПД») ґрунтується на генерації в дециметровому діапазоні частот (звичайно в межах 900 МГц) потужних шумових сигналів. В основному для пригнічування використовуються імпульсні сигнали. Випромінювані спрямованими антенами завадові сигнали, впливаючи на елементи електронної схеми диктофона (зокрема, підсилювач низької частоти і підсилювач запису), викликають в них наведення шумових сигналів. Зона приглушення диктофонів залежить від потужності випромінювання, його вигляду, а також від типу використовуваної антени. Звичайно зона приглушення являє собою сектор із кутом від 30 до 80 градусів та радіусом до 1,5 м (для диктофонів в екранованому корпусі).

Пристрої приглушення диктофонів використовують як неперервні, так і імпульсні сигнали.

Дальність пригнічування диктофонів в неекранованому корпусі становить декілька метрів.

Системи *ультразвукового пригнічування* (наприклад, типу «Завіса») випромінюють потужні нечутні людським вухом ультразвукові коливання (звичайно частота

випромінювання близько 20 кГц), які впливають безпосередньо на мікрофони диктофонів або акустичних закладок, що є їх перевагою. Даний ультразвуковий вплив призводить до перевантаження підсилювача звукової частоти (ПЗЧ) диктофону або акустичної закладки (підсилювач починає працювати в нелінійному режимі) і тим самим – до значних спотворень записуваних (передаваних) сигналів. У випадку наявності в диктофоні системи автоматичного регулювання підсилення (АРП) пригнічування буде ефективнішим, бо система АРП під впливом ультразвукового сигналу більшої амплітуди різко зменшить коефіцієнт підсилення УЗЧ, що призведе до ще більшого погіршення якості запису. У випадку одночасного випромінювання двох ультразвукових коливань із рознесенням частот у декілька кГц (наприклад, 20 кГц і 21 кГц) ефект пригнічування підвищується. Проте, системи ультразвукового пригнічування мають і один істотний недолік: ефективність їх різко зменшується, якщо мікрофон диктофону або закладки прикрити фільтром із спеціального матеріалу, або у підсилювачі низької частоти встановити фільтр низьких частот із граничною частотою 3,4...4 кГц.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Що відбувається при відбитті лазерного променя від поверхні скла під впливом акустичного сигналу?
2. Існує два варіанти побудови ЛАЛС. Який варіант забезпечує більш високу чутливість системи, але складніший в реалізації?
3. Назвіть недоліки ЛАЛС?
4. На які групи з урахуванням виділених областей розвідувального контакту діляться способи захисту від прослуховування з використанням ЛАЛС?

Тема № 10, 11. Практичне заняття № 6 на тему : Методи та засоби пошуку електронних пристроїв перехоплення інформації.

Навчальна мета заняття: вивчити основні методи та засоби пошуку електронних пристроїв перехоплення інформації.

Кількість годин – 6 год.

Навчальні питання:

1. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації.
2. Методи пошуку електронних пристроїв з використанням виявлювачів порожнеч, металопрошукачів і рентгенівських апаратів.
3. Методи пошуку з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерцепторів.

Література:

Основна

1. Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
2. Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
3. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.

5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.

Додаткова

6. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СТУК, 2018. 54 с.

7. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.

Нормативно-правові акти

8. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.

9. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.

10. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-2005: чинний від 2005-11-08. К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. 17 с. URL: <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350>.

Інформаційні ресурси в Інтернеті

11. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.

12. Каталог обладнання для виявлення каналів витoku інформації // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/>.

13. Каталог обладнання для протидії засобам знімання інформації// Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/>.

14. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/skanuyuchi-prijmachi/>.

15. Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/texnika-dlya-fizichnogo-oglyadu/>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Існує два основні способи виявлення фізичних об'єктів, що відрізняються від оточуючого середовища значенням своєї магнітної і діелектричної проникливості.

До таких методів відносяться:

- пасивне виявлення об'єктів (наприклад, шляхом контролю радіоефіру, візуального огляду й ін.);
- активне виявлення (наприклад, за допомогою локації).

II. Основна частина

1. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації

В основі виявлення об'єктів за допомогою нелінійних локаторів⁴ мають місце такі моменти:

1. перевипромінювання (віддзеркалення) електромагнітного поля межею розділу двох різних фізичних середовищ та струмопровідними елементами конструкції, які відіграють роль випадкових антен – перевипромінювачів (доріжки плати радіопристрою, арматура залізобетонних конструкцій і ін.);

2. викривлення форми токів, що наводяться електромагнітним полем у випадкових антенах p - n переходами і «нелінійними» контактами. При цьому сигнал, який випромінює випадкова антена має збільшену кількість кратних гармонік.

Основну увагу при виборі моделі слід приділяти таким *параметрам нелінійного локатора*:

- потужність випромінювання;
- режим випромінювання;
- частота випромінювання;
- наявність сертифіката на застосування за заявленим призначенням.

Потужність випромінювання має два аспекти:

- підвищує ТТХ локатора;
- є фактором небезпеки для здоров'я оператора.

Частота випромінювання поряд з потужністю випромінювання є основоположним для ТТХ нелінійного локатора. Дана обставина пов'язана з двома факторами:

- частотної залежності загасання величини потужності в середовищі поширення як зондуєчого сигналу, так і сигналів на вищих гармоніках (спостерігається експонентне зростання загасання в залежності від частоти);
- в силу фізичної природи процесу перетворення частоти напівпровідниковими приладами рівень потужності перетвореного сигналу тим вище, чим нижче частота нелінійного локатора.

Необхідність наявності сертифікаційних документів на нелінійні локатори обумовлена наступними факторами:

- за законодавством при запуску в експлуатацію передавального пристрою з такими величинами потужності обов'язково потрібен дозвіл на виділення робочої частоти передавача;
- проводиться повний цикл вимірювань на допустимий рівень випромінювання для безпеки оточуючих та обслуговуючого персоналу.

⁴ Розробки нелінійних локаторів почалися в США, Великобританії та СРСР в середині 70-х років. Першим пристроєм, що надійшов на озброєння ЦРУ, був локатор «Зірег Зсоі», серійний випуск якого почався з 1980 р. У 1981 р. з'явився британський локатор «Вгоот», який дещо поступався американському аналогу. Вітчизняний нелінійний локатор «Орхідея» з'явився в 1982 р. На відміну від зарубіжних аналогів вітчизняні розробки йшли дещо в іншому напрямку, в результаті чого «Орхідея» різко перевершувала закордонні аналоги за своїми тактико-технічними характеристиками (ТТХ), а габаритні показники були в 2 рази менші.

2. Методи пошуку електронних пристроїв з використанням виявлювачів порожнеч, металопукачів і рентгенівських апаратів

Робота виявлювачів порожнеч заснована на принципі виявлення ділянок середовища, діелектрична проникність яких істотно відрізняється від середнього значення.

Існує безліч класифікацій металопукачів.

1. Металопукачі за принципом передача-прийм.
2. Металопукачі на биття.
3. Металопукачі за принципом електронного частотоміра.
4. Імпульсні металопукачі.
5. Магнітометри.
6. Радіолокатори (георадари).

Одними з основних засобів *радіаційної інтроскопії* є системи сканування, в основі яких закладено принцип цифрової радіографії, що полягає в прямому перетворенні розподілу радіаційного поля в цифровий вигляд за допомогою детекторів іонізуючого випромінювання.

Відомі два основні методи, що реалізують процедуру отримання зображення внутрішньої структури об'єкта контролю шляхом його послідовного сканування «порменем, що біжить» або «віялових» променів та реєстрації попереднього випромінювання високоефективним протяжним детектором. Протяжний детектор може бути монолітним кристалом, газорозрядної пропорційної камерою, багатоеlementної напівпровідникової або комбінованою системою.

Ідея використання техніки «промінь, що біжить» для формування радіаційного зображення здійснюється шляхом формування та направлення на об'єкт контролю пучка рентгенівського випромінювання механічним коліматором, що представляє собою сукупність вузьких щілин, одна з яких нерухома щодо випромінювача, а інші розташовані на диску, що обертається.

При реалізації режиму «віялового» променя коліміруються випромінювач і детектор, який представляє собою протяжну матрицю, що складається з окремих детектуючих модулів: цьому випадку як детектуючих елементів застосовують пристрої типу сцинтилятор-фотоприймач, напівпровідниковий детектор або лінійку газонаповнених пропорційних детекторів. Чутливість систем, що сканують, забезпечує формування зображення в телевізійному стандарті.

Чутливість апаратури сканування за рахунок відносно малого вкладу розсіяного випромінювання при формуванні радіаційного зображення контрольованого об'єкту і практично повного поглинання енергії випромінювання детектуючої системою значно перевершує аналогічні характеристики традиційних засобів радіаційного контролю.

Системи контролю, які працюють за принципом сканування, відрізняються розмірами елементарної детектуючої системи і, відповідно, розмірами блоку детектування, величиною енергії зонduючого випромінювання, а також особливостями конструкції, зумовленими способом формування зображення.

У багатоеlementних детекторах як окремі елементи застосовуються:

- детектори на основі NaI (Tl) з фотоелектронними помножувачі (ФЕП);
- пластмасові сцинтилятори з ФЕУ;
- сцинтиляційні кристали з кремнієвими фотодіодами;
- напівпровідникові детектори (НПД);
- газонаповнені пропорційні детектори;

Головною вимогою висувається умова максимальної ефективності.

2. Методи пошуку з використанням індикаторів електромагнітного поля, радіочастотомірів та інтерсенкторів

Інформативні побічні електромагнітні випромінювання

Інформативними ПЕМВН називаються сигнали, що являють собою ВЧ – носійну, модульовану інформацією, оброблювану засобами обчислювальної техніки (ЗОТ), наприклад зображенням, виведеним на монітор, даними, оброблюваними на пристроях введення-виведення і т.д.

Методи пошуку сигналів ПЕМВН

На сьогоднішній день широко використовуються чотири основних методи пошуку сигналів ПЕМВН, а також їхні комбінації.

Перший метод – метод порівняння панорам полягає в тому, що при включенні тестового режиму в радіоефірі з'являються нові сигнали (сигнали ПЕМВН), які легко знайти шляхом порівняння двох панорам: із включеним і виключеним тестовим сигналом. Цей універсальний метод дозволяє знаходити як сигнали ПЕМВН, так і сигнали, промодульовані тестовим сигналом.

Другий метод – метод аудіовізуального пошуку сигналів ПЕМВН. Його суть полягає в тому, що оператор переглядає спектри сигналів, отримані при включеному і виключеному тестовому сигналі. Підозрілі сигнали досліджуються за видом осцилограм, спектрограм і немодульованого аудіосигналу.

Третій метод – пошук сигналу по гармоніках – полягає в прогнозуванні частоти гармоніки, абсолютно точному настроюванні на неї і наступному підборі оптимальної смуги пропускання, виходячи з конкретних умов приймання.

У даному методі пошуку ефективно використовується властивість пікового детектора: амплітуда сигналу не змінюється при зміні смуги пропускання, а рівень шуму зменшується пропорційно кореневі квадратному зі смуги пропускання.

Прилади для вимірювання ПЕМВН

У даний час для проведення досліджень ПЕМВН допустимо використовувати лише такий комплекс апаратури, основу якого складає вимірювальний приймач або аналізатор спектра з набором відповідних вимірювальних антен.

Селективні мікровольтметри цілком підходять для високоточних вимірювань напруженості слабких електричних і магнітних полів. У той же час вони не дають можливості спостерігати панораму сигналів і не витримують порівняння із сучасними вимірювальними приймачами й аналізаторами спектра по продуктивності та ергономічними показниками.

Вимірювальні приймачі найбільшою мірою відповідають вимогам, що висувуються до апаратури для досліджень ПЕМВН. Вони забезпечують високу точність вимірювань при порівняно невеликих трудовитратах.

Значна частина вимірювальних приймачів дає змогу бачити панораму досліджуваного діапазону частот, аналізувати сигнали при одночасному спостереженні результатів їхнього детектування різними типами детекторів. Однак ціна вимірювальних приймачів досить висока.

Аналізатори спектра за своїми функціональними можливостями цілком зіставлені з вимірювальними приймачами. На стадії виявлення ПЕМВН вони іноді навіть зручніші приймачів.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
2. Розкрити зміст організаційних методів захисту інформації від витоку технічними каналами.
3. Розкрити зміст технічних методів захисту інформації від витоку технічними каналами.
4. Охарактеризуйте пасивні методи та засоби захисту інформації.

5. Охарактеризуйте активні методи та засоби захисту інформації.
6. Перелічити активні методи і засоби захисту інформації, що циркулює в ТЗПІ.

Тема № 12. Практичне заняття № 7 на тему: Засоби пошуку електронних пристроїв перехоплення інформації.

Навчальна мета заняття: вивчити основні тактико-технічні характеристики засобів пошуку електронних пристроїв перехоплення інформації.

Кількість годин – 4 год.

Навчальні питання:

1. Класифікація засобів радіовиявлення.
1. Інтерсептори.
2. Вимірювальні засоби радіомоніторингу.
3. Радіочастотоміри.
4. Селективні мікровольтметри і нановольтметри.
5. Панорамні засоби радіомоніторингу.

Література:

Основна

1. Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
2. Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
3. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.
5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.

Додаткова

6. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СКУК, 2018. 54 с.
7. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.

Нормативно-правові акти

8. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF>.
9. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.
10. Порядок проведення робіт із створення комплексної системи захисту

інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-2005: чинний від 2005-11-08. К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. 17 с. URL: <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350>.

Інформаційні ресурси в Інтернеті

11. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.

12. Каталог обладнання для виявлення каналів витоку інформації // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/>.

13. Каталог обладнання для протидії засобам знімання інформації// Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/>.

14. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/skanuyuchi-prijmachi/>.

15. Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/texnika-dlya-fizichnogo-oglyadu/>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

I. Порядок проведення вступу до заняття.

Сьогодні питання класифікації різних засобів радіовиявлення в Україні регламентуються нормативним документом системи технічного захисту інформації НД ТЗІ 1.5-001-2000 «Радіовиявлювачі. Класифікація. Загальні технічні вимоги».

II. Основна частина

1. Класифікація засобів радіовиявлення

Відповідно до цього документа *радіовиявлювачі* – це технічні засоби виявлення, ідентифікації і локалізації джерел електромагнітного випромінювання в області технічного захисту інформації. Залежно від призначення і сукупності задач, розв'язуваних з їхньою допомогою, радіовиявлювачі поділяються на чотири групи А, Б, В і Г з явно вираженим зростанням функційних можливостей приладів у кожній групі. Кожна з груп має свою назву:

А – індикаторні. Технічні засоби цієї групи здійснюють виявлення й індикацію сигналів, амплітуда яких перевищує пороговий рівень, заданий оператором, і може використовуватися для локалізації джерела сигналу, що має найбільший рівень у робочому діапазоні частот пристрою.

Б – панорамні. До них належать селективні по частоті скануючі радіоприймальні пристрої для пошуку, ідентифікації і локалізації джерела випромінювання і радіомоніторингу з індикацією розподілу сигналів у робочому діапазоні частот. Мають здатність налаштування на задані частоти або обраний відгук, а також вхід для підключення зовнішніх антен.

В – вимірвальні. Селективні по частоті радіоприймальні пристрої для пошуку й ідентифікації випромінювань за рахунок точного вимірювання енергетичних, частотних і часових характеристик сигналів. Мають здатність точного вимірювання частоти налаштування і рівня сигналів, керовану смугу пропускання.

Г – аналізуючі. Селективні по частоті радіоприймальні пристрої для пошуку, ідентифікації і контролю випромінювань за рахунок якісного і кількісного аналізу

електромагнітної обстановки, частотно-часової структури і спектрального складу сигналів. Мають здатність вимірювання частоти, рівня сигналів і характеристик спектрів.

Слід зазначити, що деякі реальні пошукові прилади важко однозначно класифікувати відповідно до НД ТЗІ 1.5-001-2000 через різноманіття виконуваних ними функцій.

Індикаторні засоби радіомоніторингу

Індикаторні засоби радіомоніторингу являють собою радіовиявлювачі індикаторного типу, що дозволяють фіксувати факт перевищення рівня електромагнітного поля від певного заданого значення. До них належать *індикатори електромагнітного поля, інтерсептори й універсальні (багатофункційні) прилади* виявлення закладних пристроїв.

2. Інтерсептори

Подальшою еволюцією індикаторів поля стали спеціальні широкосмугові радіоприймальні пристрої – *інтерсептори*, що автоматично настроюються на частоту найбільш потужного в даній точці простору радіосигналу і здійснюють його детектування (амплітудне або частотне). Система перетворення частоти інтерсепторів дозволяє «переглядати» весь діапазон за кілька секунд. Деякі типи інтерсепторів визначають належність виявленого сигналу одному з 6–8 частотних піддіапазонів, на які розподілений весь частотний діапазон приладу.

3. Вимірювальні засоби радіомоніторингу

До вимірювальних засобів радіомоніторингу належать селективні по частоті радіоприймальні пристрої для пошуку та ідентифікації випромінювань за рахунок точного вимірювання енергетичних, частотних і часових характеристик сигналів. Ця група технічних засобів містить у собі радіочастотоміри, селективні мікровольтметри.

3. Радіочастотоміри

Радіочастотоміри, як і інтерсептори, автоматично настроюються на частоту сигналу з максимальним рівнем і вимірюють частоти цього сигналу. Весь процес вимірювання реалізується з використанням алгоритмів цифрової обробки сигналу (оцифрування, цифрова фільтрація, перевірка на стабільність і когерентність, вимірювання частоти) і реалізується на базі мікроконтролера. Крім частоти сигналу багато радіочастотомірів показують відносний рівень сигналу. Результати звичайно відображаються на цифровому рідкокристалічному індикаторі.

4. Селективні мікровольтметри і нановольтметри

Селективні мікровольтметри є спеціальними широкодіапазонними радіоприймачами з можливістю зміни типу детектора і ширини смуги пропускання. Перебудова по частоті, як правило, здійснюється вручну. Основне призначення цих приладів – точне вимірювання рівня напруженості електромагнітного поля (у дБмкВ). Ці прилади використовуються зараз під час проведення, наприклад, атестації засобів електронної техніки від витоку інформації по каналах побічних електромагнітних випромінювань, завдяки своїй відносно низькій вартості, високій точності вимірювань і наявності сертифікації.

5. Панорамні засоби радіомоніторингу

До *панорамних засобів радіомоніторингу* належать селективні по частоті скануючі радіоприймальні пристрої для пошуку, ідентифікації і локалізації джерела випромінювання і радіомоніторингу з індикацією розподілу сигналів у робочому діапазоні частот.

Аналізуючі засоби радіомоніторингу – це селективні по частоті радіоприймальні пристрої для пошуку, ідентифікації і контролю випромінювань за рахунок якісного і кількісного аналізу електромагнітної обстановки, частотно-часової структури і спектрального складу сигналів. Мають можливість вимірювання частоти, рівня сигналів і характеристик спектрів.

До цієї групи пристроїв можна віднести автоматизовані спеціалізовані комплекси для пошуку ЗП й аналізатори спектра.

За принципом побудови спеціалізовані комплекси даного класу можна умовно поділити на 2 групи:

1) комплекси, спеціально розроблені і конструктивно виконані у вигляді єдиного пристрою;

2) комплекси, створені на базі серійного скануючого приймача (або аналізатора спектра) і персонального комп'ютера.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Охарактеризувати методи і засоби пошуку електронних закладних засобів.
2. Охарактеризувати методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
3. Охарактеризувати методи пошуку закладок з використанням нелінійних локаторів, виявителі порожнеч (порожнеч), металошукачів і рентгенівських апаратів .
4. Перелічити засоби пошуку пристроїв перехоплення інформації. Скануючі приймачі й аналізатори спектру.
5. Засоби пошуку пристроїв перехоплення інформації.