МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA – технологій факультету № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни "Методи та засоби технічного захисту інформації"
обов'язкових компонент
освітньої програми першого (бакалаврського) 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)

№ з/п	Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
		Всього	з них:					
			лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 4								
1.	Тема № 1. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.	**14**	**4**		**2**	**4**	**4**	
2.	Тема № 2. Цілі, задачі та організація технічної розвідки.	**18**	**4**				**14**	
3.	Тема № 3. Об'єкти інформаційної діяльності: визначення, види та технічні засоби.	**14**	**4**		**2**		**8**	
4.	Тема № 4. Технічні канали витоку інформації: визначення та класифікації.	**16**	**4**		**2**		**10**	
5.	Тема № 5. Методи та засоби несанкціонованого отримання інформації по технічних каналам.	**28**	**4**		**2**	**8**	**14**	
Всього за семестр № 4:		**90**	**20**	**–**	**8**	**12**	**50**	**Залік**
Семестр № 5								
6.	Тема № 6. Акустичні технічні канали витоку інформації.	**19**	**4**			**4**	**11**	
7.	Тема № 7. Телекомунікаційні технічні канали витоку інформації.	**10**	**4**				**6**	
8.	Тема № 8. Візуально-оптичні технічні канали витоку інформації.	**12**	**4**		**4**		**4**	
9.	Тема № 9. Матеріально-речовинні технічні канали витоку інформації.	**6**	**2**				**4**	
10.	Тема № 10. Пошукова техніка для виявлення засобів технічних розвідок.	**28**	**6**		**4**	**8**	**10**	
Всього за семестр № 5:		**75**	**20**	**–**	**8**	**12**	**35**	**Залік**
Семестр № 6								
11.	Тема № 11. Засоби технічного захисту інформації.	**19**	**4**		**4**		**11**	
12.	Тема № 12. Методи технічного захисту інформації.	**18**	**4**		**4**		**10**	
13.	Тема № 13. Оцінка ефективності захисту інформації від витоку технічними каналами витоку.	**10**	**4**				**6**	
14.	Тема № 14. Методики технічного	**14**	**4**			**6**	**4**	

	контрою ефективності заходів технічного захисту інформації від витоку електромагнітними полями.							
15.	Тема № 15. Методики оцінки ефективності захищеності інформації від витоку акустичними каналами.	**14**	**4**			**6**	**4**	
Всього за семестр № 6:		**75**	**20**	**–**	**8**	**12**	**35**	**Екзамен**
Загалом		**240**	**60**	**–**	**24**	**36**	**120**	

Розподіл часу навчальної дисципліни за темами
(заочна форма навчання)

№ з/п	**Номер та назва навчальної теми**	**Кількість годин, відведених на вивчення навчальної дисципліни**						**Вид контролю**
		Всього	**з них:**					
			Лекції	**Семінарські заняття**	**Практичні заняття**	**Лабораторні заняття**	**Самостійна робота**	
Семестр № 4								
1.	Тема № 1. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.	**16**					**16**	
2.	Тема № 2. Цілі, задачі та організація технічної розвідки.	**16**					**16**	
3.	Тема № 3. Об’єкти інформаційної діяльності: визначення, види та технічні засоби.	**16**					**16**	
4.	Тема № 4. Технічні канали витоку інформації: визначення та класифікації.	**26**	**2**		**2**	**2**	**20**	
5.	Тема № 5. Методи та засоби несанкціонованого отримання інформації по технічних каналах.	**16**					**16**	
Всього за семестр № 4:		**90**	**2**		**2**	**2**	**84**	**Залік**
Семестр № 5								
6.	Тема № 6. Акустичні технічні канали витоку інформації.	**19**	**4**		**2**		**13**	
7.	Тема № 7. Телекомунікаційні технічні канали витоку інформації.	**13**					**13**	
8.	Тема № 8. Візуально-оптичні технічні канали витоку інформації.	**13**					**13**	
9.	Тема № 9. Матеріально-речовинні технічні канали витоку інформації.	**13**					**13**	
10.	Тема № 10. Пошукова техніка для виявлення засобів технічних розвідок.	**17**				**4**	**13**	

Всього за семестр № 5:		**75**	**4**		**2**	**4**	**65**	**Залік**
Семестр № 6								
11.	Тема № 11. Засоби технічного захисту інформації.	**20**	**4**		**2**		**14**	
12.	Тема № 12. Методи технічного захисту інформації.	**16**	**2**				**14**	
13.	Тема № 13. Оцінка ефективності захисту інформації від витоку технічними каналами витоку.	**13**					**13**	
14.	Тема № 14. Методики технічного контрою ефективності заходів технічного захисту інформації від витоку електромагнітними полями.	**13**					**13**	
15.	Тема № 15. Методики оцінки ефективності захищеності інформації від витоку акустичними каналами.	**13**					**13**	
Всього за семестр № 6:		**75**			**2**		**67**	**Екзамен**
Загалом		**240**	**8**		**6**	**10**	**216**	

2. Методичні вказівки до практичних занять:

Тема № 1,3,4,5

Практичне заняття № 1 на тему: Методи та засоби захисту інформації, яка обробляється ТЗПІ.

Навчальна мета заняття: проаналізувати основні складові структури захисту інформації.

Кількість годин: 8 год.

Навчальні питання:

1. Державна політика і система ТЗІ в Україні.
2. Структура системи захисту інформації.
3. Методи та засоби захисту інформації, яка обробляється ТЗПІ.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут

інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД "Гельветика", 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.

27. 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:

І. 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.

ІІ. Основна частина

1. 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, воєнній і інших сферах;

– недосконаліть 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 небездоганних 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.

2. Структура системи захисту інформації

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

– основ побудови системи захисту інформації;

– направлень 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, знижаючого 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.

ІІІ. 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 № 8.

Практичне заняття №2 «Методи захисту акустично-оптичного каналу»

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

Кількість годин – 4 год.

Навчальні питання:

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

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет "Одеська юридична академія" та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД "Гельветика", 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. 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:

І. Порядок проведення вступу до заняття.

1. ***Принцип дії 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. 13 зображено взаємне положення світлочутливого елементу та відбитого променя при правильному настроюванні.

Рис. 13

Другий варіант побудови ЛАЛС 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 14).

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

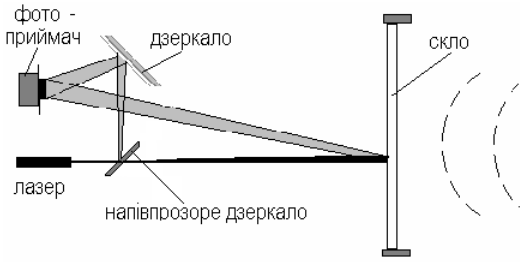

Рис. 14

До недоліків ЛАЛС можна віднести:

– складність установки (настроювання) системи при використанні ІК діапазо-ну (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 3.3.

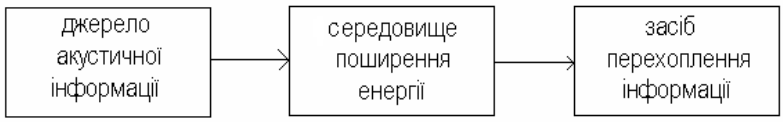

Рис. 3.3

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 заглушення 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, наприк-лад, 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 заглушення і пристрої

ультразвукового заглушення типу «Завіса».

Принцип дії пристроїв електромагнітного заглушення («Рубіж», «Шумотрон», «Буран», «УПД») ґрунтується на генерації в дециметровому діапазоні частот (звичайно в межах 900 МГц) потужних шумових сигналів. В основному для заглушення 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 заглушення диктофонів в неекранованому корпусі становить декілька метрів.

Системи *ультразвукового заглушення* (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) заглушення 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 заглушення підвищується. Проте, системи ультразвукового заглушення 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

Практичне заняття №3 «Засоби пошуку електронних пристроїв перехоплення інформації»

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

Кількість годин – 8 год.

Навчальні питання:

1. Класифікація засобів радіовиявлення.
2. Інтерсептори.
3. Вимірювальні засоби радіомоніторингу.

4. Радіочастотоміри.
5. Селективні мікровольтметри і нановольтметри.
6. Панорамні засоби радіомоніторингу.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ.

служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. 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:

І. 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».

ІІ. 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 скануючи радіоприймальні пристрої для пошуку, ідентифікації і локалізації джерела випромінювання і радіомоніторингу з індикацією розподілу сигналів у робочому діапазоні частот. Мають здатність настроювання на задані частоти або обраний відгук, а також вхід для підключення зовнішніх антен.

В – *вимірювальні*. 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 настроювання 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.

4. 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 відображуються на цифровому рідкокристалічному індикаторі.

5. 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.

6. 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 (пустот), металошукачів і рентгенівських апаратів .
4. Перелічити засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
5. Засоби пошуку пристроїв перехоплення інформації.

Тема № 11

Практичне заняття № 4 «Методи технічного захисту акустичної інформації»
Навчальна мета заняття: ознайомитися з основними методами технічного захисту інформації, яка обробляється ТЗПІ.

Кількість годин – 4 год.

Навчальні питання:

1. Загальна характеристика речового каналу витоку інформації.
2. Методи добування інформації про речові ознаки.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет "Одеська юридична академія" та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний

університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/texnika-dlya-fizichnogo-oglyadu/.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Особливість речового каналу витоку інформації викликана специфікою джерел і носіїв інформації у порівнянні з іншими каналами. Джерелами і носіями інформації у ньому є суб'єкти (люди) і матеріальні об'єкти (макротіла і мікрочастки).

ІІ. Основна частина

1. Загальна характеристика акустичного каналу витоку інформації

Основними джерелами інформації речового каналу витоку інформації є наступні:

– чернетки різноманітних документів й макети матеріалів, вузлів, блоків, пристроїв, що розроблюються у ході навчально-дослідницьких і дослідно-конструкторських робіт, що ведуться в організації;

– відходи діловодства та видавничої діяльності в організації, у тому числі використаний копіру вальний папір, забраковані аркуші при оформленні документів та їх розмноженні;

– відходи промислового виробництва досвідного і серійного випуску продукції, яка містить інформацію, що захищається у газоподібному, рідкому і твердому вигляді;

– дискети і жорсткі диски ПЕОМ, які містять інформацію, що захищається, які не читаються через фізичні дефекти та спотворення завантажувальних або інших секторів;

– бракована продукція та її елементи;

– радіоактивні матеріали.

Перенесення інформації у цьому каналі за межі контролюючої зони можливий наступними суб'єктами та об'єктами:

– людьми (співробітниками організації, відвідувачами, представниками вторсировини та ін.) і керуючими ними технічними засобами;

– повітряними масами атмосфери;

– рідким середовищем;

– випромінюваннями радіоактивних речовин.

Ці носії можуть переносити усі види інформації: с*емантичну* і *ознакову*, а також *демаскуючі речовини*.

Втрати носіїв з цінною інформацією можливі при відсутності в організації чіткої системи обліку її носіїв.

2. Методи добування інформації про речові ознаки

Речові ознаки продукції, що містять інформацію, яка захищається, визначаються у результаті хімічного, фізико-хімічного та фізичного аналізу.

Основу хімічного аналізу складають хімічні реакції досліджуваної речовини у розчині.

Фізико-хімічний аналіз передбачає вимір фізичних величин, зміну яких зумовлено хімічними реакціями.

Фізичний аналіз враховує зміну фізичних характеристик добутої проби, викликаних досліджуваною речовиною.

Принципи і методи визначення хімічного складу речовини розглядає аналітична хімія, яка включає *якісні і кількісні методи аналізу.*

Якісний аналіз представляє собою сукупність методів встановлення хімічного складу шляхом ідентифікації атомів, іонів, молекул, що входять в речовину, яка аналізується. Основними показниками якісного аналізу є *специфічність* і *чутливість*.

Специфічність характеризує можливість метода виявляти шукану речовину у присутності інших елементів. Чутливість визначається найменшою кількістю речовини, яка може бути виявлена аналізуючим методом.

Кількісний метод використовує сукупність методів визначення якісних співвідношень, в яких знаходяться елементи або окремі з'єднання в речовині, яка аналізується. Показники кількісного аналізу – *специфічність, чутливість* і *точність*.

Чутливість і точність вимірюються у процентах вмісту досліджуваної речовини в пробі. Чутливість сучасних методів досягає 10^{-12} -10^{-15} %. Точність, яка виражена значенням відносної помилки, складає 1-2%.

Основними методами аналітичної хімії є:

- методи поділу речовин;
- термічні методи;
- хімічні методи;
- електрохімічні методи;
- хроматографічні методи;
- спектральний аналіз;
- мас-спектографічні методи;
- радіоактивні методи;
- біологічні методи.

Термічні методи аналізу застосовують термічні ефекти, які являються причиною чи наслідком хімічних реакцій, і процеси виділення чи поглинання теплоти у результаті фізичних процесів.

В основі *хімічних методів* аналізу лежать хімічні реакції трьох типів: кислотно – основні, окислювально – відновлювальні і комплексоутворення.

Електрохімічні методи аналізу вивчають і використовують процеси, що протікають на поверхні електрода і в електродному просторі. Розрізняють прямі та непрямі електрохімічні методи. В прямих методах використовують зв'язок між силою струму (величиною потенціалу і т. ін.) і концентрацією визначуваної речовини, в зворотних залежність вимірюваного електричного параметра від об'єму титрату (розчина з певною концентрацією).

Хроматографія – фізико-хімічний метод поділу і аналізу сумішей, заснований на розподілі їх компонентів між рухомими і нерухомими речовинами. Рідина або газ (рухома речовина) протікають повз нерухому тверду речовину або плівки рідини, нанесеної на неї. Хроматографічні методи класифікуються за агрегатним станом суміші (газ, рідина), за механізмом поділу, за формою проведення хроматографічного процесу (колоночна, капілярна, площинна).

Спектральний аналіз проводиться з метою визначення складу речовини за її спектром. Розрізняють атомарний, молекулярний, спектральний, емісійний (за спектрами випромінювання) та абсорбційний (за спектрами поглинання) методи аналізу.

Мас-спектрометричні методи дозволяють дослідити речовини шляхом визначення мас і розподілу часток, що містяться в речовині. З цією метою виробляється іонізація атомів і молекул досліджуваної речовини і поділ утворюваних іонів у просторі або часі.

Методи аналізу речовин, засновані *на радіоактивності*, поділяють радіоактивний аналіз, радіо індикаторні, засновані на поглинанні і розсіюванні радіоактивних випромінювань, і радіометричні.

Біохімічні методи використовують біологічні компоненти (ферменти, антитіла та ін.).

Якщо кількість добутої речовини дуже мала (близько 100 мкг), то застосовують *мікрохімічний аналіз,* при меншій кількості (одиниці і долі мкг) – методи *ультрамікрохімічного аналізу.*

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Охарактеризуйте пасивні й активні методи і засоби захисту мовної інформації.

2. Звукоізоляція приміщень як метод блокування витоку акустичної інформації.
3. Охарактеризувати методи та засоби виявлення та подавлення диктофонів.
4. Охарактеризувати методи і засоби захисту телефонних ліній.
5. Охарактеризуйте основні методи добування інформації про речові ознаки.

Тема № 12

Практичне заняття № 5 «Засоби технічного захисту інформації»

Навчальна мета заняття: ознайомитися з засобами технічного захисту інформації, яка обробляється ТЗПІ.

Кількість годин – 4 год.

Навчальні питання:

1. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ.
2. Класифікація засобів захисту інформації від витоку технічними каналами.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.

15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. 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:

І. 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 неправомірне оволодіння зловмисником інформацією.

ІІ. 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 утворять 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 і атестація об’єктів ТСПІ 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 ТСПІ у ВТСС;
– встановлення контрольованої зони навколо об’єкту;

– залучення до робіт по будівництву, конструкції об'єктів ТСПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

– організація контролю і обмеження доступу на об'єкти ТСПІ 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 технічний заходам з використанням пасивних засобів відносяться :

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

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

– локалізація випромінювань **:**

- екранування ТСПІ та їх ліній з'єднання;
- заземлення ТСПІ 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 ТСПІ;

- встановлення облаштувань гарантованого живлення ТСПІ (наприклад, мотор-генераторів);

- встановлення в ланцюгах електроживлення ТСПІ, 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 ВТСС, що мають вихід за межі контрольованої зони;

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

ІІІ. 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.
6. Що становить правову основу технічного захисту інформації в Україні?
7. Як можна розділити нормативно-правову й методичну базу в області ТЗІ з урахуванням області застосування?
8. Що таке «інформаційна система»?
9. Як можна представити систему захисту інформації для конкретних об'єктів?
10. Що таке матриця знань інформаційної безпеки і як вона формується?

Тема № 8

Практичне заняття № 4. Методи захисту акустично-оптичного каналу та пошуку електронних пристроїв перехоплення інформації.

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

Кількість годин– 4 год.

Навчальні питання:

1. Принцип дії лазерної акустичної локаційної системи і методи захисту акустично-оптичного каналу.
2. Методи і засоби виявлення та заглушення диктофонів.
3. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації.
4. Методи пошуку електронних пристроїв з використанням виявителів пустот, металошукачів і рентгенівських апаратів.
5. Методи пошуку з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерцепторів.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. 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:

І. Порядок проведення вступу до заняття.

1. Принцип дії 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. 13 зображено взаємне положення світлочутливого елементу та відбитого променя при правильному настроюванні.

Рис. 13

Другий варіант побудови ЛАЛС 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 14).

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

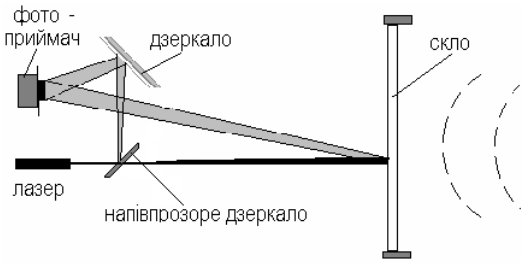

Рис. 14

До недоліків ЛАЛС можна віднести:

– складність установки (настроювання) системи при використанні ІК діапазо-ну (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 рис. 15.

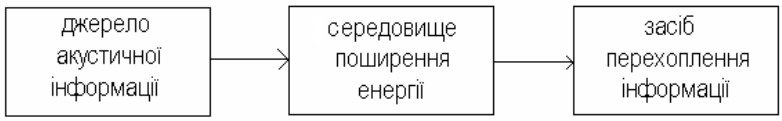

Рис. 15

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 заглушення 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 заглушення і пристрої

ультразвукового заглушення типу «Завіса».

Принцип дії пристроїв електромагнітного заглушення («Рубіж», «Шумотрон», «Буран», «УПД») ґрунтується на генерації в дециметровому діапазоні частот (звичайно в межах 900 МГц) потужних шумових сигналів. В основному для заглушення 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 заглушення диктофонів в неекранованому корпусі становить декілька метрів.

Системи *ультразвукового заглушення* (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) заглушення 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 заглушення підвищується. Проте, системи ультразвукового заглушення 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.

3. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації

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).

В основі *виявлення об’єктів за допомогою нелінійних локаторів*[1] 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,

[1] Розробки нелінійних локаторів почалися в США, Великобританії та СРСР е 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.

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 залежністю загасання величини потужності в середовищі поширення як зондуючого 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. Методи пошуку електронних пристроїв з використанням виявителів пустот, металошукачів і рентгенівських апаратів

Робота *виявителів пустот* заснована на принципі виявлення ділянок середовища, діелектрична проникність яких істотно відрізняється від середнього значення.

Існує безліч *класифікацій металошукачів*.

1. Металошукачі за принципом передача-прийом.
2. Металошукачі на биття.
3. Металошукачі за принципом електронного частотоміра.
4. Імпульсні металошукачі.
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, багатоелементної 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 зондуючого випромінювання, а також особливостями конструкції, зумовленими способом формування зображення.

У багатоелементних 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.

5. Методи пошуку з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерсепторів

Інформативні побічні електромагнітні випромінювання

Інформативними ПЕМВН називаються сигнали, що являють собою ВЧ – носійну, модульовану інформацією, оброблюваною 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 аудіо-візуального 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 висуваються 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.
7. Що відбувається при відбитті лазерного променя від поверхні скла під впливом акустичного сигналу?
8. Існує два варіанти побудови ЛАЛС. Який варіант забезпечує більш високу чутливість системи, але складніший в реалізації?
9. Назвіть недоліки ЛАЛС?
10. На які групи з урахуванням виділених областей розвідувального контакту діляться способи захисту від прослуховування з використанням ЛАЛС?

Тема № 12

Практичне заняття № 5 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:

7. Класифікація засобів радіовиявлення.
8. Інтерсептори.
9. Вимірювальні засоби радіомоніторингу.
10. Радіочастотоміри.
11. Селективні мікровольтметри і нановольтметри.

12. Панорамні засоби радіомоніторингу.

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 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. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут інтелектуальної власності та права – К.: КІІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
11. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова,
12. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
13. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

14. 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.
15. 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.
16. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
17. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 230 с.
18. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2019. 187 с.

Інформаційні ресурси в Інтернеті

19. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
20. 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.
21. 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/.
22. 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.
23. 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.
24. 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/.
25. 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/.
26. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
27. 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:

І. 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».

ІІ. 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 скануючи радіоприймальні пристрої для пошуку, ідентифікації і локалізації джерела випромінювання і радіомоніторингу з індикацією розподілу сигналів у робочому діапазоні частот. Мають здатність настроювання на задані частоти або обраний відгук, а також вхід для підключення зовнішніх антен.

В – *вимірювальні*. 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 настроювання 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.

4. 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 відображуються на цифровому рідкокристалічному індикаторі.

5. 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.

6. 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:

6. Охарактеризувати методи і засоби пошуку електронних закладних засобів.
7. Охарактеризувати методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
8. Охарактеризувати методи пошуку закладок з використанням нелінійних локаторів, виявителі порожнеч (пустот), металошукачів і рентгенівських апаратів .
9. Перелічити засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
10. Засоби пошуку пристроїв перехоплення інформації.