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.

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 контрою ефективності заходів	**14**	**4**			**6**	**4**	

	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 лабораторних занять

Тема І. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.

Лабораторна робота № 1 на тему: Дослідження побічних електромагнітних випромінювань та наведень (ЕМВН) у діапазоні частот 30 – 1000 МГц із використанням селективного мікровольтметра SMV 8.5. (тренажер).

Навчальна мета заняття: Набуття основних навичок роботи із селективним мікровольтметром SMV 8.5, генераторами шуму і генераторами стандартних високочастотних сигналів.

Кількість годин – 4 год.

Навчальні питання:

1. Основні технічні характеристики селективного мікровольтметра SMV – 8.5.

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 ного 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.

Селективний мікровольтметр SMV 8.5 є високочутливим гетеродинним вимірювальним приймачем, що працює в частотному діапазоні від 26 до 1000 МГц. Прилад призначений для вимірювання напруг синусоїдних високочастотних сигналів, напруженості поля радіозавад та імпульсних завад.

ІІ. Основна частина.

Основні технічні характеристики селективного мікровольтметра SMV – 8.5

	Параметр	**Значення**
1	Частотний діапазон	від 26 до 1000 МГц
2	Межі вимірювання напруги	ступенями по 5 дБ і 10 дБ
3	Калібрування напруги	внутрішнім каліброваним генератором, регульованим по напрузі та частоти
4	Похибка при вимірюванні напруги	± 0,8 дБ
5	Вхідний опір	50 Ом
6	Ширина смуги пропускання	120, 20, 1 кГц
7	Ослаблення по каналу дзеркальної частоти	60...80 дБ
8	Ослаблення по каналу проміжної	

	частоти	70...80 дБ
9	Напруга мережі	220/110 В
10	Частота мережі	від 48 до 62 Гц і 400 Гц
11	Споживана потужність	15 Вт
12	Живлення від зовнішньої батареї	
	• нерегульоване	12 В
	• регульоване	від 16 до 30 В
13	Габаритні розміри	550x200x400 мм
14	Маса	22 кг

2. Органи керування селективного мікровольтметра SMV 8.5 (рис. 4.3)

1 – **HF –** дільник напруги ВЧ (від 0 до 60 дБ, ступенями по 10 дБ);

– калібрування частоти (на вхід приймача подаються частотні мітки 5 або 20 МГц) ;

2 – **ZF –** дільник напруги ПЧ (від 0 до 55 дБ, ступенями по 5 дБ);

3 – перемикач виду робіт (індикаторний прилад показує при ненатиснутих кнопках робочі напруги приладу);

– калібрування I (кнопка натиснута: індикатор показує напругу калібрувального генератора);

/AV I – вимірювання середнього значення АМ-сигналів (межа відліку 20 дБ);

/ P – вимірювання пікового значення АМ-сигналів;

/QP – вимірювання квазіпікового значення імпульсних напруг (квазіпікова характеристика відповідно до вимог МСКР);

/AV II – вимірювання середнього значення АМ – сигналів (межа відліку 40 дБ);

4 – – лампа для індикації настроювання (працює тільки при ширині смуги частот 120 кГц – кнопки 30 не натиснуті);

5 – індикаторний прилад (верхня шкала: межа відліку 20 дБ; нижня шкала: межа відліку 40 дБ);

6 – механічна корекція нульової точки індикаторного приладу;

7 – шкала частот;

8 – гвинт для корекції візирної лінії;

9 – перемикач піддіапазонів частот;

10 – – вимикач мережі (прилад працює з живленням від мережі або від батареї 16-30 В);

11 – – вимикач батареї (прилад працює з живленням від батареї 12 В, кнопки 10 і 11 натиснуті: зарядка зовнішньої батареї 15 В від мережі);

12 – - вихід для головного телефону;

13 – – перемикач “Вимірювання – калібрування” (кнопка не натиснута: калібрування, приймач з'єднаний з калібрувальним генератором; кнопка натиснута: вимірювання, приймач з'єднаний із вхідним гніздом);

14 – – вхід приймача;

15 – – калібрування підсилення (кнопка не натиснута: калібрування вручну за допомогою регулятора 21);

– (кнопка натиснута: автоматичне калібрування підсилення);

16 – – частотні позначки (кнопка не натиснута: 20 МГц; кнопка натиснута: 5 МГц);

17 –  – регулятор гучності;

18 –  – автоматичне підстроювання частоти (кнопка не натиснута: АПЧ приймача на приймальну частоту);

 – (кнопка натиснута: АПЧ калібрувального генератора на приймальну частоту);

19 – **Р** – регулятор компенсаційної напруги (для вимірювання пікового значення АМ-сигналів);

20 –  – електрично нульова точка (при виді роботи «QP» для корекції нульової точки індикаторного приладу);

21 –  – регулятор калібрування підсилення (для установки підсилення приймача вручну);

22 –  – регулятор корекції калібрування підсилення (корекція автоматичного калібрування підсилення);

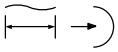
23 –  – регулятор калібрування I (для установки напруги калібрувального генератора);

24 –  – підстроювання генератора (для підстроювання частоти калібрувального генератора);

25 – точне настроювання приймача;

26 – грубе настроювання приймача;

27 –  – вихід для підключення осцилографа;

28 –  – вхід для подачі напруги хитання (хитання частоти 3-го гетеродина приймача);

29 –  – вихід проміжної частоти (3-я ПЧ, f = 1,67 МГц);

30 –  120 kHz – перемикач ширини смуги частот (кнопки «120 кГц» і «1 кГц» не натиснуті: ширина смуги частот 120 кГц);

 20 kHz – перемикач ширини смуги частот (кнопка натиснута: ширина смуги 20 кГц, індикаторна лампа 4 не горить:

– якщо кнопка 15 знаходиться в положенні  , то відключений генератор НЧ для АПЧ калібрувального генератора;

– якщо кнопка 15 знаходиться в положенні  , то включена ширина смуги частот 120 кГц);

 1 kHz – перемикач ширини смуги частот (кнопка натиснута: ширина смуги частот 1 кГц; індикаторна лампа настроювання 4 не горить);

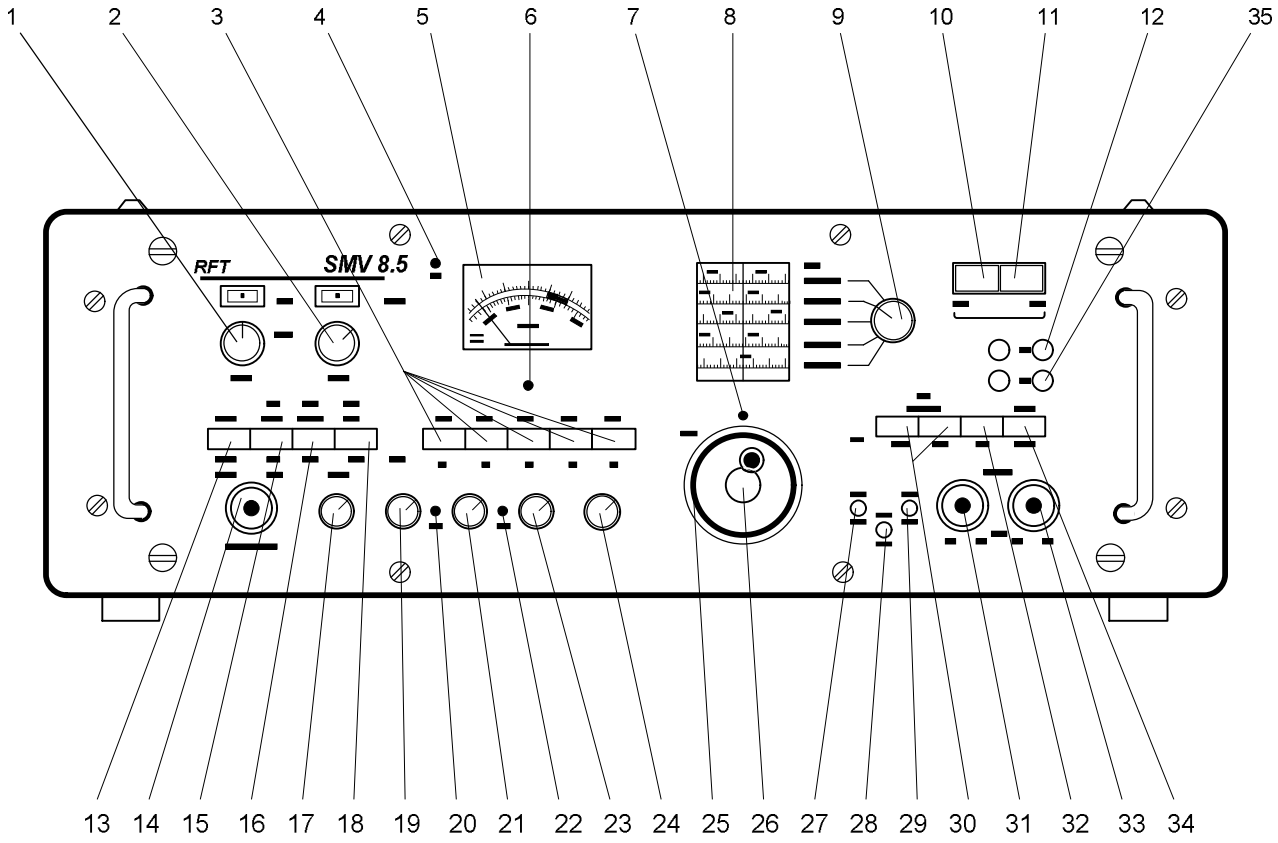
31 –  – вихід калібрувального генератора (від 26 до 300 МГц);

32 –  – вихід калібрувального генератора (від 300 до 1000 МГц);

33 –  – вимикач калібрувального генератора (кнопка натиснута: генератор включений, пристрій для прослуховування не працює);

34 – **АМ/ FM** – перемикач виду демодуляції (кнопка не натиснута: детектування АМ-сигналів; кнопка натиснута: детектування ЧМ-сигналів, індикаторна лампа 4 не горить);

35 –  – вихід для самозаписувача (для підключення самозаписувача або іншого індикаторного приладу).



II. Основна частина

Порядок роботи із селективним мікровольтметром SMV 8.5

1. Калібрування підсилення вручну

- установити перемикач (13) у положення «Калібрування» (кнопка не натиснута);
- установити перемикач (15) у положення «Калібрування вручну» (кнопка не натиснута);
- натиснути кнопку (3) і за допомогою регулятора калібрування (23) установити напругу калібрувального генератора на позначку на індикаторному приладі (5);
- відпустити кнопку (3);
- за допомогою підстроювання частоти генератора (24) настроїти калібрувальний генератор на частоту приймача.

При смузі пропускання 120 кГц генератор у більшості випадків, при середньому положенні підстроювання частоти генератора (24), автоматично настроюватиметься на приймальну частоту.

Перед калібруванням підсилення при виді роботи «QP» слід перевірити електрично нульову точку (положення дільника проміжної частоти – 30 дБ, без вхідного сигналу). Корекцію електричної нульової точки можна робити регулятором (20).

Калібрування слід виконувати перед кожним вимірюванням, а також при включенні іншого виду робіт або ширини смуги пропускання.

2. Настроювання на вимірюваний сигнал

– вибрати вид відліку перемикачем виду робіт «QP» *(3)*;

– вибрати смугу пропускання за допомогою перемикача ширини смуги *(30)* 120 кГц;

– установити дільник високочастотної напруги ***(1)*** і дільник напруги проміжної

частоти (2) на приблизний рівень вимірюваного сигналу;

– установити перемикач (13) у положення «Вимірювання»;

– настроїти приймач перемикачем діапазону частот (9) і настроюванням приймача (25, 26) на частоту сигналу.

Переключення виду демодуляції здійснюється за допомогою перемикача (34).

3. Вимірювання імпульсних напруг при виді робіт «QP»

Цей вид роботи призначений головним чином для квазіпікового вимірювання імпульсних напруг завад. Крім того, цей вид роботи може застосовуватися для вимірювання високочастотних сигналів з імпульсною модуляцією.

Перед вимірюванням необхідно зробити калібрування підсилення (див. п. 1).

Після цього установити кнопку (13) у положення «Вимірювання» і точно настроїти приймач на вимірюваний сигнал (див. п. 4.5.2).

Вибрати смугу пропускання 120 кГц.

Для запобігання перевантаження приладу при вимірюванні імпульсних напруг завад слід звернути увагу на максимально допустиме ослаблення дільника напруги проміжної частоти. При невідомій частоті проходження імпульсів завад або у випадку одиночних імпульсів, ослаблення дільника напруги проміж-ної частоти (2) не повинно перевищувати 5 дБ. При відомій частоті проходження імпульсів, ослаблення дільника напруги проміжної частоти може бути підвищене до значень, вказаних у таблиці 1.1.

Таблиця 1.1 – Значення ослаблення дільника напруги проміжної частоти

Частота проходження імпульсів, Гц	Максимальне ослаблення ПЧ, дБ
≥ 2	10
≥ 5	15
≥ 10	20
≥ 50	30
≥ 100	35
≥ 500	40
≥ 1000	45

Ослаблення дільників напруги високої частоти і проміжної вибираються таким чином, щоб індикація індикаторного приладу складала по можливості від +5 до +10 дБ.

Вимірюване значення відраховується від суми ослаблення дільників напруги і значення показників індикаторного приладу в «дБ» відносно 1 мкВ (за замовчуванням $U_{шуму} = 1$ дБ). Тоді $U_{сигн} = U_{показ} – U_{шуму}$.

III. Заключна частина заняття

1. Набуття навиків роботи на селективному мікровольтметрі SMV 8.5 за допомогою тренажера.

Тема № 5. Методи та засоби несанкціонованого отримання інформації по технічних каналам

Лабораторна робота № 2 на тему: Захист мовної інформації від витоку з акустичного каналу методом енергетичного приховування.

Навчальна мета заняття: вивчити методи енергетичного приховування сигналів для захисту акустичного каналу витоку інформації на прикладі ультразвукового заглушувача акустичних закладних пристроїв та диктофонів.

Кількість годин – 8 год.

Навчальні питання:

1. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від частоти другого генератора F2, зменшуючи останню на 300 кГц.
2. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від напруги другого генератора F2.
3. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від відстані до мікрофона.
4. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від кута Ф між мікрофонами.

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.: КІВП, 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 ного 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.

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. Електрорушійна сила, наведена цим полем в магнітній антені, підсилюється і виділяється з шуму спеціальним блоком оброблення сигналів. При перевищенні рівня прийнятого сигналу деякого встановленого порогового значення спрацьовує світлова або звукова сигналізація. Щоб уникнути хибних спрацьовувань, поріг виявлення необхідно коригувати практично перед кожним сеансом роботи, що є недоліком приладів подібного типу.

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. В ході переговорів оператор наближує антену (руку) до можливого місця встановлення диктофону (портфель, одяг співрозмовника і т. ін.). 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 (наприклад, детектор PTRD-18 має можливість під'єднання до 16 подавачів одночасно), 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.

Через слабкий рівень магнітного поля, створюваного працюючими диктофонами (особливо в екранованих корпусах), дальність їх виявлення детекторами незначна. Наприклад, дальність виявлення диктофону L-400 в режимі запису в умовах офісу навіть при використанні стаціонарного детектора PTRD-018 не перевищує 45…65 см. Дальність

виявлення диктофонів у неекранованих корпусах може становити 1…1,5 м.

Для виявлення непрацюючих диктофонів застосовуються нелінійні локатори. До типових представників пристроїв цього класу належить, наприклад, нелінійний локатор «Циклон-Рамка». Локатор має два подавача, виносний пульт керування і може приховано встановлюватися в дверний проріз виділеного приміщення, що дозволяє контролювати наявність у відвідувачів (як у ручному вантажі, так і під одягом) будь-яких радіоелектронних пристроїв, у тому числі диктофонів та підслуховувальних пристроїв як у включеному, так і у виключеному стані. 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. Внаслідок цього одночасно з інформаційним сигналом (мовою) здійснюється запис і детектованого шумового сигналу, що призводить до значного спотворення першого. 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. Наприклад, заглушувач диктофонів «Шумотрон-2» працює в імпульсному режимі на частоті 915 МГц. Тривалість випромінюваного імпульсу не більше 300 мкс, а імпульсна потужність – не менше 150 Вт. При середній потужності випромінювання 20 Вт забезпечується дальність заглушення диктофонів в екранованому корпусі (типу «Olimpus-400») до 1,5 м в секторі близько 30 градусів. 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. У спектрі записуваних сигналів з'являються інтермодуляційні завади у вигляді заважальних сигналів з комбінаційними частотами ультразвукових коливань. Найбільшою за амплітудою буде завада з частотою однакової різниці частот ультразвукових коливань (1 кГц), і така, що лежить у смузі пропускання ПЗЧ.

На відміну від систем електромагнітного заглушення подібні системи забезпечують заглушення в значно більшому секторі. Наприклад, комплекс «Завіса» при використанні двох ультразвукових випромінювачів здатний забезпечити заглушення диктофонів та акустичних закладок у приміщенні об'ємом 27 м^3. 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.

II. Основна частина

Порядок виконання роботи

Структурна схема лабораторного макету ультразвукового заглушувача акустичних закладних пристроїв та диктофонів подана на рис. 1.

Макет містить два ідентичних канали, що виконують функції генераторів ультразвукових коливань, та виносний мікрофон з мікрофонним підсилювачем.

Коливання з частотами 18-21 кГц надходять або з внутрішніх генераторів, або із зовнішніх генераторів Г3-33 через попередні підсилювачі. Зовнішній вигляд макету поданий на рис. 2.

1.Зібрати схему для проведення вимірювання, для чого:

– під'єднати два зовнішні генератори Г3-33 до клем «Вход внешнего генератора-1» та «Вход внешнего генератора-2»;

– ручки «Регулировка уровня» встановити у крайнє праве положення;

– перемикачі «Генератор-1» «Генератор-2» встановити в положення «внешний»;

– під'єднати гучномовці до клем «Динамик-1» и «Динамик-2» і розташувати їх згідно з рисунком 3;

– встановити вихідний опір генераторів Г3-33 600 Ом, а вихідну напругу 1,4 мВ; (вихідна напруга генераторів не повинна перевищувати 200 мВ).

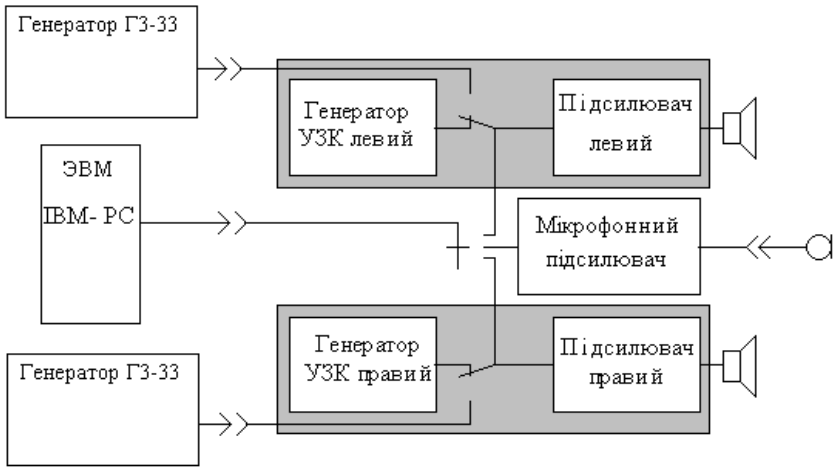


Рис. 1.

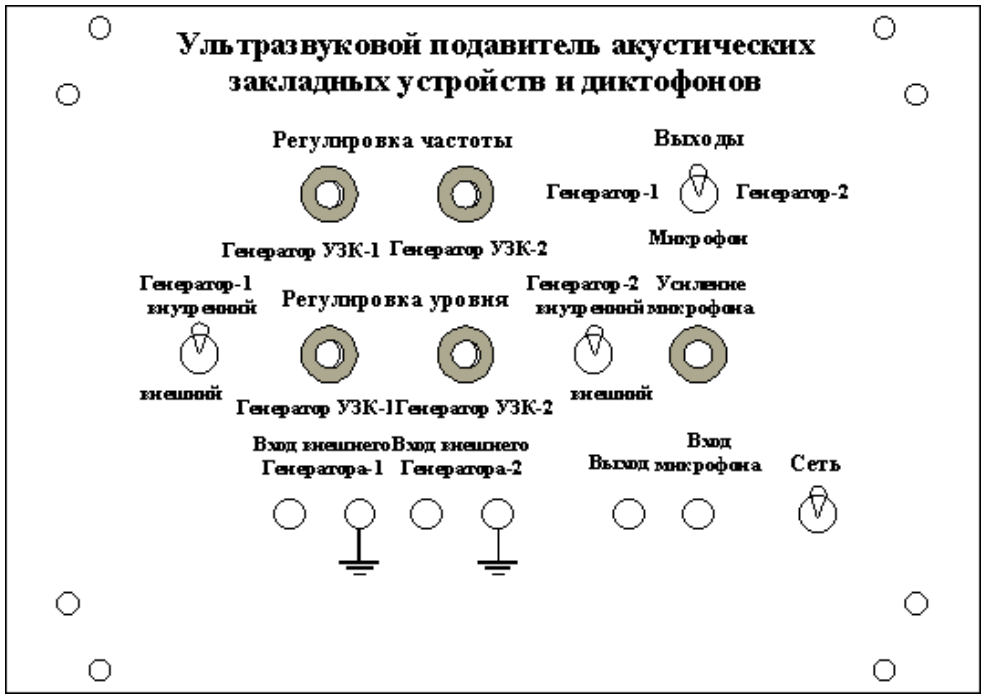


Рис. 2.

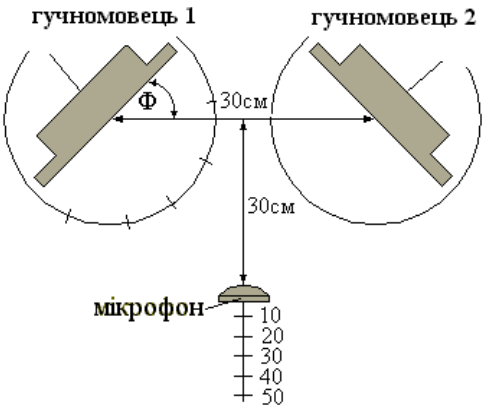


Рис. 3.

– встановити частоту генераторів 20 кГц і 19,3 кГц.

– під'єднати вихід мікрофонного підсилювача до звукової плати ЕОМ;

– для проведення вимірювання ввімкнути програму Spectra Plus та здійснити її настроювання.

2. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від частоти другого генератора F_2, зменшуючи останню на 300 кГц. Результати вимірювань внести в таблицю 1.1

Таблиця 1.1

F_2,кГц	19,3	19	18,7	18,4	18,1	17,8	17,5
U, дБ							

3. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від

напруги другого генератора F_2. Встановити частоту генераторів 20 кГц і 19 кГц. Напругу першого генератора встановити 40 мВ, рівень напруги другого генератора встановити згідно з таблицею 1.2

Таблиця 1.2

U,мВ	0	8	16	24	32	40
U, дБ						

4. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від відстані до мікрофона. Мікрофон розташувати згідно з рисунком 4.4. Результати вимірювань внести в таблицю 1.3

Таблиця1.3

L, см	0	6	15	20	30	48
U, дБ						

5. Зняти залежність рівня першої гармоніки інтермодуляційних спотворень від кута Ф між мікрофонами. Мікрофон розташувати згідно з рисунком 4.4. Результати вимірювань внести в таблицю 1.4.

Таблиця 1.4

Ф ,^{0}	0	15	30	45	60	75	90
U, дБ							

Зміст звіту

Звіт з лабораторної роботи має містити:

– структурну схему лабораторного макету;

– спектрограму сигналу на виході мікрофону при максимальних рівнях на виходах генераторів та різницею частот 1 кГц;

– результати вимірювань (таблиці та графіки);

– висновки.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Назвіть основні методи захисту інформації від витоку з акустичного каналу.
2. Назвіть основні методи виявлення диктофонів, що працюють в режимі запису.
3. Назвіть типи і основні технічні характеристики засобів виявлення диктофонів.
4. Нати пояснення принципу дії засобів електромагнітного подавлення.
5. Дати пояснення принципу дії засобів ультразвукового подавлення.
6. Назвіть типи і основні технічні характеристики засобів електромагнітного та ультразвукового подавлення.

Тема № 6 Акустичні технічні канали витоку інформації

Лабораторна робота № 3 на тему: Дослідження побічних електромагнітних випромінювань та наведень (ПЕМВН) у діапазоні частот 30 – 1000 МГц із використанням селективного мікровольтметра SMV 8.5 (тренажер).

Навчальна мета заняття: дослідження побічних електромагнітних випромінювань та наводок ПЕМВН у діапазоні частот 30 – 1000 МГц із використанням селективного мікровольтметра SMV 8.5. Набуття основних навичок роботи із селективним мікровольтметром SMV 8.5, генераторами шуму і генераторами стандартних ВЧ – сигналів.

Кількість годин – 4 год.

Навчальні питання:

1. У діапазоні частот, зазначеному викладачем, із кроком 5 МГц виміряти рівень шуму у досліджуваному приміщенні.
2. За допомогою селективного мікровольтметра SMV – 8.5 зробити пошук сигналів на різних частотах і діапазонах, що відповідають тестовому сигналу.
3. Відключити досліджуваний об'єкт і на частотах, на яких було виявлене випромінювання, зняти рівень шуму $U_{Ш1.}$
4. Розрахувати значення $U_{c1.}$

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 ного 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.

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 (рис. 4.1), даними, оброблюваними на пристроях введення-виведення і т. д. [5, 6].

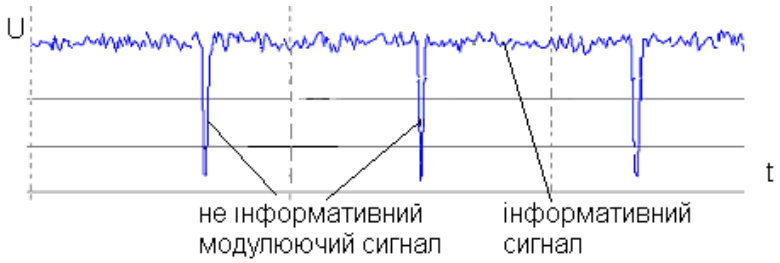


Рис. 1 Сигнал виведення зображення на монітор

Неінформативними ПЕМВН називають сигнали, аналіз яких може дати уявлення тільки про режим роботи ЗОТ і ніяк не відбиває характер оброблюваної інформації.

Джерела ПЕМВН

У ЗОТ виділяють два основних вузли ймовірних джерел ПЕМВН: сигнальні кабелі і високовольтні блоки. Для випромінювання сигналу в ефір необхідна узгоджена на конкретній частоті антена. Такою антеною є довгі лінії передачі даних – з'єднувальні кабелі. У той же час підсилювачі променів в електронно-променевих трубках моніторів ЗОТ мають набагато більшу енергетику і також виступають як випромінюючі системи.

Методи пошуку сигналів ПЕМВН

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

Перший метод – *метод порівняння панорам*. Він 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.

На практиці даним методом стійко виявляються ПЕМВН, що перевищують рівень шуму не менше ніж на 6–10 дБ. Слабші сигнали модулюються шумом і виявляються нестабільно. Для виявлення слабких сигналів використовуються алгоритми накопичення й усереднення, які уже давно застосовуються для виділення сигналів ізшуму. На рис. 4.2 показана одна й та сама ділянка спектра, отримана без усереднення (ліва частина рисунка) і з усередненням 15 разів). Застосування алгоритмів усереднення на сертифікаційних випробуваннях дало змогу стійко виявляти сигнали, що перебувають усього на 0,5 дБ вище рівня шуму і навіть на 1 дБ нижче рівня шуму.

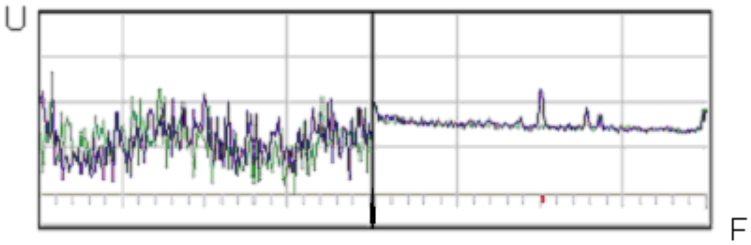


Рис. 2 Ділянка спектра, отримана без усереднення (ліва частина рисунка) і з усередненням 15 разів (права частина рисунка)

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.

За звичай цим методом виявляються лише ті сигнали, які можна почути в динаміках і побачити на графіках, тобто сигнали, що мають відношення сигнал/шум понад 2–4 дБ. Реалізація методів накопичення й усереднення при одержанні панорам забезпечує візуальне виявлення навіть тих сигналів, що на слух ідентифікуються надто важко.

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.

Практичні результати показали, що даним методом легко виявляють навіть такі сигнали, які досвідченому операторові знайти вкрай важко або в розумних межах знайти просто неможливо. Тридцять-сорок частот ПЕМВН монітора – нормальне явище для цього методу виявлення.

Відображений останнім часом у рекламі *кореляційний метод* пошуку разом з перевагами має і ряд недоліків, що знижує його застосування у вимірювальних комплексах.

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.

У більшості аналізаторів спектра відсутній преселектор. Разом з тим, ціна сучасного аналізатора спектра вдвічі-втричі нижча ціни аналогійного за частотним діапазоном вимірювального приймача.

У деяких окремих ситуаціях можна визнати допустимим використання для виявлення і вимірювання ПЕМВН зв'язкового скануючого радіоприймача, що калібрується за допомогою зовнішнього еталонного генератора. Проте споживачі повинні мати чітке уявлення застосування такої апаратури.

В даний час існують також автоматизовані вимірювальні комплекси ПЕМВН, такі як «Навігатор», що дозволяють вести пошук сигналів як в автоматичних, так і в напівавтоматичних і ручних режимах.

Вибір детектора

Для вимірювань використовуються слідуючи типи детекторів: піковий, квазіпіковий, середньоквадратичний.

Для вимірювання амплітуди сигналу застосовується піковий детектор. Детектор середньоквадратичних значень рекомендований для вимірювання шуму (спектральної густини потужності шуму), оскільки «здійснює коректні вимірювання шуму незалежно від його джерела».

Інші детектори (квазіпіковий, середній та ін.) призначені для вимірювання параметрів сигналів при використанні спеціальних методик. Результати вимірювань цими детекторами не мають значення якоїсь фізичної величини. Так, зокрема, квазіпіковий детектор застосовується для уніфікації вимірювань радіозавад.

II. Основна частина

Порядок виконання роботи

1. Ознайомитися з основними технічними характеристиками селективного мікровольтметра SMV – 8.5 й органами його керування (див. п. 4.3, 4.4).

2. Включити селективний мікровольтметр SMV 8.5 і генератор Г4-107. Прогріти прилади не менше 5 хвилин.

3. На генераторі Г4-107 виставити довільну частоту (глибина модуляції 60 %, кнопки «ВНУТР», «ЧМ», «ВКЛ» натиснуті, інші – ні, ослаблення – 0). Підключити антену.

4. За допомогою селективного мікровольтметра SMV 8.5 знайти несучу частоту. Для чого:

– вибрати межу відліку перемикачем виду робіт «QP» (3);

– вибрати смугу пропускання за допомогою перемикача ширини смуги (30) 120 кГц;

– поставити дільник високочастотної напруги (1) і дільник напруги проміжної частоти (2) на приблизний рівень вимірюваного сигналу;

– установити перемикач (13) у положення «Вимірювання»;

– вибрати тип антени і її довжину. Причому на частотах до 79 МГц – довжина стрижнів вібраторів відповідає довжині стрижнів вібраторів для частоти 80 МГц, на частотах від 80 до 141 МГц необхідне застосування вібраторів з довгими стрижнями, на частотах від 142 до 300 МГц – застосування вібраторів з короткими стрижнями, на частотах понад 300 МГц – необхідне застосування логоперіодичної антени (ЛПА). Настроювання симетричних вібраторів на задану частоту провадиться або за допомогою спеціальної частотної лінійки, або за допомогою звичайної лінійки (у цьому випадку довжина стрижнів вібраторів визначається за допомогою таблиці 4.2, значення вказані в міліметрах). При пошуку сигналу в смузі частот 26 – 300 МГц слід враховувати, що перемикач на узгоджувальному пристрої повинен бути в одному з трьох положень (26 - 46 МГц, 46 - 80 МГц, 80 - 300 МГц) залежно від частоти, на якій відбувається виявлення сигналу (для вимірювання з ЛПА в узгоджувальному пристрої немає потреби);

– настроїти приймач перемикачем діапазону частот (9) і настроюванням приймача (25, 26) на частоту сигналу. Свідченням знаходження несучого сигналу є загоряння лампи (4) (для випадку АМ).

Таблиця 1.1 – Довжина стрижнів вібраторів

f (МГц)	+ 0 МГц	+ 1 МГц	+ 2 МГц	+ 3 МГц	+ 4 МГц	+ 5 МГц	+ 6 МГц	+ 7 МГц	+ 8 МГц	+ 9 МГц	
80	887	875	863	851	839	827	817	807	797	787	Довгі стрижні
90	777	769	761	753	745	737	729	721	713	705	
100	697	690	683	676	669	662	656	650	644	638	
110	632	626	620	614	608	602	8597	592	587	582	
120	577	572	567	562	557	552	548	544	540	536	
130	532	528,5	525	521,5	518	514,5	511	507,5	504	500,5	
140	497	493,5	490	486,5	483	479,5	476	472,5	469	465,5	Короткі стрижні
150	462	458,5	455	451,5	448	444,5	441	437,5	434	460,5	
160	427	424,5	422	419,5	417	414,5	412	409,5	407	404,5	
170	402	399,5	397	394,5	392	389,5	387	384,5	382	379,5	
180	377	375	373	371	369	367	365	363	361	359	
190	357	355	353	351	349	347	345	343	341	339	
200	337	335	333	331	329	327	325	323	321	319	
210	317	315,5	314	312,5	311	309,5	308	306,5	305	303,5	
220	302	300,5	299	297,5	296	294,5	293	291,5	290	288,5	
230	287	285,5	284	282,5	2681	279,5	278	276,5	275	273,5	
240	272	270,5	269	267,5	266	264,5	263	261,5	260	258,5	
250	257	256	255	254	253	252	251	250	249	248	
260	247	246	245	244	243	242	241	240	239	238	
270	237	236	235	234	233	232	231	230	229	228	
280	227					223					
290	219					215					
300	211										

5. Установити вимірювальну антену на відстані 1 м від обраного об’єкта дослідження (монітора).

6. Відкалібрувати селективний мікровольтметр SMV 8.5.

7. У діапазоні частот, зазначеному викладачем, із кроком 5 МГц виміряти рівень шуму у досліджуваному приміщенні. Отримані дані занести в таблицю 4.3 наступного вигляду (див. програму «EVT.xsl» вкладень «Volna»):

Таблиця 1.2 – Рівень шуму у досліджуваному приміщенні

	f, МГц	Uш, дБ

Після кожного вимірювання необхідно калібрувати прилад.

8. Запустити тестову програму «test.xsl» на моніторі, одержати чергувальні чорно-білі смуги (міру).

9. За допомогою селективного мікровольтметра SMV – 8.5 зробити пошук сигналів на різних частотах і діапазонах, що відповідають тестовому сигналу. Отримані дані занести в таблицю 1.3 (стовпці 1 і 2)

Таблиця 1.3 – Рівень сигналів ПЕМВН

f, МГц	$U_{С+Ш}$, дБ	$U_{с1}=(U_{с+ш}{}^2 - U_{ш1}{}^2)^{0,5}$, дБ	$U_{Ш1}$, дБ

Примітка: $U_{Ш1}$ – рівень шумів у досліджуваному приміщенні на частоті інформаційного сигналу;

$U_{С+Ш}$ – рівень сигналу і шуму на даній частоті;

$U_{с1}$ – рівень інформаційного сигналу.

10. Відключити досліджуваний об'єкт і на частотах, на яких було виявлене випромінювання, зняти рівень шуму $U_{Ш1}$ (стовпець 4 таблиці 4.4).

11. Розрахувати значення $U_{с1}$ (стовпець 3 таблиці). Розраховані величини занести в таблицю 1.3.

12. Запустити програму «EVT.xsl». У вкладці «Volna» у таблицю занести результати, отримані в п. 8. Натиснути кнопку «Діаграма». Потім із вкладки «електрична» скопіювати графік електричної складової шуму в звіт, на тому самому графіку побудувати вручну графік $U_{С+Ш}$ від функції частоти.

13. У вкладці «Video» у таблицю занести результати, отримані в п. 9-11.

Натиснути «GO!». У вікні, що з'явилося, вибрати категорію об'єкта – «1», присвоїти значення, рівне 0,23, потім у рядку «Video» виставити поточне розрізнення монітора і частоту відновлення (які знаходяться в: Пуск / Панель керування / Екран / Параметри / Адаптер). Отриману таблицю скопіювати в звіт.

14. Уключити шумовий генератор «Волна 4Р».

15. Повторити пп. 3 –9.

16. За результатами двох серій вимірювань зробити остаточні висновки.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Що називається інформативними ПЕМВН?
2. Що може бути джерелом ПЕМВН?
3. Назвіть методи пошуку сигналів ПЕМВН.
4. Які типи детекторів застосовуються при вимірюванні ПЕМВН?
5. Назвіть прилади для вимірювання ПЕМВН.

ТЕМА № 10 Пошукова техніка для виявлення засобів технічних розвідок

Лабораторна робота № 4 на тему: Захист мовної інформації від витоку з акустично-оптичного каналу.

Навчальна мета заняття: Вивчити принцип дії лазерної акустичної локаційної системи (ЛАЛС), способи демодуляції оптичних сигналів, відбитих від скла, дослідити спектр оптичного сигналу в області низьких частот і методи захисту інформації від витоку зі складеного акустично-оптичного каналу.

Кількість годин – 8 год.

Навчальні питання:

1. Дослідити спектр сигналу, відбитого від віконного скла.
2. Дослідити залежність амплітуди відбитого сигналу від залежності від відстані зайчика променя лазера до краю віконної рами при впливі на скло акустичним сигналом з частотою 1 кГц.
3. Дослідити ефективність протидії прослуховуванню приміщень за допомогою ЛАЛС застосуванням активних методів захисту.
4. Дослідити ефективність протидії прослуховуванню приміщень за допомогою ЛАЛС застосуванням пасивних методів захисту.

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 ного 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.

Принцип дії лазерної акустичної локаційної системи і методи захисту акустично-оптичного каналу.

При відбитті лазерного променя від вібрувальної 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 (рис. 4). В 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 практиці юстирування провадиться за суб'єктивною оцінкою оператором розбірливості мови. На рисунку 4 зображено взаємне положення світлочутливого елементу та відбитого променя при правильному настроюванні.

Рис. 4

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. 5).

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

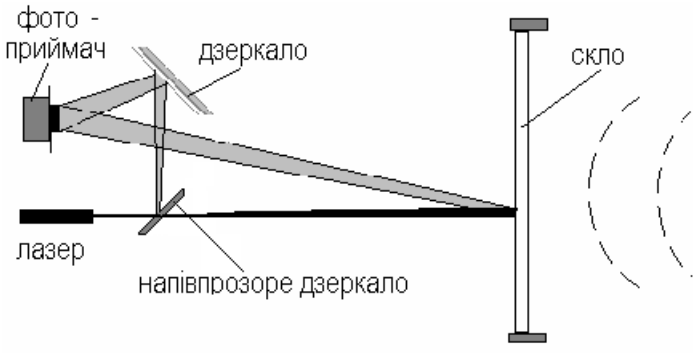


Рис. 5

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, які за своїми акустичними характеристиками наближа-ються до об'ємного резонатора Гельмгольца, коли всі двері і вікна приміщення досить добре герметизовані. Ефективні вони і для підслуховування розмов, які ведуться в салонах автомашин.

Сучасні ЛАЛС дозволяють знімати інформацію не лише від зовнішніх, але й внутрішніх віконних шибок, дзеркал, скляних дверей та інших предметів. Для збільшення коефіцієнта відбиття лазерного випромінювання, а отже і дальності розвідки, скло може оброблятися спеціальним складом.

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.

Засоби акустичної розвідки можуть використовуватися не лише для прослуховування і запису розмов, але й для перехоплення акустичних коливань, що виникають при виведенні на друк тексту на принтері.

Спектр відбитого сигналу містить у своєму складі низькочастотні коливання, що відповідають механічним резонансним частотам, від яких необхідно звільнитися шляхом фільтрації з використанням смугових фільтрів, або за допомогою програм звукових редакторів, що дозволяють записати сигнал і потім обробити його на ЕОМ.

Подвійні віконні рами не дозволяють захиститися від ЛАЛС, тому що промінь відбивається від кожної поверхні скла і можливе настроювання на приймання відбитого сигналу від внутрішнього скла.

Модель розвідувального контакту при зніманні інформації з використанням ЛАЛС подана на рисунку 6.

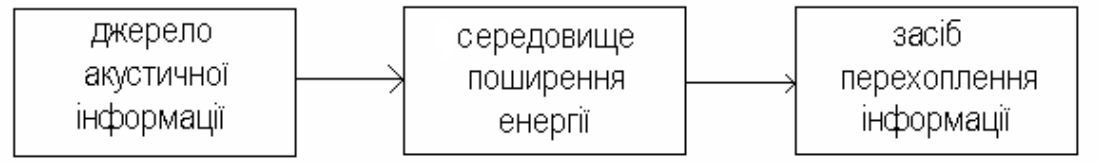


Рис. 6

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:

– використання недоступних для лазерного підслуховування приміщень (вікна приміщень виходять на двір; підвальні, напівпідвальні приміщення);

– розміщення робочих місць, яке виключає проходження акустичних сигналів до вікон;

– захист вікон віконницями, щільними драпуваннями, спеціальними екранами;

– організаційно-технічні:

– використання звукопоглинальних облицювань, покриттів, килимів усередині приміщень;

– використання спеціальних покриттів шибок;

– застосування дзеркально-прозорих плівок;

– технічні:

– використання засобів акустичного зашумовування приміщень;

– встановлення на вікна коливальних шайб, що створюють активні завади;

– застосування відеомоніторинга вікон із використанням відеокамер на базі ПЗС-матриць.

Використання спеціальних покриттів і спеціальних шибок передбачає:

а) індофтористе покриття на шибках – працює за принципом абсолютно чорного тіла, тобто поглинає випромінювання лазера;

б) матове покриття шибок з високим коефіцієнтом поглинання лазерних променів;

в) застосування ситалових шибок, що мають кристалічну поверхню, яка розсіює промені, що падають на неї. Деякі домішки у складі ситалових шибок викликають активну флюоресценцію під впливом падаючих променів, які в свою чергу створюють активну світлову заваду і є сигналізатором про лазерне випромінювання.

Засоби активного захисту вікон являють собою п’єзокристалічні коливальні шайби та електромагнітні генератори шумів. Коливальні шайби приклеюють на поверхню скла. До їх обкладинок підводиться напруга низькочастотних коливань від генераторів шуму, і під його впливом скло коливається. Потужність, що підводиться до вікна, значно перевищує потужність акустичного сигналу, який досягає поверхні вікна. Звичайно генератори шуму працюють в діапазоні звукових частот.

II. Основна частина

Порядок виконання роботи

1. Опис лабораторної установки

Лабораторний макет ЛАЛС призначений для дистанційного одержання інформації шляхом локації оптичним сигналом відбивної поверхні віконного скла, яке піддається впливові акустичних коливань. Схема електрична принципова досліджуваного пристрою наведена на рисунку 7.

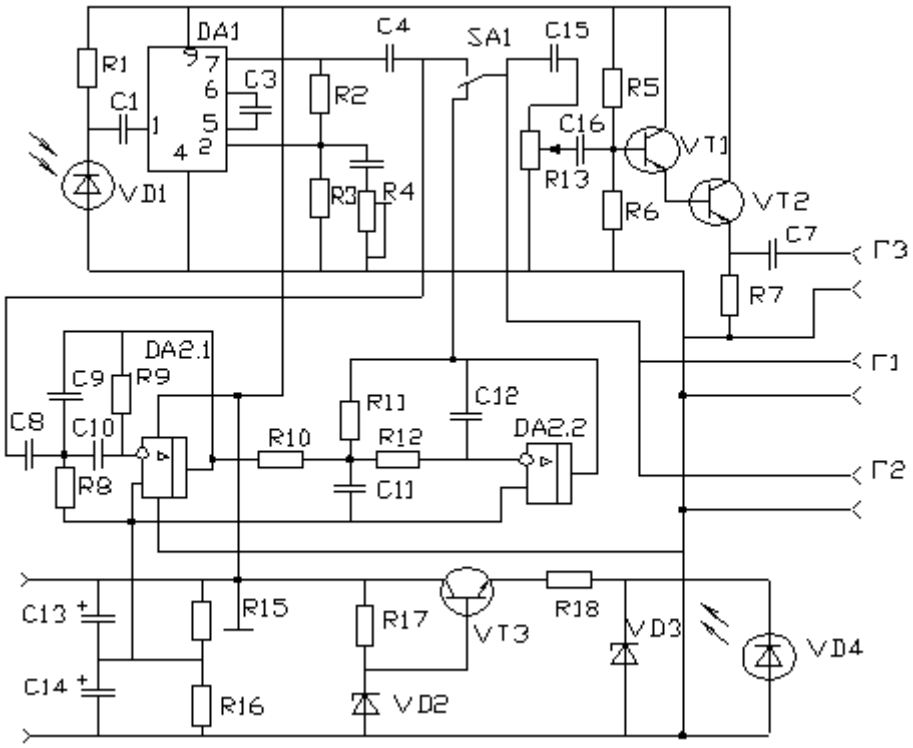


Рисунок 3.4

Як випромінювач застосовується напівпровідниковий лазер VD4, що має наступні основні характеристики:

– діапазон випромінюваних хвиль 630-680 нм;

– випромінювана потужність < 5 мВт.

Лазер живиться від стабілізатора напруги VT3 VD2 R17 через струмообмежувальний резистор R18. Для додаткового захисту лазера від перенапруги паралельно йому підключений стабілітрон VD3.

Відбитий від скла, промінь лазера попадає на фотодіод VD1 фотоприймача. Прийнятий сигнал виділяється на резисторі R1 і через роздільний конденсатор C1 надходить на вхід підсилювача, побудованого на ИМС DA1 типу К548УН1. Резистори R2 і R3 задають режим роботи DA1 за постійним струмом. Коефіцієнт підсилення визначається ланцюжком R2R4C5.

Сигнал з виходу підсилювача надходить в залежності від положення перемикача SA1 або безпосередньо до гнізд підключення осцилографа (Г1) і вольтметра (Г2), або через фільтр до тих самих гнізд.

Фільтр побудований на операційному підсилювачі DA2 типу К157УД2 і складається зі двох послідовно з’єднаних каскадів: фільтра верхніх частот (ФВЧ) - DA2.2, C8, C9, C10, R8, R9 фільтра нижніх частот (ФНЧ) - DA2.2, R10, R11, R12, C11, C12.

Крім гнізд Г1 і Г2 вихідний сигнал надходить на емітерний повторювач на складеному транзисторі VT1, VT2, який призначений для підсилення вихідного сигналу по струму і поданні його на гніздо Г3 для під’єднання низькоомного навантаження (головних телефонів). Мінімальний опір навантаження даного підсилювача – 15 Ом.

Живлення схеми здійснюється від джерела постійної напруги 12,6 В, що входить до складу базового блоку лабораторної установки. Для живлення фільтра використовується резистивний подільник напруги живлення на два R15, R16.

Корпус лабораторного макета встановлений на поворотний пристрій штативу, який дозволяє змінювати напрямок променя для настроювання системи.

2. Порядок виконання лабораторної роботи

2.1 Настроїти системи

Підключити вихід лабораторної установки Г1 до виходу звукової карти ЕОМ IBM-PC. Включити лабораторний макет, ЕОМ, викликати програму SPECTRA PLUS і перейти в режим REAL TIME.

Обертаючи ручки поворотного пристрою штатива і змінюючи нахил лабораторного макета, спрямувати промінь лазера на віконне скло та домогтися попадання відбитого променя в отвір фотоприймача.

Підключити гучномовець до виходу лабораторного генератора звукових частот Г3-33 або Г3-109 і, вибравши коефіцієнт підсилення й швидкість горизонтальної розгортки осцилографа, спостерігати вихідний синусоїдний сигнал, прийнятий фотоприймачем лабораторного макета.

2.2 Зняти амплітудно-частотні характеристики системи з відключеним смужковим фільтром.

Перевести тумблер «Фільтр» в положення «Откл.» Встановити на генераторі частоту 300 Гц.

Зняти АЧХ системи в логарифмічному масштабі, змінюючи частоту генератора від 300 до 4000 Гц із кроком 1/3 октави.

Заповнити таблицю АЧХ системи:

Фільтр	F, Гц	300					
Відкл.	$U_{вих.}$, мВ						
Вкл.	$U_{вих.,}$ мВ						

Заповнити таблицю мінімумів та максимумів АЧХ

Фільтр	F, Гц	300					
Відкл.	$U_{вих.}$, мВ						
Вкл.	$U_{вих.,}$ мВ						

Зарисувати частоти максимумів та мінімумів АЧХ і значення амплітуд на цих частотах.

Побудувати АЧХ системи з відключеним фільтром.

2.3 Зняти АЧХ системи з включеним смужковим фільтром.

Перевести тумблер “Фільтр” в положення “Вкл.” і зняти АЧХ системи. Одержану залежність зарисувати.

2.4 Дослідити спектр сигналу, відбитого від віконного скла.

За допомогою програми SPECTRA PLUS записати відбитий сигнал в пам’ять ЕОМ. Дослідити спектр відбитого сигналу (зі смужковим фільтром і без нього).

За допомогою звукового редактора програми SPECTRA PLUS відфільтрувати сигнал без завад і зарисувати часові діаграми та спектри сигналу до і після фільтрації.

2.5 Дослідити залежність амплітуди відбитого сигналу від залежності від відстані зайчика променя лазера до краю віконної рами при впливі на скло акустичним сигналом з частотою 1 кГц.

2.6 Дослідити ефективність протидії прослуховуванню приміщень за допомогою ЛАЛС застосуванням активних методів захисту. Прикріпити мембрану випромінювача завад до віконного скла, включити живлення генератора. За допомогою програми SPECTRA PLUS записати відбитий сигнал в пам’ять ЕОМ . Зарисувати спектр завадового сигналу.

Переконатися в ефективності пригнічення корисного акустичного сигналу.

2.7 Дослідити ефективність протидії прослуховуванню приміщень за допомогою ЛАЛС застосуванням пасивних методів захисту.

Зміст звіту

Після виконання роботи оформити звіт, який повинен містити:

– структурну схему лабораторної установки;
– таблиці і графіки АЧХ системи, спектри сигналів і завад;
– висновки по роботі.

ІІІ. Заключна частина заняття

Результати заняття узагальнюються за допомогою наступних питань:

1. Назвіть основні технічні характеристики та призначення ЛАЛС.
2. Надайте пояснення принципу дії ЛАЛС.
3. Назвіть параметри відбитого від віконного скла кімнати оптичного сигналу такі, що містять в собі інформацію про акустичні коливання, які поширюються в кімнаті.
4. Назвіть основні методи боротьби з витоком акустичної інформації з акустично-оптичного каналу.

Тема № 14. Методики технічного контрою ефективності заходів технічного захисту інформації від витоку електромагнітними полями

Лабораторна робота. «Вивчення принципу роботи локатора нелінійних переходів»

Час проведення: 6 год. Місце проведення: комп'ютерний клас.

Навчальна мета заняття: Вивчення принципу роботи локатора нелінійних переходів на основі моделювання схеми роботи локатора в онлайн середовищі Circuit Simulator.

Навчальні питання:

1. Ознайомитись із декількома сучасними локаторами нелінійних переходів (ЛНП).
2. Скласти порівняльну таблицю характеристик ЛНП.
3. Побудувати еквівалентну схему роботи ЛНП при опроміненні нелінійних електричних елементів (p-n переходів) і прийомі відбитого сигналу.
4. Зняти часові і спектральні діаграми сигналів ЛНП для режиму безперервного зондуючого сигналу.
5. Скласти звіт про виконану роботу із зазначенням висновків.

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

План проведення заняття:

І. Порядок проведення вступу до заняття.

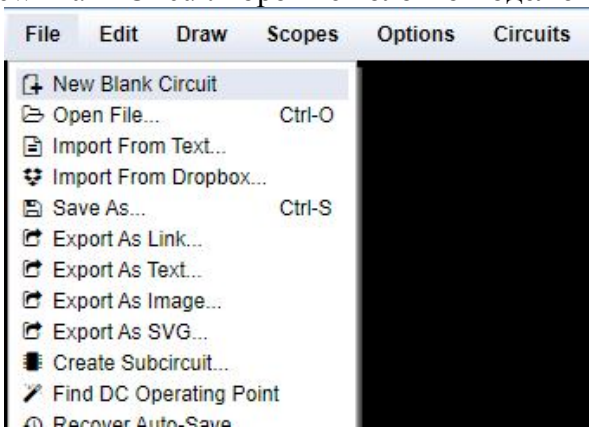
Принцип дії, призначення технічні особливості нелінійних локаторов.

ІІ. Основна частина

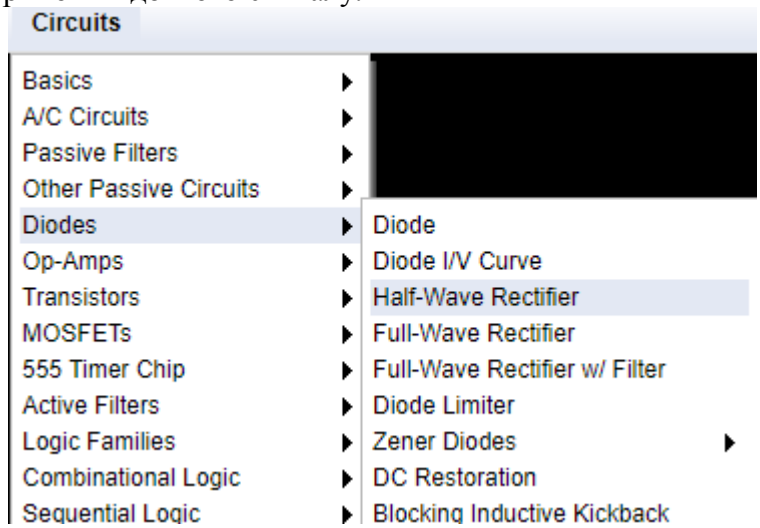
Порядок виконання роботи

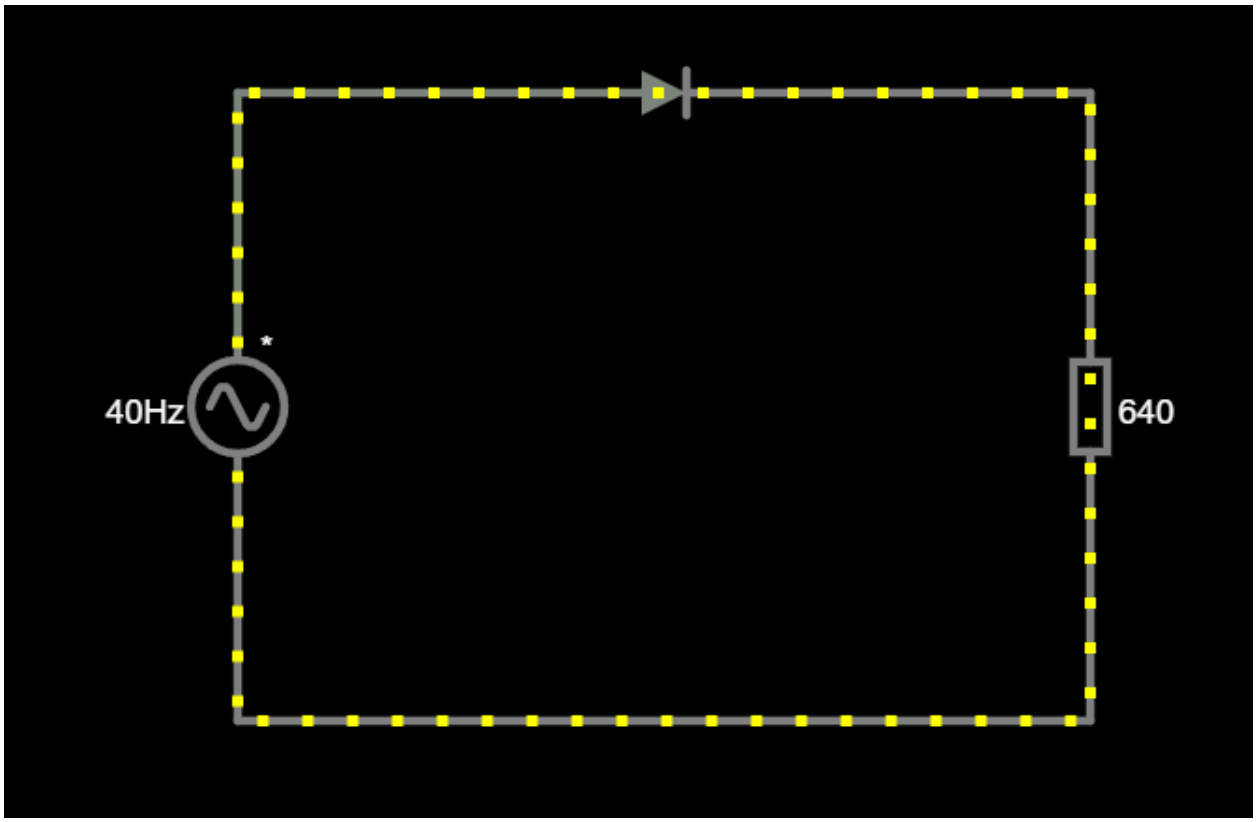
1. Ознайомитись із характеристиками і порядком експлуатації ЛНП EDD-24T:
   https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/lokator-nelinijnix-perexodiv-edd-24t/
   https://www.jjndigital.com/products/edd-24t/
2. Ознайомитись із характеристиками ряду ЛНП, наприклад:
   https://www.selcomsecurity.com/en/products/data-leakage-channels-detection/non-linear-junction-detectors
   https://www.spyshopeurope.com/en/non-linear-junction-detectors/151

3. Скласти порівняльну таблицю характеристик 3-х ЛНП, які на ваш погляд, мають краще співвідношення ціна/якість. Розкрити, що можна розуміти під поняттям “якість” для ЛНП.
4. Через браузер увійти до онлайн середовища моделювання електричних схем Circuit Simulator (https://www.falstad.com/circuit/circuitjs.html), виконати лабораторне дослідженя
5. Обрати в меню File - New Blank Circuit порожнє полотно моделювання.

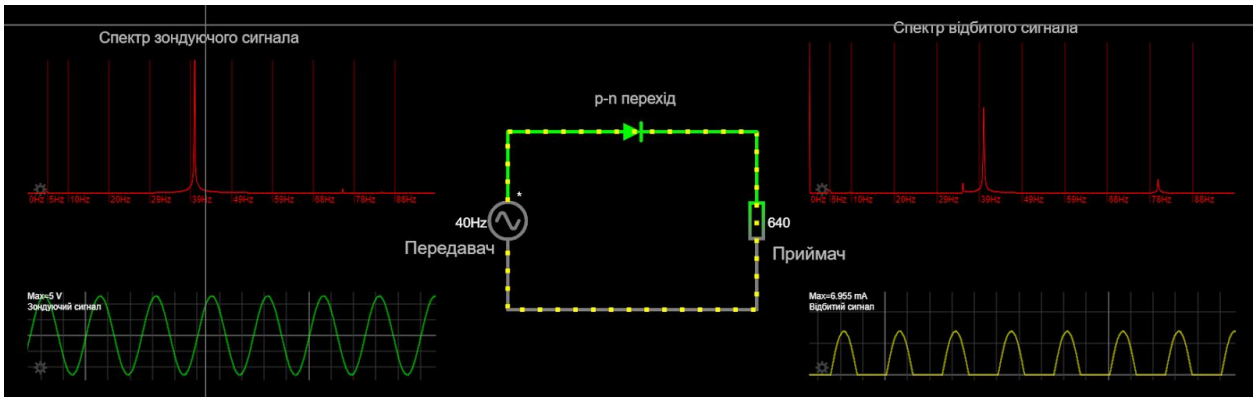


6. Вибрати в меню Circuits - Diodes - Half-Wave Rectifier електричну схему, що еквівалентна роботі НЛ при опроміненні нелінійних електричних елементів (p-n переходів) і прийомі відбитого сигналу.





7. Вивести на схемі часові і спектральні діаграми зондуючого і відбитого сигналів.



8. Пояснити принцип виявлення нелінійних переходів за допомогою аналізатора спектра.
9. Скласти звіт, в якому:
   - привести завдання для лабораторної роботи;
   - навести результати експериментів відповідно до завдання;
   - зробити висновки;
   - відповісти на контрольні питання.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою обговорення навчальних та контрольних питань, аналізу отриманих результатів виконання лабораторної роботи.

Контрольні питання

1. Наведіть визначення нелінійного елемента і назвіть кілька видів нелінійних об'єктів.
2. У чому полягає принцип нелінійної локації?
3. Чому у відбитому сигналі від нелінійного елемента з p-n-переходом переважає друга гармоніка?

4. Як залежить потужність сигналу, відбитого від об'єкта, від частоти локатора?

Рекомендовані джерела

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.

Тема № 15 Методики оцінки ефективності захищеності інформації від витоку акустичними каналами.

Лабораторна робота «Спектральне представлення акустичних сигналів»

Час проведення: 6 год. Місце проведення: комп'ютерний клас.

Навчальна мета заняття: Вивчити принцип спектрального представлення акустичних сигналів, способи демодуляції акустичних сигналів, дослідити спектр акустичних сигналів в області низьких частот і методи захисту інформації від витоку. Змоделювати реконструкцію сигналу типу меандр через суму гармонічних складових для усвідомлення суті спектрального представлення акустичних сигналів.

Навчальні питання:

1. Вимоги до вимірювальної лабораторії.
2. Вимірювання в області акустики.
3. Вимірювання вібрацій (віброприскорень).
4. Вимірювання електричних сигналів.
5. Вибір засобів вимірювання у ВЧ області.
6. Вимірювання електромагнітного поля.

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

План проведення заняття:

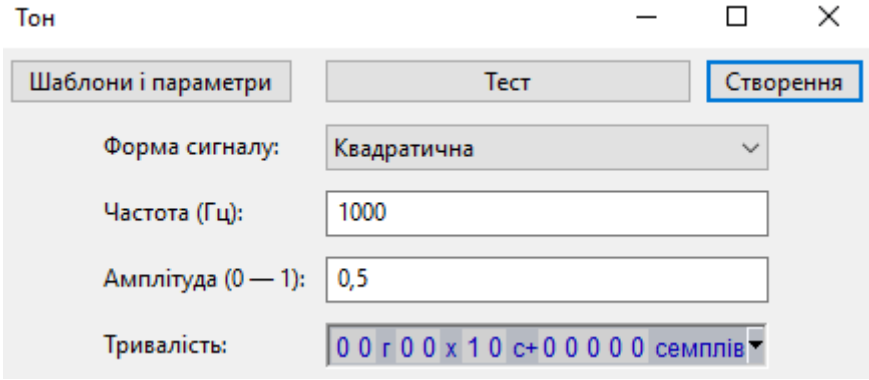
І. Порядок проведення вступу до заняття.

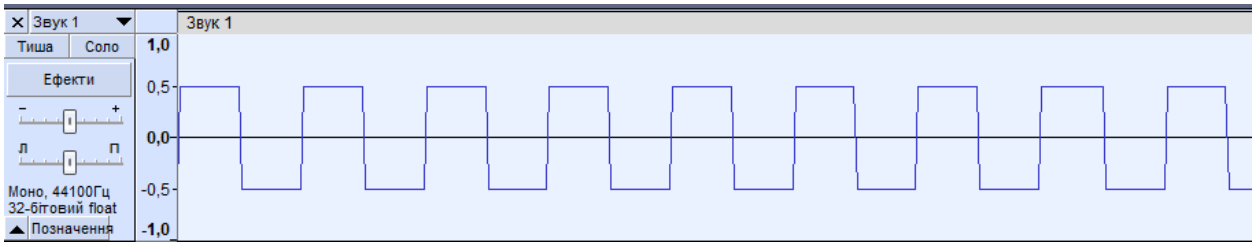
1. Поняття спектральної густини акустичного сигналу. Спектральний Фур'є-аналіз неперіодичних сигналів.

ІІ. Основна частина

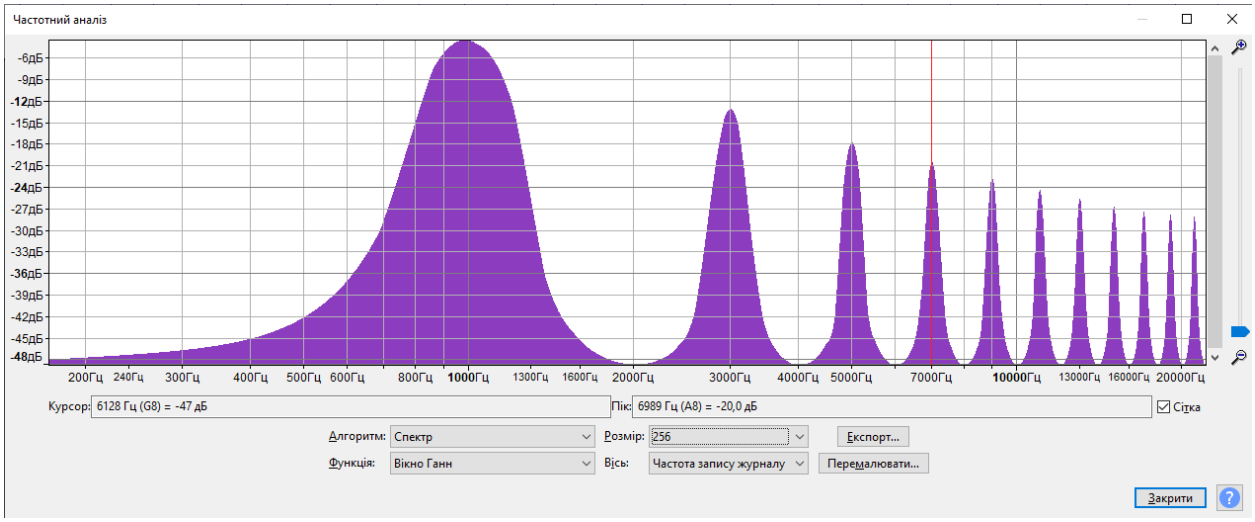
Порядок виконання роботи

1. Встановити звуковий редактор Audacity. (https://www.audacityteam.org/download/windows/)
2. Через меню Створення - Тон створити квадратичний сигнал з параметрами f=1 КГц, Am=0,5, t=30 с. Прослухати акустичний сигнал.





3. Виділити сигнал і через меню Аналіз побудувати графік спектра з параметрами як на рисунку.



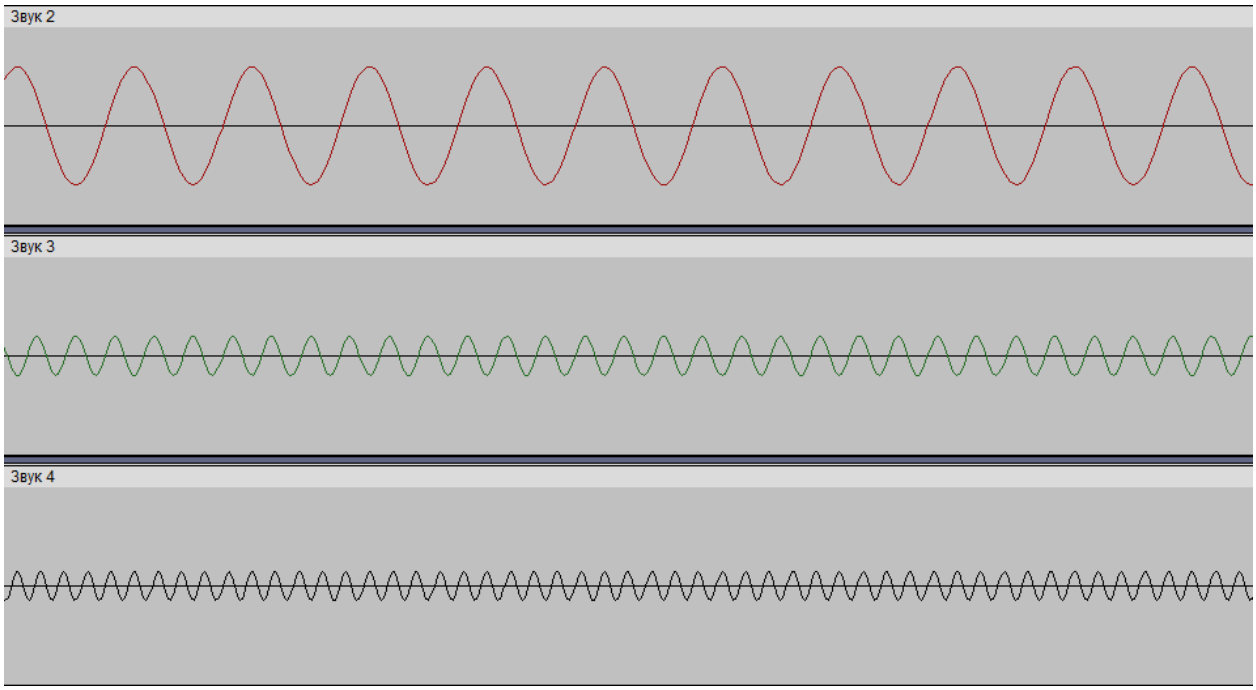
4. Експортувати числові значення спектру у текстовий файл, який далі імпортувати у таблицю MS Excel. Обчислити параметри перших чотирьох спектральних складових і записати в таблицю.

№ гармоніки	**1**	**3**	**5**	**7**
Частота, Гц	1000	3000	5000	7000
Амплітуда гармонік , дБ				
Відносні амплітуди гармонік	0,6			

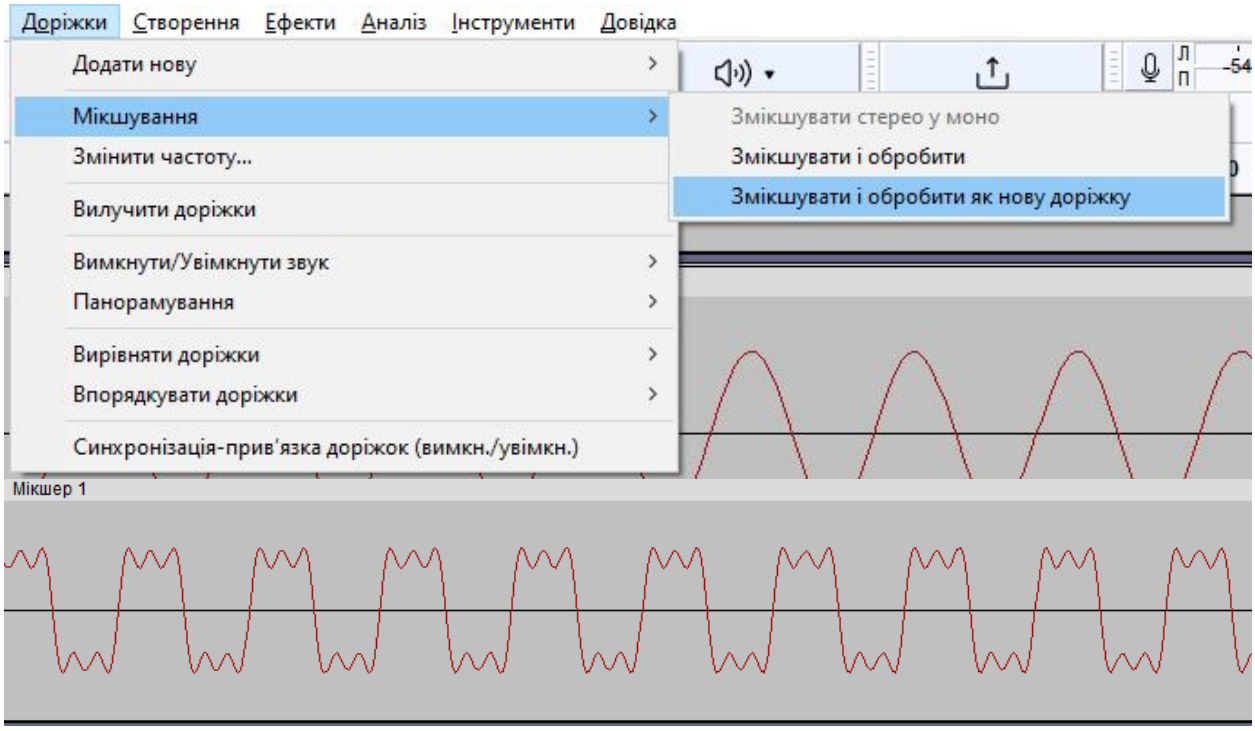
5. Для амплітуд сигналу перехід від логарифмічної шкали (дБ) в лінійну обчислюється із виразів:

$$L=20lgPP0\ [дБ],\ PP0=10L/20$$

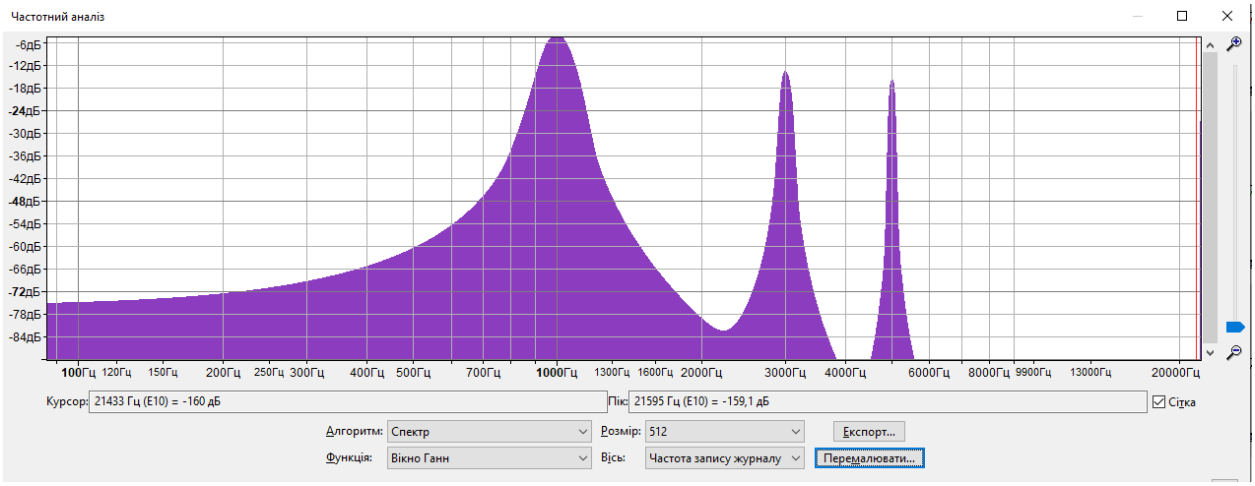
6. В Audacity створити окремі гармоніки з частотами 1, 3, 5, 7 КГц і відповідними обчисленими амплітудами. Окремо відтворити їх через акустичні системи.



7. Через меню “Доріжки - Мікшування - Змікшувати і обробити як нову доріжку” створити новий сигнал. Порівняти створений сигнал із вихідним. Відтворити його через акустичну систему.



8. Побудувати графік спектру створеного сигналу, експортувати його в MS Excel та порівняти графічно зі спектром вихідного сигналу.



9. Зробити висновки щодо частотного (спектрального) представлення акустичних сигналів.

III. Заключна частина заняття

Результати заняття узагальнюються за допомогою обговорення навчальних питань та аналізу отриманих результатів виконання лабораторної роботи.

Рекомендовані джерела

5. 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.
6. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
7. 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.
8. 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.