МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО - КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна наукова праця
На правах рукопису

ЦМОКАНИЧ ІВАН ВОЛОДИМИРОВИЧ

УДК 004.056.5: 621.391.825 (043.3)

ДИСЕРТАЦІЯ

МЕТОДИ ТА АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

Спеціальність 125 «Кібербезпека»
Галузь знань 12 «Інформаційні технології»
Подається на здобуття наукового ступеня
доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____І.В. Цмоканич
(підпис)

Науковий керівник: КРЮЧКОВА Лариса Петрівна, доктор технічних наук, професор.

Електронний підпис
ЦМОКАНИЧ
ІВАН
ВОЛОДИМИРОВИЧ
Ідентифікаційний
код
3525009750
Підписано у Вчасно

Київ – 2023

АНОТАЦІЯ

Цмоканич І.В. Методи та алгоритми захисту інформації від високочастотного нав’язування – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека». – Державний університет інформаційно-комунікаційних технологій Міністерства освіти і науки України, Київ, 2023.

У дисертаційній роботі вирішується актуальне науково-технічне завдання щодо розробки методів та алгоритмів захисту інформації від високочастотного нав’язування.

Розвиток та постійне вдосконалення способів перехоплення інформації з обмеженим доступом, яка є основою для функціонування критично важливих державних систем, збільшення частки інформації з обмеженим доступом в інформаційному просторі, постійне розширення та вдосконалення загальних практик захисту інформації з обмеженим доступом вимагає проведення досліджень щодо розробки нового методу захисту інформації від витоку каналами високочастотного нав’язування.

Для досягнення поставленої мети в роботі потрібно вирішити наступні окремі завдання дослідження:

1. Проаналізувати сучасний стан захищеності інформації від витоку каналами високочастотного нав’язування на обєктах інформаційної діяльності та критичної інфраструктури.

2. Дослідити сучасні методи та способи захисту інформації від витоку каналами високочастотного нав’язування.

3. Розробити модель блокування перехоплення інформації, яка забезпечує руйнацію інформативних параметрів небезпечних сигналів, сформованих високочастотним нав’язуванням.

4. Розробити модель захисту інформації, яка забезпечує пошук оптимальних параметрів ефективних завадових захисних сигналів, здатних

забезпечити руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування на основній частоті та комбінаційних гармоніках зондуючого сигналу.

5. Експериментально перевірити достовірність розроблених моделей та методу захисту інформації від витоку каналами високочастотного нав’язування.

6. Розробити модель розрахунку коефіцієнту захищеності інформації від небезпечних сигналів високочастотного нав’язування

7. Розробити методику захисту інформації від небезпечних сигналів високочастотного нав’язування.

8. Провести оцінку ефективності впливу захисних сигналів на небезпечні сигнали високочастотного нав’язування, в якій використано інформаційно-ентропійний критерій якості приймання радіосигналів.

Об'єктом дослідження є процес захисту інформації від витоку каналами, утвореними методом високочастотного нав’язування.

Предметом дослідження є методи та алгоритми захисту інформації від високочастотного нав’язування.

Методи досліджень ґрунтуються на використанні теорії ймовірностей, параметричної ідентифікації систем, спектрального оцінювання, методів цифрової обробки сигналів, кореляційного аналізу, математичного аналізу, лінійної алгебри, математичного та комп'ютерного моделювання, а також теоретичних основ статистичної радіотехніки.

Вірогідність наукових результатів, висновків та рекомендацій, викладених у дисертаційній роботі, обґрунтовано коректним використанням математичного апарату та моделюванням на ЕОМ, збігом результатів теоретичних досліджень з результатами моделювання та лабораторних експериментів.

Наукова новизна одержаних результатів. У процесі теоретичних і експериментальних досліджень та моделювання одержано наступні нові наукові результати:

1. Вперше запропоновано модель блокування процесу перехоплення інформації каналами високочастотного нав'язування, яка на основі процесу суперпозиції близьких по частоті гармонічних коливань дозволяє забезпечити ефект «биття» частот шляхом руйнування інформативних параметрів небезпечних сигналів і блокує витік інформації каналами високочастотного нав'язування.

2. Удосконалено модель захисту інформації від витоку каналами високочастотного нав'язування, яка, на відміну від існуючих, побудована на основі навмисного «качання» частоти і забезпечує руйнування інформативних параметрів небезпечних сигналів високочастотного нав'язування не тільки на основній частоті, а й на комбінаційних гармоніках небезпечного зондуючого сигналу.

3. Удосконалено модель розрахунку коефіцієнта оцінки захищеності інформації, яка, на відміну від існуючих, побудована на основі порівняння енергетичних складових, виміряних в смугах, достатніх для перехоплення, небезпечних та захисних сигналів і забезпечує кількісну оцінку захищеності на основі встановленого значення коефіцієнта з врахуванням параметрів та значень небезпечного зондуючого сигналу.

4. Вперше розроблено метод захисту інформації від витоку каналами високочастотного нав'язування, який базується на основі алгоритму блокування та руйнування інформативних параметрів небезпечного сигналу високочастотного нав'язування, що забезпечує захист інформації по заданих значеннях коефіцієнта захищеності.

Практичне значення одержаних результатів у галузі розробки та створення ефективних методів захисту інформації від витоку каналами високочастотного нав'язування полягає в наступному:

Запропоновані моделі та методи можуть бути використані дослідно-конструкторськими організаціями та державними структурами при розробці та удосконаленні оцінки захищеності інформації під час проведення інструментального контролю різнотипних об'єктів інформаційної діяльності

критичної інфраструктури та вирішення комплексних проблем щодо захисту інформації на об’єктах інформаційної діяльності критичної інфраструктури.

Дисертаційна робота складається з вступу, чотирьох розділів в яких логічно, на високому науково-технічному рівні викладено рішення поставлених задач дослідження.

В першому розділі проведено аналіз сучасного стану проблеми перехоплення інформації методами високочастотного нав’язування. Проведено аналітичний огляд відомих технічних рішень захисту інформації від витоку каналами високочастотного нав’язування. У прикінцевій частині першого розділу, враховуючи проведений аналіз та виявлені проблеми, сформовано цілі та завдання дослідження.

В другому розділі проведено синтез активного методу захисту інформації від витоку каналами високочастотного нав’язування. Проаналізовано принципи блокування перехоплення інформації методами високочастотного нав’язування. Досліджено основні проблеми захисту інформації з обмеженим доступом від витоку та обґрунтовано використання активного методу захисту інформації від витоку каналами високочастотного нав’язування. Проаналізовано теоретичну ефективність використання вищевказаного методу в порівнянні з іншими методами та здійснено визначення основних критеріїв проведення імітаційних та експериментальних досліджень задля доведення ефективності методу. Отримані у другому розділі результати дозволяють укрупнено оцінити ефективність використання активного методу захисту інформації від витоку каналами високочастотного нав’язування.

В третьому розділі подано моделі і методи імітаційних досліджень для визначення параметрів захисних сигналів та ефективності використання активного методу захисту інформації від витоку каналами високочастотного нав’язування. Здійснено дослідження моделей і методів забезпечення захисту інформації від витоку каналами високочастотного нав’язування. Проведено математичне моделювання в середовищі MathCad 14 та визначено

оптимальний діапазон значень захисних сигналів для забезпечення ефективного захисту інформації від перехоплення. На основі теоретичних відомостей та математичного моделювання в середовищі MathCad 14 проведено імітаційні дослідження з використанням пакету LabVIEW версії 20.0.1. Дослідження проводились за робочими блок-схемами, що складаються з трьох основних частин: група генераторів, що в сумі сигналів генерують небезпечний сигнал; група генераторів, що в сумі сигналів генерують захисний сигнал; група контрольних пристроїв для спостереження за сигналами. Зроблено висновки проведення імітаційних досліджень та сформовано основні завдання та критерії проведення експериментальних досліджень ефективності використання активного методу захисту інформації від витоку каналами високочастотного нав’язування.

Четвертий розділ присвячено проведенню експериментальних досліджень. Сформовано задачі, які стали основою для проведення експериментальних досліджень. Проаналізовано теоретичні відомості, математичне моделювання та імітаційні дослідження, на основі отриманих даних розроблено методику та програму проведення експериментальних досліджень. Проведено аналіз наявних та визначено оптимальні схеми і апаратні засоби для проведення експериментальних досліджень. Під час проведення експериментальних досліджень визначено основні параметри захисних сигналів, які здатні забезпечувати ефективніший захист інформації від витоку каналами високочастотного нав’язування. При проведенні експериментальних досліджень встановлено основні критерії, які забезпечують максимальну ефективність методу задля захисту інформації від витоку.

Ключові слова: перехоплення інформації, метод високочастотного нав'язування, зондувальний сигнал, небезпечний сигнал, завадовий захисний сигнал, параметри захисних сигналів.

ANNOTATION

Tsmokanych I.V. Methods and algorithms for protecting information from high-frequency interference - Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 - "Cyber Security". - State University of Information and Communication Technologies of the Ministry of Education and Science of Ukraine, Kyiv, 2023.

The thesis solves the current scientific and technical task of developing methods and algorithms for protecting information from high-frequency interference.

The development and continuous improvement of methods of interception of information with limited access, which is the basis for the functioning of critically important state systems, the increase of the share of information with limited access in the information space, the constant expansion and improvement of general practices for the protection of information with limited access require conducting research on the development of a new method of protection information from leakage through channels of high-frequency imposition.

In order to achieve the set goal in the work, it is necessary to solve the following separate research tasks:

1. To analyze the current state of information security against leakage through high-frequency interference channels on objects of information activity and critical infrastructure.

2. To study modern methods and ways of protecting information from leakage through channels of high-frequency imposition.

3. To develop a model of blocking the interception of information, which ensures the destruction of informative parameters of dangerous signals formed by high-frequency imposition.

4. To develop an information protection model that ensures the search for optimal parameters of effective interference protective signals capable of destroying

the informative parameters of dangerous signals of high-frequency imposition on the fundamental frequency and combinational harmonics of the probing signal.

5. Experimentally verify the reliability of the developed models and the method of information protection against leakage through channels of high-frequency imposition.

6. Develop a model for calculating the information security factor against dangerous high-frequency interference signals

7. Develop a method of protecting information from dangerous high-frequency interference signals.

8. To evaluate the effectiveness of the impact of protective signals on dangerous signals of high-frequency interference, in which the information-entropy criterion of the quality of reception of radio signals is used.

The object of the research is the process of protecting information from leakage through channels formed by the method of high-frequency imposition.

The subject of research are methods and algorithms for protecting information from high-frequency imposition.

Research methods are based on the use of probability theory, parametric identification of systems, spectral estimation, methods of digital signal processing, correlation analysis, mathematical analysis, linear algebra, mathematical and computer modeling, as well as theoretical foundations of statistical radio engineering.

The plausibility of the scientific results, conclusions and recommendations presented in the dissertation is substantiated by the correct use of mathematical apparatus and computer simulations, the coincidence of the results of theoretical studies with the results of simulations and laboratory experiments.

Scientific novelty of the obtained results. In the process of theoretical and experimental research and modeling, the following new scientific results were obtained:

1. For the first time, a model of blocking the process of interception of information by channels of high-frequency imposition is proposed, which, based on

the process of superposition of harmonic oscillations close in frequency, allows to ensure the effect of «beating» frequencies by destroying the informative parameters of dangerous signals and blocks the leakage of information through channels of high-frequency imposition.

2. The model of information protection against leakage through high-frequency interference channels has been improved, which, unlike the existing ones, is built on the basis of intentional frequency «swinging» and ensures the destruction of the informative parameters of dangerous high-frequency interference signals not only on the main frequency, but also on combination harmonics of a dangerous probing signal.

3. The model for calculating the information security assessment coefficient has been improved, which, unlike the existing ones, is built on the basis of a comparison of the energy components measured in the bands sufficient for interception of dangerous and protective signals and provides a quantitative assessment of security based on the established value of the coefficient, taking into account the parameters and values of the dangerous probing signal.

4. For the first time, a method of protecting information from leakage through high-frequency jamming channels was developed, which is based on the algorithm of blocking and destroying informative parameters of a dangerous high-frequency jamming signal, which ensures information protection according to the given values of the security factor.

The practical significance of the obtained results in the field of development and creation of effective methods of information protection against leakage through channels of high-frequency imposition is as follows:

The proposed models and methods can be used by research and development organizations and state structures in the development and improvement of information security assessment during the instrumental control of various objects of information activity of critical infrastructure and solving complex problems regarding information protection at objects of information activity of critical infrastructure.

The dissertation consists of an introduction, four chapters in which logically, at a high scientific and technical level, the solutions to the research problems are presented.

In the first chapter, an analysis of the current state of the problem of interception of information by methods of high-frequency imposition is carried out. An analytical review of known technical solutions for information protection against leakage through high-frequency interference channels was conducted. In the final part of the first chapter, taking into account the conducted analysis and identified problems, the goals and tasks of the research are formed.

In the second section, a synthesis of an active method of information protection against leakage through high-frequency imposition channels is carried out. The principles of blocking interception of information by methods of high-frequency imposition are analyzed. The main problems of protecting confidential information from leakage have been studied and the use of an active method of protecting information from leakage through high-frequency imposition channels has been substantiated. The theoretical effectiveness of using the above-mentioned method in comparison with other methods was analyzed and the main criteria for conducting simulation and experimental studies were determined in order to prove the effectiveness of the method. The results obtained in the second section make it possible to comprehensively assess the effectiveness of using an active method of protecting information against leakage through high-frequency imposition channels.

The third section presents models and methods of simulation studies for determining the parameters of protective signals and the effectiveness of using an active method of protecting information against leakage through high-frequency imposition channels. A study of models and methods of ensuring information protection against leakage through high-frequency imposition channels was carried out. Mathematical modeling was carried out in the MathCad 14 environment and the optimal range of values of protective signals was determined to ensure effective protection of information from interception. On the basis of theoretical information and mathematical modeling in the MathCad 14 environment, simulation studies

were carried out using the LabVIEW version 20.0.1 package. The research was carried out according to working block diagrams consisting of three main parts: a group of generators that, in the sum of the signals, generate a dangerous signal; a group of generators that in the sum of signals generate a protective signal; a group of control devices for monitoring signals. The conclusions of simulation studies were drawn, and the main tasks and criteria for conducting experimental studies of the effectiveness of using an active method of protecting information against leakage through high-frequency imposition channels were formed.

The fourth chapter is devoted to experimental research. Tasks were formed, which became the basis for conducting experimental research. Theoretical information, mathematical modeling and simulation studies were analyzed, and a methodology and program for conducting experimental studies was developed based on the obtained data. An analysis of the existing and optimal schemes and hardware for conducting experimental research was determined. During experimental studies, the main parameters of protective signals were determined, which are able to provide more effective protection of information against leakage through channels of high-frequency imposition. When conducting experimental research, the main criteria are established that ensure the maximum effectiveness of the method for protecting information from leakage.

Key words: interception of information, method of high-frequency imposition, probing signal, dangerous signal, interfering protective signal, parameters of protective signals.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у закордонних фахових виданнях, які включені до інших наукометричних баз даних

1. Larysa Kriuchkova, & Ivan Tsmokanych. (2021). Overview of methods of protection of acoustic information against leaks by channels formed by high-frequency impositions. *International Journal of Innovative Technologies in Social Science*, 3(31).

https://doi.org/10.31435/rsglobal_ijitss/30092021/7685

Статті у фахових виданнях, що входять до переліку, затвердженого МОН України

2. Крючкова, Л., Цмоканич І., Вовк. М. (2022). Удосконалений метод захисту конфіденційної інформації від перехоплення методами високочастотного нав'язування. *Computer Systems and Information Technologies*, 2021, № 3, с. 14–20.

https://doi.org/10.31891/CSIT-2021-5-2.

3. Крючкова, Л., & Цмоканич, І. (2022). Методичні аспекти визначення параметрів захисних впливів на зондувальні сигнали високочастотного нав'язування. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2(18), с. 197–204.

https://doi.org/10.28925/10.28925/2663-4023.2022.18.197204.

4. Крючкова, Л., & Цмоканич, І. (2023). Удосконалення захисних впливів на небезпечні сигнали високочастотного нав'язування. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 3(19), с. 243–253.

https://doi.org/10.28925/2663-4023.2023.19.243253.

Матеріали й тези доповідей на конференціях

5. Larysa Kriuchkova, Maksym Vovk, Ivan Tsmokanych, and Denys Tarasenko. Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition, *CEUR Workshop Proceedings CPITS-II-2 2021*, pp. 265-272. (**Scopus**)

https://ceur-ws.org/Vol-3188/short9.pdf.

6. Larysa Kriuchkova, Ivan Tsmokanych, Svitlana Shevhenko, Oleksandr Bohdanov, and Nataliia Mazur. Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, *CEUR Workshop Proceedings CPITS-II-2 2023*, pp. 261-268. (**Scopus**)

https://ceur-ws.org/Vol-3550/short10.pdf.

7. Л.П. Крючкова, І.В. Цмоканич / Удосконалений метод захисту інформації від перехоплення методом високочастотного нав'язування // Науково-практична інтернет-конференція «Цифрова трансформація кібербезпеки». – Державний університет телекомунікацій. Навчально-науковий інститут захисту інформації, 2020. – С. 146 – 149.

https://duikt.edu.ua/uploads/n_9126_17047934.pdf?file=n_9126_17047934.pdf

8. Л.П. Крючкова, І.В. Цмоканич / Удосконалений метод захисту інформації від витоку каналами високочастотного нав'язування// Комп'ютерні системи та мережні технології: XIII Міжнародна науково-практична конференція - Національний авіаційний університет.–Київ, 2021. – С. 62–63. https://er.nau.edu.ua/handle/NAU/50696;

9. Л.П. Крючкова, І.В. Цмоканич / Захист інформації від високочастотного нав'язування на об'єктах критичної інфраструктури // IV Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)" – Київський національний університет імені Тараса Шевченка. – Київ, 2021. – С. 37 – 38.

10. Л.П. Крючкова, І.В. Цмоканич // XII Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» - Національна академія Служби безпеки України. – Київ, 2021. – С. 227 – 229.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ……. 16
ВСТУП……..... 17
РОЗДІЛ 1. АНАЛІЗ ПРОЦЕСУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ.. 24
1.1. Аналіз основних принципів дії методу високочастотного нав'язування…….. 24
1.2. Аналіз технологій перехоплення інформації методами високочастотного нав'язування…….. 27
1.3. Аналітичний огляд відомих технічних рішень захисту інформації від витоку каналами високочастотного нав'язування…….. 33
1.4. Постановка наукового завдання……... 39
Висновки до розділу 1……. 40
РОЗДІЛ 2. СИНТЕЗ АКТИВНОГО МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ…… 42
2.1. Загальна постановка задачі дослідження……... 42
2.2. Розробка моделі блокування перехоплення інформації методами високочастотного нав'язування……..... 49
2.3. Розробка моделі і методу захисту інформації інформації від витоку каналами високочастотного нав'язування……..…..... 60
Висновки до розділу 2……. 72
РОЗДІЛ 3. СИНТЕЗ МОДЕЛЕЙ І МЕТОДІВ ІМІТАЦІЙНИХ ДОСЛІДЖЕНЬ …… 73
3.1. Розробка моделі і методики дослідження параметрів завадових сигналів шляхом математичного та імітаційного моделювання ……. 73
3.2. Удосконалення моделі оцінки оптимальних параметрів захисних сигналів шляхом експериментальних досліджень……. 83
Висновки до розділу 3……. 92

РОЗДІЛ 4 ПРОВЕДЕННЯ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ПАРАМЕТРІВ ЗАВАДОВИХ ЗАХИСНИХ СИГНАЛІВ..... 94
4.1. Постановка задач і розробка методик експериментальних досліджень …….……... 94
4.1.1. Розробка програми і методики експериментальних досліджень параметрів захисних сигналів……. 96
4.1.2. Розробка програми і методики експериментальних досліджень оцінки ефективності завадових захисних сигналів……...…….. 103
4.2. Опис схеми і апаратних засобів для проведення експериментальних досліджень…….. 108
4.2.1. Опис схеми і апаратних засобів для проведення експериментальних досліджень параметрів захисних сигналів…….. 108
4.2.2. Опис схеми і апаратних засобів для проведення експериментальних досліджень оцінки ефективності завадових захисних сигналів…… 112
4.3. Проведення експериментальних досліджень параметрів захисного сигналу…….. 116
4.3.1. Визначення різниці частот між захисним та небезпечним сигналами…….. 116
4.3.2. Дослідження впливу зміни фази захисного сигналу на захищеність інформації……... 121
4.4. Експериментальна оцінка ефективності завадових захисних сигналів……. 125
4.5. Визначення коефіцієнту захищеності інформації від витоку та можливості відтворення……... 127
Висновки до розділу 4……. 132
ВИСНОВКИ…….. 134
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ……. 137
Додаток А……...……..... 149

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Високочастотне «нав’язування»	ВЧН
Високочастотні сигнали	ВЧ-сигнали
Високочастотні завади	ВЧ-завади
Основні технічні засоби і системи	ОТЗС
Допоміжні технічні засоби і системи	ДТЗС
Амплітудно-модульовані коливання	АМ коливання
Частотно-модульовані коливання	ЧМ коливання
Фазово-модульовані коливання	ФМ коливання
Електромагнітна сумісність	ЕМС
Контрольована зона	КЗ
Технічні засоби приймання, обробки, зберігання та передання інформації	ТЗПІ

ВСТУП

Актуальність теми дослідження. В умовах глобальної інформатизації суспільства реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій. У загальній проблемі забезпечення безпеки інформації питання захисту інформації з обмеженим доступом є одним із найважливіших. Це пояснюється, зокрема, тим, що частка такої інформації в загальному інформаційному потоці являє собою значну частину.

Захист інформації з обмеженим доступом став одним із головних пріоритетів державної політики, у тому числі й у нашій країні. Віднесення інформації до категорії з обмеженим доступом та її засекречування є важливою складовою теорії і практики захисту інформації.

Перехоплення інформації, яка обробляється на об'єктах інформаційної діяльності, може здійснюватись шляхом спеціальних впливів на елементи технічних засобів.

Одним із активних способів перехоплення інформації є метод високочастотного нав'язування (ВЧН), який може бути здійснений шляхом подання струмів на основних та комбінаційних гармоніках високої частоти від відповідного генератора системи перехоплення інформації в нелінійні та (чи) параметричні кола ОТЗС та ДТЗС, в яких є присутнім з тих або інших причин небезпечний сигнал, і одночасного прийому (виявлення) промодульованих небезпечним сигналом струмів високої частоти за допомогою узгодженого за технічними характеристиками з генератором і іншими компонентами взаємодіючих систем оптимального приймаючого пристрою.

Таким чином, у зв’язку з потребою захисту інформації від витоку каналами ВЧН та постійним удосконаленням технологій перехоплення інформації, потрібно розробка нового методу захисту інформації від витоку каналами ВЧН, який буде впливати на сформовані високочастотним нав'язуванням небезпечні сигнали на основних та комбінаційних гармоніках

для забезпечення максимально можливої руйнації їх інформативних параметрів і, як результат, надійного блокування каналів витоку інформації.

Методи та алгоритми захисту інформації від високочастотного нав'язування, що описані в попередніх роботах, не враховують можливість перехоплення інформації на бічних гармоніках небезпечного сигналу, відповідно рішень щодо захисту інформації від перехоплення не тільки на основних, а й на бічних гармоніках сигналу.

При вирішенні визначеної в дисертаційній роботі проблеми автор у своїх дослідженнях спирався на праці вітчизняних вчених, які зробили значний внесок у розвиток теорії побудови методів та алгоритмів захисту інформації від високочастотного нав'язування. А саме: Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.

Аналіз наукових досліджень вітчизняних вчених показав, що завданням підвищення ефективності захисту інформації від витоку каналами високочастотного нав'язування шляхом унеможливлення перехоплення на всіх гармоніках небезпечного сигналу, яке б враховувало всі особливості параметрів сигналів, можливості блокування та руйнування сигналів не приділяється достатньої уваги. На підставі цього можна стверджувати, що, по суті, формується нове наукове завдання щодо розробки методу захисту інформації від високочастоного нав'язування як на основних, так і на бічних гармоніках сигналу.

Розв'язання вказаного завдання передбачає проведення наукових досліджень та розробку на їх основі методів та алгоритмів підвищення ефективності захиту інформації від високочастотного нав'язування, що визначило мету та зміст даної дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження відповідає вимогам статті 5 Закону України «Про пріоритетні напрями розвитку науки і техніки» від 11 липня 2001 рок № 2623-III (зі змінами та доповненнями від 29.01.2021 р.), пункту першого розділу другого «Переліку пріоритетних тематичних напрямів наукових досліджень і

науково-технічних розробок на період до 2021 року», затвердженого Постановою КМУ від 7 вересня 2011 р. № 942.

Метою дисертаційної роботи є підвищення ефективності захисту інформації від витоку каналами високочастотного нав’язування.

Для досягнення поставленої мети в роботі потрібно вирішити наступні окремі завдання дослідження:

1. Проаналізувати сучасний стан захищеності інформації від витоку каналами високочастотного нав’язування на обєктах інформаційної діяльності та критичної інфраструктури.
2. Дослідити сучасні методи та способи захисту інформації від витоку каналами високочастотного нав’язування.
3. Розробити модель блокування перехоплення інформації, яка забезпечує руйнацію інформативних параметрів небезпечних сигналів, сформованих високочастотним нав’язуванням.
4. Розробити модель захисту інформації, яка забезпечує пошук оптимальних параметрів ефективних завадових захисних сигналів, здатних забезпечити руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування на основній частоті та комбінаційних гармоніках зондуючого сигналу.
5. Експериментально перевірити достовірність розроблених моделей та методу захисту інформації від витоку каналами високочастотного нав’язування.
6. Розробити модель розрахунку коефіцієнту захищеності інформації від небезпечних сигналів високочастотного нав’язування
7. Розробити методику захисту інформації від небезпечних сигналів високочастотного нав’язування.
8. Провести оцінку ефективності впливу захисних сигналів на небезпечні сигнали високочастотного нав’язування, в якій використано інформаційно-ентропійний критерій якості приймання радіосигналів.

Об'єктом дослідження є процес захисту інформації від витоку

каналами, утвореними методом високочастотного нав’язування.

Предметом дослідження є методи та алгоритми захисту інформації від високочастотного нав’язування.

Методи досліджень ґрунтуються на використанні теорії ймовірностей, параметричної ідентифікації систем, спектрального оцінювання, методів цифрової обробки сигналів, кореляційного аналізу, математичного аналізу, лінійної алгебри, математичного та комп'ютерного моделювання, а також теоретичних основ статистичної радіотехніки.

Вірогідність наукових результатів, висновків та рекомендацій, викладених у дисертаційній роботі, обґрунтовано коректним використанням математичного апарату та моделюванням на ЕОМ, збігом результатів теоретичних досліджень з результатами моделювання та лабораторних експериментів.

Наукова новизна одержаних результатів. У процесі теоретичних і експериментальних досліджень та моделювання одержано наступні нові наукові результати:

1. Вперше запропоновано модель блокування процесу перехоплення інформації каналами високочастотного нав’язування, яка на основі процесу суперпозиції близьких по частоті гармонічних коливань дозволяє забезпечити ефект «биття» частот шляхом руйнування інформативних параметрів небезпечних сигналів і блокує витік інформації каналами високочастотного нав’язування.

2. Удосконалено модель захисту інформації від витоку каналами високочастотного нав’язування, яка, на відміну від існуючих, побудована на основі навмисного «качання» частоти і забезпечує руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках небезпечного зондуючого сигналу.

3. Удосконалено модель розрахунку коефіцієнта оцінки захищеності інформації, яка, на відміну від існуючих, побудована на основі порівняння

енергетичних складових, виміряних в смугах, достатніх для перехоплення, небезпечних та захисних сигналів і забезпечує кількісну оцінку захищеності на основі встановленого значення коефіцієнта з врахуванням параметрів та значень небезпечного зондуючого сигналу.

4. Вперше розроблено метод захисту інформації від витоку каналами високочастотного нав'язування, який базується на основі алгоритму блокування та руйнування інформативних параметрів небезпечного сигналу високочастотного нав'язування, що забезпечує захист інформації по заданих значеннях коефіцієнта захищеності.

Практичне значення одержаних результатів у галузі розробки та створення ефективних методів захисту інформації від витоку каналами високочастотного нав'язування полягає в наступному:

Запропоновані моделі та методи можуть бути використані дослідно-конструкторськими організаціями та державними структурами при розробці та удосконаленні оцінки захищеності інформації під час проведення інструментального контролю різнотипних об'єктів інформаційної діяльності критичної інфраструктури та вирішення комплексних проблем щодо захисту інформації на об'єктах інформаційної діяльності критичної інфраструктури.

Особистий внесок здобувача. Наукові положення та результати дисертації отримані автором особисто. У опублікованих у співавторстві роботах автором дисертації зроблено такий особистий внесок. В [1] подано особисто отриманий аналіз відомих методів захисту інформації від витоку каналами високочастотного нав'язування. В [2] опубліковано особисто розроблену структуру моделі блокування каналів перехоплення інформації методами високочастотного «нав'язування», при якому в середовище, яке використовується для подачі зондуючого коливання, вводяться прицільні активні завадові захисні сигнали, спрямовані на руйнування інформативних параметрів небезпечних сигналів, що унеможливлює перехоплення мовленнєвої інформації. В [3] подано особисто встановлені методичні аспекти визначення параметрів захисних впливів на зондувальний сигнал для

забезпечення надійного блокування каналу витоку інформації. В [4] подано особисто розроблену структуру удосконалення захисних впливів на сформовані високочастотним нав'язуванням небезпечні сигнали для забезпечення максимально можливої руйнації їх інформативних параметрів і, як результат, надійного блокування каналів витоку інформації.

Апробація результатів дисертації. Основні положення і результати дисертації, практичні висновки і рекомендації, які одержані в ході роботи, апробовані та оприлюднені в ході: Науково-практичної інтернет-конференції «Цифрова трансформація кібербезпеки» – (Київ, Державний університет телекомунікацій, 2020), XIII міжнародної науково-практичної конференції «Комп’ютерні системи та мережні технології» – (Київ, Національний авіаційний університет, 2021), IV Міжнародної науково-практичної конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” (Київ, Київський національний університет імені Тараса Шевченка, 2021), XII Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави» - (Київ, Національна академія Служби безпеки України, 2021), Міжнародного семінару CEUR Workshop Proceedings CPITS-II-2 2021 (**Scopus**), Міжнародного семінару CEUR Workshop Proceedings CPITS-II-2 2023 (**Scopus**).

Публікації. Основні наукові положення та результати дисертаційного дослідження опубліковано в 4 наукових працях. У томи числі: у 1 науковій статті у закордонному фаховому виданні, яке включене до інших наукометричних баз даних, в 3 наукових статтях у періодичних виданнях України включених до “Переліку наукових фахових видань України”, тезах доповідей та матеріалах конференцій, опублікованих у 6 збірниках, в тому числі 2, які індексовані в науково-метричній базі **Scopus**.

Структура дисертації та її обсяг. Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків і має 136 сторінок основного тексту, 67 рисунків, 4 сторінки додатків. Список використаних джерел містить 92 найменування і займає 12 сторінок. Загальний обсяг дисертаційної роботи – 152 сторінки.

РОЗДІЛ 1
АНАЛІЗ ПРОЦЕСУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ’ЯЗУВАННЯ

1.1. Аналіз основних принципів дії методу високочастотного нав’язування

В умовах глобальної інформатизації суспільства реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій. У загальній проблемі забезпечення безпеки інформації питання захисту інформації з обмеженим доступом є одним із найважливіших [1-20]. Це пояснюється, зокрема, тим, що частка такої інформації в загальному інформаційному потоці являє собою значну частину. Захист інформації став одним із головних пріоритетів державної політики, у тому числі й у нашій країні. Віднесення інформації до категорії з
обмеженим доступом та її засекречування є важливою складовою теорії і практики захисту інформації [20-38].

В даний час відомо багато способів перехоплення інформації, серед яких є метод високочастотного «нав’язування».

Під високочастотним «нав'язуванням» розуміється спосіб несанкціонованого отримання інформації, при якому відбувається зондування радіосигналом приміщення і його струмопровідних комунікацій, в якому відбуваються переговори. В результаті взаємодії з технічними засобами або спеціально впровадженими пристроями відбувається модуляція зондуючих сигналів мовленнєвими. В колах технічних засобів, що знаходяться в зоні впливу високочастотних випромінювань, наводяться сигнали напруги до декількох вольт. Якщо в зазначених колах є елементи, параметри яких (індуктивність, ємність або опір) змінюються під дією низькочастотних сигналів, то в навколишньому просторі буде створюватися вторинне поле

високочастотного випромінювання, модульоване низькочастотним сигналом [39-43].

Високочастотне «нав’язування» (зондування) є дуже ефективним способом перехоплення інформації, що циркулює в апаратурі основних технічних засобів і систем (ОТЗС) або наводиться у допоміжних технічних засобах і системах (ДТЗС) за рахунок акустоелектричних перетворень, що утворюються при одночасному впливі на елементи технічних засобів мовленнєвих сигналів та зондуючого сигналу, якщо в останніх при їх розробці не було вжито радикальних заходів, що перешкоджають проникненню струмів високої частоти всередину цієї апаратури.

Високочастотне «нав’язування» є активним способом перехоплення інформації, який може бути здійснений шляхом подання струмів високої частоти від відповідного генератора системи перехоплення інформації в нелінійні та (чи) параметричні кола ОТЗС та ДТЗС, в яких є присутнім з тих або інших причин небезпечний сигнал, і одночасного прийому (виявлення) промодульованих небезпечним сигналом струмів високої частоти за допомогою узгодженого за технічними характеристиками з генератором і іншими компонентами взаємодіючих систем оптимального приймаючого пристрою.

В основі методу високочастотного «нав’язування» лежить використання фізичного явища відбиття енергії високої частоти від неузгодженого навантаження.

Під навантаженням розуміється повний опір якого-небудь нелінійного або параметричного кола, величина якого змінюється під впливом небезпечного сигналу згідно із законом, властивим цьому сигналу. Таким чином, навантаження може розглядатися як модулятор високочастотного коливання небезпечним сигналом. Подання на ОТЗС (у тому числі при одночасній дії акустичного поля мовленнєвих сигналів на ДТЗС) і знімання з них високочастотних коливань при застосуванні даного методу здійснюється за допомогою різноманітних ліній зв'язку, що відходять до ОТЗС і ДТЗС.

Лініями зв'язку можуть виступати лінії передачі (у симетричному і несиметричному режимах), кола електроживлення, заземлення, управління, сигналізації – так звані струмопровідні комунікації – і т.п., а також лінії, утворені паразитними зв'язками між різними колами ОТЗС, ДТЗС, конструктивними елементами будівель, споруд, устаткування.

Ефективність методу високочастотного «нав’язування» в загальному вигляді визначається як результат взаємодії наступних технічних систем:

- системи перехоплення інформації;
- системи передачі, обробки і зберігання інформації;
- системи (лінії) зв'язку.

Апріорні результати взаємодії цих систем можуть бути оцінені проведенням системного аналізу функціонування складної технічної системи, що складається з трьох вказаних складових частин [43].

Структурну схему каналу високочастотного «нав’язування» представлено на рис.1.

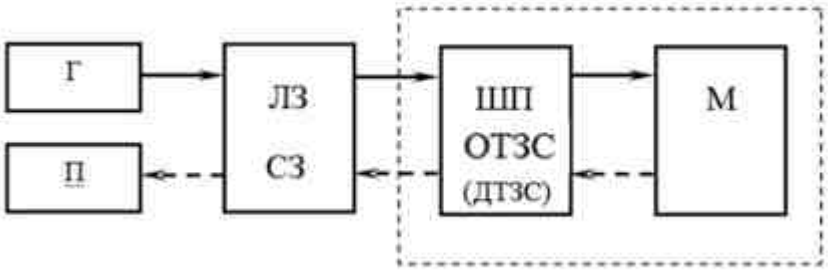


Рис.1.1. Структурна схема каналу високочастотного «нав’язування»

У представленій схемі зондуючий високочастотний сигнал, що виробляється в генераторі (Г), поступає через лінію (систему) зв'язку (ЛЗ, СЗ) на елементи ОТЗС чи ДТЗС. В ОТЗС може циркулювати (у режимі виконання ним основній функції) або впливати на нього (у режимі очікування або використання як ДТЗС за умов, що описані вище) небезпечний сигнал (НС), що несе секретну інформацію. Усередині ОТЗС зондуючий високочастотний

сигнал з виходу лінії зв'язку (ЛЗ) поступає по відповідних шляхах проникнення (ШП) на модулюючий елемент (М). Отримавши в модулюючому елементі М модуляцію якого-небудь параметра високочастотного коливання (наприклад, амплітуди, фази) небезпечним сигналом НС (тут можна вважати, що небезпечний сигнал як би «нав'яже» якому-небудь параметру високочастотного сигналу свій закон зміни), зондуючий сигнал відбивається від неузгодженого навантаження, яке представляє модулятор М для цього зондуючого сигналу в діапазоні частот зондування, і поширюється у зворотному напрямі, як показано на рисунку пунктиром, до приймача П, який в результаті цього отримує інформацію про небезпечний сигнал [43].

1.2. Аналіз технологій перехоплення інформації методами високочастотного нав’язування

Аналіз способів перехоплення мовленнєвої інформації. Втрата мовленнєвої інформації каналами ВЧ-нав’язування являється одною із проблем людства в час промислового шпіонажу. Постійні переговори, телефонні розмов, наради та зустрічі стають під загрозою перехоплення ключової інформації зловмисниками. Для перехоплення мовленнєвої інформації зловмисники використовують відомі технічні канали витоку акустичної інформації за допомогою ВЧ-нав’язування, оскільки даний канал являється найефективнішим в нас час.

Засоби отримання мовленнєвої інформації каналами витоку ВЧ-нав’язування спроможні отримувати інформацію в акустичному, віброакустичному, акустоелектричному, оптикоелектричному та параметричному каналах витоку інформації, що робить даний метод отримання інформації найбільш небезпечним та різноманітнішим у засобах отримання інформації [44].

Розроблені технічні рішення протидії високочастотному каналу витоку інформації не можуть в повній мірі забезпечити захист мовленнєвої

інформації, опираючись на встановлені сучасні вимоги до технічних рішень забезпечення захисту від витоку інформації каналами ВЧ-нав’язування.

Для забезпечення захисту мовленнєвої інформації необхідний синтез технології та алгоритмів захисту, який відповідатиме вимогам захисту інформації та дозволить за допомогою своїх властивостей виключити можливі канали витоку інформації ВЧ-нав’язуванням.

Сутність способу полягає в тому, що його застосування змінює властивості сигналу зондування ВЧ-нав’язування, що робить його непридатним для отримання акустичної інформації [45].

Для підтвердження заявлений властивостей запропонованого синтезованої технології захисту, потрібно дослідити фізичне явище, на якому базується принцип забезпечення захисту інформації. Розгляд принципу дії синтезованої технології дозволить отримати відомості можливого застосування технології.

Аналіз методів перехоплення цифрових даних, оброблюваних засобами обчислювальної техніки. При розгляді проблеми ВЧ-нав'язування мережевими кабелями необхідно відзначити наступні її нюанси:

1. Елементом електронної апаратури, за рахунок нелінійності якого сигнал ВЧ-нав'язування взаємодіє з низькочастотними (щодо нього) сигналами, є елемент мережного адаптера або модему.

Невідомо при цьому, який елемент мережного адаптера чи модему вважати «активним», тобто елементом, властивості якого дозволяють здійснити модуляцію високочастотного сигналу та відображення його назад у мережу.

Як «активний» слід розглядати «вихідний» нелінійний елемент (ВНЕ) мережевого адаптера або модема, наприклад транзистор (навіть якщо його розглядати у складі деякої мікросхеми, що часто зустрічається). Вплив наступних («передвихідного» і т.д.) каскадів можна знехтувати, зважаючи на те, що робочий діапазон частот «вихідного» нелінійного елемента зазвичай

набагато нижче частоти сигналу ВЧ нав'язування, що обумовлює значне його ослаблення (на кілька порядків) при проходженні даного елемента.

2. Елементом електронної апаратури, що виконує роль «модулятора», тобто джерела розвідуваної інформації, може бути відеокарта СВТ (є генератором залежно від типу відеокарти та монітора сигналів із частотою від 25 МГц до приблизно 80 МГц [46]), будь-який внутрішній (припускаємо, що «витоку» через корпус немає) кабель (резонансні частоти внутрішніх кабелів можуть бути в діапазоні 200-800 МГц [46]) і т.д.

Слід зазначити, що частота сигналу ВЧ-нав'язування має бути, як мінімум, в 10 разів вище частоти сигналу, який вважається модулюючим (розвідуваним). Це означає, що розвідуючи сигнал відеокарти, у якого частота $f_{\text{с}}$=70 МГц, слід використовувати сигнал ВЧ-нав'язування з мінімальною частотою $f_{\text{вчн}}$=700 МГц і т.д. При цьому дуже актуальним стає питання загасання такого сигналу та його «віддзеркалення» в мережевому кабелі.

«Вихідний» нелінійний елемент, як і передбачалося, входить у склад інтегральної мікросхеми, що не дозволяє розглядати його окремо та аналізувати характеристики даного елемента як виділеного. У складі мережевих адаптерів (модемів) «вихідний» нелінійний елемент у ракурсі розглянутої проблеми виконує такі функції [47]:

а) приймає сигнал ВЧ-нав'язування;

б)змінює свої характеристики під впливом модулюючого (розвідуваного) сигналу;

в) відображає назад у лінію сигнал (частина сигналу) ВЧ-нав'язування, параметри якого змінюються відповідно до змін параметрів самого "вихідного" нелінійного елемента;

г) розсіює у вигляді тепла та пропускає у наступні каскади мережевого адаптера (модему) частину енергії сигналу ВЧ-нав'язування.

При цьому актуальними є такі питання:

1. Яку частину енергії сигналу ВЧ-нав'язування можна дозволити пропустити, не викликавши при цьому збоїв у роботі всього пристрою

(мережевого адаптера або модему) в цілому? Даний аспект аналізованої проблеми важливий у зв'язку з тим, що одним з якостей заходів щодо розвідки інформації є їх прихованість. Тому необхідно визначити, яка може бути енергія високочастотного сигналу (сигналу ВЧ-нав'язування), пройшов через «вихідний» нелінійний елемент, при якому спостерігатимуться збої функціонування пристрою, отже, можна буде визначити факт спроби використання методу ВЧ-нав'язування для організації каналів витоку цифрових даних за допомогою каналів передачі.

2. Яка має бути частка розсіюваної у вигляді енергії сигналу ВЧ-нав'язування, яка зможе викликати перегрів пристрою та збій його функціонування, а значить, і виявлення факт спроби ВЧ-нав'язування?

Враховуючи вищезгадане, сигнал ВЧ-нав'язування пропонується розглядати не тільки як «зондуючий сигнал», але і як «перешкоду». Чим більша потужність сигналу ВЧ-нав'язування, тим більшої дальності можна проводити розвідку, але при цьому підвищується ймовірність збоїв функціонування «випромінюваних» пристроїв, отже, і можливість розкриття факту ведення розвідки методом ВЧ-нав'язування [48].

При зміні характеристик вихідного нелінійного елемента під впливом модулюючого (розвідуваного) сигналу опір нелінійного елемента у випадку носить комплексний характер [49].

У процесі модуляції він змінюється, а значить вихідна провідність даного елемента може бути охарактеризована в процесі модуляції змінними складовими реактивної ($\Delta b_{\text{не}}(t)$) і активною ($\Delta g_{\text{не}}(t)$) провідністю [10]:

$$\Delta y_{\text{рл}}(t) = \Delta g_{\text{рл}}(t) + j\Delta b_{\text{рл}}(t) \tag{1.1}$$

Під дією модулюючої напруги буде змінюватися як активна, так і реактивна складова провідності нелінійного елемента. Зміна реактивної

складової ($\Delta b_{\text{не}}(t)$) викликатиме частотну модуляцію, а активною складовою ($\Delta g_{\text{не}}(t)$) - амплітудну модуляцію.

«Вихідний» нелінійний елемент у складі інтегральної мікросхеми мережевого адаптера (модему) авторами статті пропонується розглянути як деякий чотириполюсник.

Як показано в [50], існуючі моделі транзисторів, що розглядаються, могли б застосовуватись, якби їх елементи були змінені з високою точністю. На жаль, це не так. У зв'язку з цим можна використовувати безструктурні моделі, тобто представляти досліджуваний пристрій у вигляді деякого «чорного ящика», чотириполюсника, що описується, наприклад, S-матрицею. В даний час для опису багатополюсників використовуються матриці опорів, провідностей, відображення та розсіювання. У цьому випадку використовувати матрицю розсіювання [S] доцільно. При цьому, як показано на малюнку, аналізований чотири полюсники має два плечі (1 і 2), вхідний і вихідний [50].

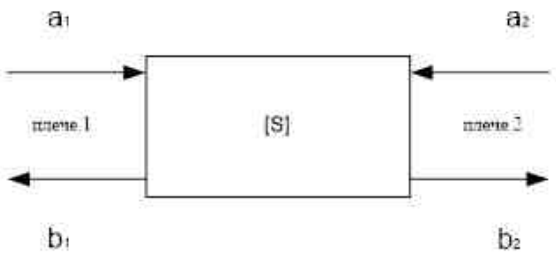


Рис. 1.2. S-матриця

Хвиля, що виходить із плеча 1, має амплітуду b_1 і збуджується хвилями a_1 і a_2 на основі принципу суперпозиції:

$$\begin{cases} b_1 = s_{11}a_1 + s_{12}a_2 \\ b_2 = s_{21}a_1 + s_{22}a_2 \end{cases}, \tag{1.2}$$

де $s_{i,j}$ – елементи S-матриці;

$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}$ – матриця розсіювання, яка встановлює зв'язок відбитих від чотирьохполюсника (які розходяться від нього) хвиль із такими, що сходяться (падають на нього) хвилями;

$S_{11} = \frac{U_{1\text{отр}}}{U_{1\text{пад}}}\Big| U_{2\text{пад}} = 0$ – комплексний коефіцієнт відбиття від плеча 1 при узгодженому плечі 2;

$S_{22} = \frac{U_{2\text{отр}}}{U_{2\text{пад}}}\Big| U_{1\text{пад}} = 0$ - комплексний коефіцієнт відбиття від плеча 2 при узгодженому плечі 1;

$S_{21} = \frac{U_{2\text{отр}}}{U_{1\text{пад}}}\Big| U_{2\text{пад}} = 0$ - комплексний коефіцієнт пропускання (передачі) з плеча 1 в плече 2 при узгодженому плечі 2;

$S_{12} = \frac{U_{1\text{отр}}}{U_{2\text{пад}}}\Big| U_{1\text{пад}} = 0$ - комплексний коефіцієнт пропускання (передачі) з плеча 2 в плече 1 при узгодженому плечі 1;

$$\begin{cases} U_{1\text{отр}} = S_{11}U_{1\text{пад}} + S_{12}U_{2\text{пад}} \\ U_{2\text{отр}} = S_{21}U_{1\text{пад}} + S_{22}U_{2\text{пад}} \end{cases}. \quad (1.3)$$

Розглянутий випадок відповідає вивченню електричного ланцюга зі змінними в часі параметрами, наприклад нелінійного чотириполюсника, а в таких пристроях можливе виникнення наступних фізичних явищ [51].

Виникнення інтенсивних коливань загалом вищої гармоніці за відсутності її у вхідній напрузі.

Виникнення субгармонічних коливань, тобто коливань на частоті, ціле число разів менше частоти джерела ЕРС (найчастіше спостерігається коливання на частотах ω/2, ω/3, ω/5 і т.д.).

1.3. Аналітичний огляд відомих технічних рішень захисту інформації від витоку каналами високочастотного нав'язування

На сьогодні використовуються пасивні, активні та комбіновані методи захисту інформації від перехоплення. Також існує поділ на організаційні та технічні методи захисту інформації.

До основних організаційних заходів відносять [52]:

1. Залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ).

2. Категоріювання й атестацію об'єктів ОТЗС та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності.

3. Використання на об'єкті сертифікованих ОТЗС та ДТЗС.

4. Встановлення КЗ навколо об'єкта.

5. Залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;

6. Організацію контролю та обмеження доступу на об'єкти ОТЗС та у виділені приміщення.

7. Введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту.

8. Відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Серед загальновідомих методів захисту інформації від перехоплення за допомогою високочастотного нав'язування можна вказати наступні: встановлення додаткових конструкцій екранування на початкових етапах розробки апаратури, яка буде використовуватись; встановлення додаткового

екранування конструкції; встановлення фільтрації високочастотних зондуючих сигналів в усіх підключених до апаратури електричних колах і лініях зв’язку. Однак вказані пасивні методи не забезпечують повноцінного захисту інформації [53].

Мета пасивних і активних методів захисту – зменшення відношення сигнал / шум на межі контрольованої зони до величин, які забезпечують неможливість виділення засобом розвідки зловмисника небезпечного інформаційного сигналу. В пасивних методах захисту зменшення відношення сигнал/шум досягається шляхом зменшення рівня небезпечного сигналу, в активних методах – шляхом збільшення рівня шуму [54].

Як пасивні, так і активні засоби захисту мають свої характерні переваги і недоліки. Як зазначають автори, перевагами пасивних засобів захисту є:

- малі габарити, проста електрична схема;
- зовнішнє електроживлення не потрібно;
- вони включаються в розрив ланцюгів і тому вихід з ладу деяких елементів електричної схеми виявляється в процесі експлуатації;
- невисока вартість щодо інших типів засобів.

Водночас, активні засоби захисту, в порівнянні з пасивними, мають більш складну будову, високу вартість, а також вимагають зовнішнього джерела електроживлення. Але, незважаючи на ці недоліки, часто виявляється, що ефективність активних засобів захисту вище, ніж у пасивних.

Відповідно комбіновані засоби захисту побудовані на основі комбінації пасивних і активних засобів. До найбільш широко застосовуваних пасивних методів захисту відносяться:

- обмеження сигналів малої амплітуди;
- фільтрація сигналів високочастотного нав'язування;
- відключення перетворювачів (джерел) сигналів [55].

Слід зауважити, що у даній статті розглядається проблематика захисту інформації від перехоплення в телефонних лініях. Серед перелічених методів

відсутній такий, який впливав би безпосередньо на параметри небезпечного сигналу, який генерується з метою перехоплення інформації.

В [56] зазначають, що використання активних засобів має певні недоліки:

- при зміні розташування джерела інформаційного сигналу (наприклад, перестановки ПК або додавання нових), загальний рівень сигналу в приміщенні можуть змінитися таким чином, що сигнали можна виявити поза приміщенням, незважаючи на зашумлення;
- необхідно зашумлювати сигнали в широкому діапазоні частот. Межі цього діапазону не завжди можна чітко визначити через биття кількох сигналів, а також можливого зовнішнього ВЧ впливу;
- наявність пригнічуючих випромінювань демаскує об'єкт і може перешкоджати роботі інших чужих пристроїв за межами контрольованої зони;
- використання активних засобів передбачає постійні додаткові дії (наприклад, підготовка комплексу до роботи, включення, виключення, профілактика, постійна перевірка його практики та тому подібне);
- необхідні додаткові джерела живлення. Іноді це приводить до обмеження працездатності генераторів шуму в часі.

Автори у статті [57] зробили висновок, що метод перехоплення інформації високочастотного нав’язування складний для виявлення тому, що має широкий діапазон допустимих частот, в той час пристрої, робота яких спрямована на виявлення високочастотного нав’язування, мають змогу здійснювати перевірку тільки у вузькому діапазоні частот.

В цій статті пропонується варіант захисту інформації від перехоплення шляхом організації каналу в певній полосі частот. В такому разі передача даних буде здійснюватись з певними спотвореннями. Відповідно зловмиснику буде потрібно періодично повторювати параметри свого небезпечного сигналу, що на практиці дуже важко реалізувати. Однак навіть у такому випадку у зловмисника є можливість аналізувати весь спектр, який утворюється від високочастотного нав’язування, накопичувати варіації

сигналів та виділяти важливі для себе частини. Тому цей метод також не гарантує повноцінного захисту інформації, якщо навіть не враховувати складність його реалізації.

Одним із найбільш дієвих методів захисту інформації можна вважати метод, який базується на генеруванні сигналів завади. У роботі [58] розглядається поняття моделі сигналу та пропонується використовувати різні моделі сигналів завади, так як від моделі залежить ефективність її використання задля захисту інформації від перехоплення.

Згідно статті при оцінці електромагнітної обстановки потрібно враховувати три складові:

1. ВЧ-сигнал.
2. Завади.
3. Внутрішні або власні шуми приймача сигналу.

Відповідно до цього в сумі організовується так звана адитивна суміш, яка має наступний вигляд:

$$U_{Bx_i}(x,t) = U_v(x,t,\beta_h) + n(x,t) \text{ при } t = 0 \quad (1.4)$$

$$U_{Bx_i}(x,t) = U_{31}(x,t,\alpha_3,\beta_3) + U_v(x,t,\beta_c) + n(x,t) \text{ при } t = 1, \quad (1.5)$$

де $U_{31}(x,t,\alpha_3,\beta_3)$ – сигнал ВЧ нав’язування,

$U_v(x,t,\beta_h)$ – сигнал завади, який є непередбаченим,

$n(x,t)$ – власні шуми приймаючого пристрою, перераховані до входу прийомника.

Корисні сигнали відрізняються один від одного параметрами, на кількість яких вказує індекс і-го класу сигналу. Велика кількість видів корисних сигналів та сигналів завади систематизуються шляхом введення типових моделей або типових видів сигналів.

Такими сигналами є детерміновані, квазідетерміновані і випадкові (складні) корисні сигнали, детерміновані, квазідетерміновані, випадкові і групові сигнали завади. В якості видової ознаки типових моделей сигналів і завад виступають амплітуда та початкова фаза.

Детерміновані сигнали і завади мають невипадкові амплітуди і початкові фази (із умови нормування амплітуди беруться рівними одиниці).

Квазідетерміновані сигнал і завада мають випадкові амплітуди та (або) початкові фази. При цьому типовим видом є сигнали із випадковими амплітудами і випадковими початковими фазами, які характеризуються найбільшим ступенем випадковості в цьому вигляді сигналів і найбільш часто зустрічаються на практиці. Але у відношенні сигналів завади потрібно також використовувати і модель з невипадковою амплітудою і випадковою початковою фазою, яка адекватна непередбачуваній заваді, яка створюється при умові близького розташування джерела і рецептора завад. При невипадковій амплітуді її значення приймають рівним одиниці, а при випадковій амплітуді остання нормується таким чином, щою її другий початковий момент, який є нормованим множником потужності сигналу, був рівним одиниці.

Випадкові сигнали на відміну від детермінованих і квазідетермінованих сигналів, які відносяться до простих сигналів, є складними. Вони характеризуються наявністю послідовності в часі і (або) прсоторі ряду квазідетермінованих сигналів. Кожен з таких сигналів називається елементарним і має незалежні від інших елементарних сигналів випадкові несуттєві параметри (амплітуду і початкову фазу). До числа складних відносяться випадкові шумові і не шумові сигнали. Тому складні сигнали часто називають випадковими.

Аналогічним чином визначаються детерміновані, квазідетерміновані і випадкові сигнали завади. Додатковим видом до цього відноситься групова завада, яка представляє собою суму сигналів завади перших трьох типів, які накладаються один на одного в часі та (або) в просторі.

Підсумовуючи вищесказане, слід зауважити, що на об’єктах, де обробляється критично важлива інформація, можуть бути присутні різні види сигналів та завад. У варіанті, коли системи з непорушними антенами знаходяться на близьких відстанях одна від одної, сигнали завади мають постійні або відомі несуттєві параметри. В таких умовах робочою є модель детермінованої завади.

В роботі [57] описується вплив високочастотного нав’язування на абонентські телефонні лінії. Серед варіантів вирішення питання захисту інформації від перехоплення пропонується використання загороджувальних фільтрів. Амплітудно-частотна характеристика таких фільтрів має забезпечувати так звану «прозорість» в інтервалі каналу тональної частоти (300 – 3400 Гц) і якомога більше згасання на частотах позазвукового діапазону. Найпростішим варіантом загороджувального фільтра є конденсатор, встановлений у мікрофонне коло телефонного апарата або у коло електромагнітного дзвінка виклику. Ємність конденсатора вибирають так, що зашунтувати зондувальні сигнали високочастотного нав’язування і разом з тим істотно не впливати на корисні сигнали.

Складнішим варіантом розглядається можливість використання активних засобів. Він полягає у накладанні захисного шуму на небезпечний сигнал. Розрізняють низькочастотні маскувальні сигнали в діапазоні від 100 Гц до 10 кГц та високочастотні широкосмугові – від 20 кГц до 30 МГц. Внаслідок ефекту маскування не вдається засобами технічної розвідки виділити інформативні параметри сигналів витоку.

Ідею застосування активних засобів можна реалізувати не тільки для захисту інформації в телефонних каналах, але й для захисту акустичної інформації. Складність реалізації полягає в тому, що маскувальні сигнали, як вже зазначалось вище, повинні бути змінними відносно того, як змінюється небезпечний сигнал. В цьому полягає недолік даного методу.

1.4. Постановка наукового завдання

Підсумовуючи, можна сказати, що станом на сьогодні в умовах постійного розвитку технологій перехоплення інформації на об’єктах інформаційної діяльності та критичної інфраструктури критично важливо здійснювати заходи щодо створення нових та удосконалення існуючих методів захисту інформації від витоку каналами високочастотного нав’язування.

З проведеного огляду зроблено висновок про те, що станом на сьогодні задля захисту інформації від перехоплення каналами високочастотного нав’язування використовують активні, пасивні та комбіновані методи захисту інформації. Жоден з існуючих методів не забезпечує прийнятного рівня захисту інформації. Аналітичний огляд показав, що при високочастотному нав’язуванні канали витоку інформації утворюються як в колах електроживлення та заземлення, так і в оточуючому середовищі. Це додає зловмиснику варіативності та збільшує шанси на перехоплення інформації. Водночас це зобов’язує забезпечувати комплексний підхід при побудові системи захисту інформації [58].

Необхідною умовою для забезпечення захисту інформації є універсальність методів та способів, а також можливість удосколанення взалежності від умов застосування. Такі методи повинні забезпечувати комплексний підхід до захисту інформації від перехоплення, але також бути простими у застосуванні.

Відповідно, найбільш актуальним в цьому напрямі є використання активних методів захисту інформації від витоку. Стрімкий розвиток засобів перехоплення зобов’язує постійний пошук рішень щодо удосконалення існуючих та розробки нових методів захисту інформації, тому що відомі методи дозволяють забезпечувати захист інформації, але всі вони здебільшого вузькоспеціалізовані та не універсальні.

Висновки до розділу 1

В розділі проведено аналіз процесу захисту інформації від витоку каналами високочастотного нав’язування.

1. Огляд наявної інформації щодо відомих методів захисту інформації від витоку дозволив систематизувати знання та загальновідомі дані про методи захисту інформації від високочастотного нав’язування. Відомо, що на рівні країни постійно виконується робота з удосконалення загальних систем захисту інформації від витоку, зокрема і питання протидії методам перехоплення інформації шляхом високочастотного нав’язування. Проте також і удосконалюються самі методи перехоплення інформації шляхом високочастотного нав’язування.

2. Проведений в розділі аналіз відомих методів захисту інформації від перехоплення методами високочастотного нав’язування показав, що загалом існують різні варіанти захисту інформації, але всі вони є вузькоспеціалізованими, не універсальними та не забезпечують захист на бічних гармоніках небезпечного сигналу.

3. Аналітичний огляд відомих технічних рішень захисту інформації від витоку каналами високочастотного нав’язування показав, що наявні методи та алгоритми не передбачають впливу на сформовані високочастотним нав'язуванням небезпечні сигнали для забезпечення максимально можливої руйнації їх інформативних параметрів і, як результат, надійного блокування каналів витоку інформації.

4. Актуальним є наукове завдання щодо розробки методу захисту інформації від високочастоного нав’язування як на основних, так і на бічних гармоніках сигналу.

Для вирішення вказаного завдання необхідно:

1. Здійснити аналіз можливих варіантів покращення захисту інформації від витоку каналами високочастотного нав’язування.

2. Розробити математичну та імітаційну моделі блокування інформації від перехоплення та захисту інформації від перехоплення каналами високочастотного нав’язування.

3. Провести експериментальні дослідження для підтвердження теоретичних відомостей та розроблених моделей.

4. Удосконалити модель оцінки захищеності інформації від витоку каналами високочастотного нав’язування.

РОЗДІЛ 2
СИНТЕЗ АКТИВНОГО МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

2.1. Загальна постановка задачі дослідження

Зондуючі сигнали високої частоти, використовувані при перехопленні інформації методом високочастотного «нав'язування», поступають по лініях зв'язку на ТЗПІ і проникають потім всередину цих пристроїв наступними шляхами [59, 60]:

- колами, утвореними паразитними електричними і магнітними зв'язками між елементами пристроїв;
- за допомогою електромагнітного випромінювання з одних ділянок дротів і кіл, і прийому цих випромінювань іншими дротами і колами (антенний ефект);
- безпосередньо колами прямого гальванічного зв'язку (наприклад, при підключенні генератора зондуючих коливань до систем заземлення, електроживлення).

При дії на кола і елементи ОТЗС зондуючими високочастотними коливаннями, останні в деяких випадках виявляються промодульованими циркулюючими в цих колах небезпечними (мовленнєвими, телеграфно-телекодовими і іншими порівняно низькочастотними) сигналами і можуть бути виділені при подальшій їх обробці в системі перехоплення інформації.

Таким чином, зондуючі високочастотні коливання стають носіями інформації небезпечного сигналу і створюють канал можливого витоку інформації.

Фізична сутність процесу модуляції полягає в тому, що зондуючі високочастотні коливання, що створюються системою перехоплення інформації, характеризуються в початковому стані певним числом постійних параметрів.

У простому випадку в якості зондуючого коливання супротивником може бути застосоване гармонічне (синусоїдальне) коливання. Аналітичне вираження таких коливань в загальному випадку має вигляд [40, 41]:

$$F(t) = A_0 \cos(\omega_0 t + \varphi_0) \tag{2.1}$$

де A_0 – амплітуда коливання,

$(\omega_0 t + \varphi_0)$ – фаза коливання.

При постійних значеннях параметрів A_0 і $(\omega_0 t + \varphi_0)$ коливання, що визначається вказаним співвідношенням, не несе ніякої смислової інформації про стан об'єкта спостереження. Якщо ж в такт з керуючим НЧ сигналом (небезпечним сигналом) змінюватимуться основні параметри цього коливання, то результуюче коливання може бути представлене у вигляді:

$$F(t) = A(t) \cdot \cos \Phi(t) \tag{2.2}$$

Тобто, зондуюче коливання в цьому випадку характеризуватиметься двома основними величинами, що змінюються в часі: амплітудою $A(t)$ і фазовим кутом $\Phi(t)$.

Процес, який полягає в тому, що той або інший параметр зондуючого коливання змінюється в часі згідно з оброблюваними в ОТЗС сигналами низької частоти (небезпечними сигналами), є процесом небажаної (паразитної) модуляції.

Відоме [40, 41] представлення АМ коливання:

$$u(t) = U_H \cos \omega_0 t + \frac{m}{2} U_H \cos(\omega_0 + \Omega)t + \frac{m}{2} U_H \cos(\omega_0 - \Omega)t \tag{2.3}$$

показує, що модульоване коливання, на підтвердження вищесказаного, є складним коливанням. Перший член суми являє собою зондуюче високочастотне коливання, яке не несе, як було відмічено вище, ніякої інформації про небезпечний сигнал, тоді як два інші члени є інформативними і формують огинаючу та представляють собою нові частотні складові гармонічного характеру, величини амплітуд яких визначаються як $m \cdot U_H / 2$. Оскільки уся перехоплювана інформація знаходиться саме в цих додаткових членах, то, отже, для зменшення або виключення витоку інформації, необхідно зменшити або виключити величини m і U_H.

Отже, сутність явища ВЧ «нав'язування» полягає в отриманні модульованих високочастотних коливань (коли модулюючим сигналом є перехоплюваний небезпечний сигнал) при дії зондуючого немодульованого коливання високої частоти на вузли технічних засобів (ОТЗС і ДТЗС). Додаткові частотні складові, що з'явилися при цьому, формують високочастотний інформаційний сигнал, мають частоти $(\omega_0 + \Omega)$ та $(\omega_0 - \Omega)$, зрушені відносно зондуючого високочастотного коливання ω_0 на величину модулюючих частот і, отже, за умови $\omega_0 \gg \Omega$, є також високочастотними.

Враховуючи викладене вище, можна зробити висновок, що дане явище супроводжується процесом лінійного переносу спектра низькочастотного сигналу (мовного, телекодового і тому подібне) в область радіочастотного діапазону. Лінійність характеру вказаного процесу полягає в тому, що при його здійсненні вид і співвідношення між компонентами спектра первинного інформаційного сигналу залишаються незмінними.

Крім того, виходячи з (2.3) це явище можна розглядати як результат перемноження двох початкових коливальних процесів, що взаємодіють між собою в електричних колах ОТЗС. Процес такого перемноження двох коливань може бути здійснений двома способами.

Перший спосіб заснований на використанні елементів, що мають нелінійну провідність. З теорії електричних і радіотехнічних кіл відомо [43],

що якщо на деякий нелінійний елемент з вольтамперною характеристикою, що апроксимується виразом:

$$i = i_0 + \alpha u + \beta u^2 + \gamma u^3, \tag{2.4}$$

де діятимуть дві напруги u_c і $u_г$, то вихідний струм цього елементу міститиме множину комбінаційних складових з частотами:

$$\omega_к = \left(\pm r\omega_г \pm q\Omega_c\right), \tag{2.5}$$

де r і q – цілі позитивні числа (включаючи і шум), а амплітуди і фази їх залежатимуть відповідно від амплітуд і фаз прикладених напруг u_c і $u_г$. Таким чином, елементи з нелінійною провідністю дозволяють реалізувати процес перемноження двох початкових напруг і при цьому, разом з різними комбінаціями їх вищих гармонічних складових, отримати частоти, рівні сумі і різниці частот інформаційної небезпечної і допоміжної (зондуючої) напруг.

Другий спосіб перемноження базується на використанні лінійних кіл зі змінними параметрами (параметричних кіл). Так, якщо деякий чотириполюсник, лінійний по відношенню до зондуючої напруги, матиме періодично змінюваний коефіцієнт передачі:

$$K(t) = K_0\left(1 + \cos\Omega t\right) \tag{2.6}$$

то при поданні на його вхід напруги коливань на виході чотириполюсника отримаємо:

$$u_{вих.} = K(t) \cdot u_г \tag{2.7}$$

і тоді:

$$u_{вих.} = K_0(1+\cos\Omega t)\cdot u_{mг}\cos(\omega_г t+\varphi\omega), \qquad (2.8)$$

тобто, в результаті перемножувальної дії даної системи можна виділити напруги, за своїм вираженням аналогічні (2.3).

Таким чином, тільки в результаті нелінійного або параметричного перемноження двох напруг, на відповідному селективному навантаженні можна виділити сигнал, що має вигляд

$$u = u_m(t)\cos[\omega t+\varphi\omega(t)], \qquad (2.9)$$

який відповідає шуканому, зміни амплітуди u_m або фази φ якого повністю визначаються законами зміни амплітуд і фаз вхідних напруг небезпечних сигналів.

В результаті численних досліджень було показано [61, 62], що в колах ОТЗС і ДТЗС, які містять нелінійні елементи і мікрофони, модульовані коливання виникають внаслідок зміни їх опору при спільній дії небезпечного – інформативного сигналу акустоелектричних перетворень, у тому числі – високочастотного зондуючого сигналу. У загальному випадку модулюючі елементи кіл ОТЗС – випадкові модулятори – можна розділити на дві групи:

- нелінійні і лінійні активні опори (мікрофони, діоди, транзистори, електронні лампи);
- нелінійні і лінійні реактивні опори (індуктивності трансформаторів, дроселів, обмоток реле, дзвінкових котушок, ємність конденсаторних мікрофонів та ін.).

Елементи 1-ої групи є, в основному, причиною появи АМ коливань в резистивних колах. Елементи 2-ої групи – ФМ коливань або коливань складнішої форми (наприклад, АМ і ФМ).

Виникнення ненавмисної модуляції в ОТЗС може мати місце лише за цілком певних умів. Для оцінки цих умов передусім з'ясуємо механізм дії високочастотних коливань на кола з навантаженнями, провідність яких змінюється за законом зміни низькочастотного сигналу Ω. Для прикладу розглянемо процес при зміні параметра хоча б одного з елементів кола (наприклад, резистивного опору у вугільному мікрофоні під впливом акустичного поля).

Для випадку, коли $Z = R$ і $Z_M = R_1$, коло складається з джерела напруги частоти $\omega e = U_M cos\omega t$ і двох послідовно включених опорів, постійного – R і змінного – R_1:

$$R_0 = R + R_1. \tag{2.10}$$

Під впливом звукових коливань мембрана коливається і, натискаючи на вугільний порошок, що знаходиться в мікрофоні, змінює його провідність. Припустимо, що мікрофон строго лінійний, тобто що провідність суть лінійна функція звукового тиску. Тоді для провідності змінного елементу маємо:

$$g = g_0 + kP\,. \tag{2.11}$$

Нехай зміна звукового тиску:

$$P = P_m \cos\Omega t\,. \tag{2.12}$$

Тоді для провідності змінної частини кола можна записати

$$g(t) = g_0 + kP_m \cos \Omega t = g_0 + g_1 \cos \Omega t\,. \qquad (2.13)$$

Позначивши коефіцієнт модуляції для провідності

$$m = \frac{g_1}{g_0}\ , \qquad (2.14)$$

маємо:

$$g(t) = g_0(1 + m \cos \Omega t). \qquad (2.15)$$

Якщо для електрорушійної сили e, створюваної зовнішнім високочастотним генератором у розглядуваному колі, справедливий вираз:

$$e = E_m cos\omega_0 t\ , \qquad (2.16)$$

де ω_0 – частота високочастотного генератора, то струм в колі буде рівним добутку електрорушійної сили e на провідність кола:

$$i_{\text{вих}} = eg = E_m g_0(1 + mcos\Omega t)cos\omega_0 t. \qquad (2.17)$$

Отримуємо звичайний вираз амплітудно-модульованого коливання, тому що добуток $E_m g_0(1 + mcos\Omega t)$можна розглядати як амплітуду коливань $E_m(1 + mcos\Omega t)$ частоти ω_0, що змінюється з частотою Ω при постійній величині провідності кола, тобто має місце лінійна параметрична амплітудна модуляція.

Амплітудна модуляція може бути здійснена також за наявності коливальних контурів і нелінійних елементів в колах.

2.2. Розробка моделі блокування перехоплення інформації методами високочастотного нав’язування

Виконання при розробці апаратури ОТЗС і ДТЗС вимог по екрануванню, фільтрації і розв'язкам в широкому діапазоні частот (від 10кГц до 30МГц і більше) і ряду інших, викладених вище, спрямованих на виключення можливостей перехоплення інформації по каналу витоку, що утворюється при застосуванні методу високочастотного «нав’язування», суттєво зменшить імовірність витоку інформації по переважній більшості інших, відомих нині каналів витоку інформації.

Доцільно на підставі вище викладеного розробити спеціальні тимчасові вимоги і рекомендації для розробників апаратури ОТЗС і ДТЗС, забезпечити їх обов'язкове виконання при створенні апаратури ОТЗС і ДТЗС, для яких апріорі пред'являються вимоги забезпечення захищеності інформації від витоку каналами високочастотного «нав’язування».

Використання тих чи інших методів і засобів захисту визначається характеристиками об'єкта захисту та апаратури розвідки, а також вимогами, що пред'являються до ефективності захисту інформації.

Наприклад, для оцінки розбірливості мови застосовують інструментально-розрахунковий метод, заснований на результатах експериментальних досліджень. Сутність цього методу полягає в наступному [63, 64].

Явище «биття» коливань спостерігається при складанні двох гармонічних процесів з близькими частотами і полягає в амплітудній низькочастотній модуляції сумарного високочастотного коливання.

Негармонічні коливання, що виходять в результаті складання однаково спрямованих гармонічних коливань з близькими частотами $\omega 1 \approx \omega 2$,

називаються биттям (рис. 3.1а). Іншими словами різниця між частотами коливань, що складаються повинна бути багато менше будь-який з цих частот: $|\omega_1 - \omega_2| \ll \omega_1$ i $|\omega_1 - \omega_2| \ll \omega_2$ (критерій спостереження биття).

За початок відліку часу приймемо момент $t_0 = \frac{\varphi_1 - \varphi_2}{\omega_1 - \omega_2}$, коли фази обох коливань, що складаються x1 і x2 збігаються і дорівнюють $\varphi_0 = \frac{\varphi_2\omega_1 - \varphi_1\omega_2}{\omega_1 - \omega_2}$.

Для простоти аналізу отриманих далі виразів знайдемо середню частоту коливань, що складаються $\overline{\omega} = \frac{1}{2}(\omega_1 + \omega_2)$ і різницю частот $\Delta\omega = \omega_2 - \omega_1$. Так як частоти ω1 ≈ ω2 близькі, різниця частот |Δω| мала величина. Частоти коливань, що складаються можна виразити через введені величини: $\omega_1 = \overline{\omega} - \frac{1}{2}\Delta\omega$, $\omega_2 = \overline{\omega} + \frac{1}{2}\Delta\omega$. При цьому коливання що складаються приймуть вигляд

$$x_1 = A_1\, cos\left(\overline{\omega}t + \varphi_0 - \frac{1}{2}\Delta\omega t\right), \tag{2.18}$$

$$x_2 = A_1\, cos\left(\overline{\omega}t + \varphi_0 + \frac{1}{2}\Delta\omega t\right). \tag{2.19}$$

Тоді різниця фаз коливань слабо залежить від часу $\Delta\Phi = \Phi_2(t) - \Phi_1(t) = \Delta\omega t$. Амплітуда результуючого коливання $A^2 = A_1^2 + A_2^2 + 2A_1A_2\, cos(\Delta\omega t)$ повільно змінюється з часом. За допомогою тригонометричних тотожностей тангенс фази результуючого коливання можна представити у вигляді:

$$tg\Phi(t) = \frac{tg(\overline{\omega}t + \varphi_0) + tg\varphi}{1 - tg(\overline{\omega}t + \varphi_0)\cdot tg\varphi} = tg(\overline{\omega}t + \varphi_0 + \varphi), \tag{2.20}$$

де $tg\varphi = \frac{A_2 - A_1}{A_1 + A_2} tg\left(\frac{1}{2}\Delta\omega t\right)$.

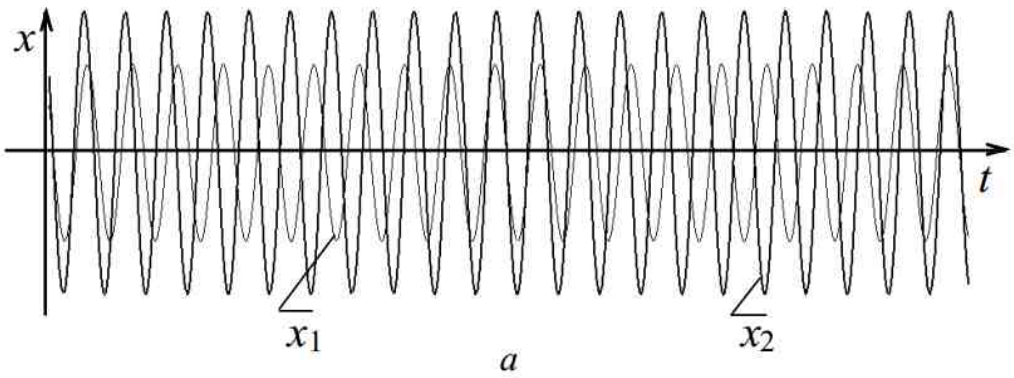


Рис. 2.1. Складання двох сигналів

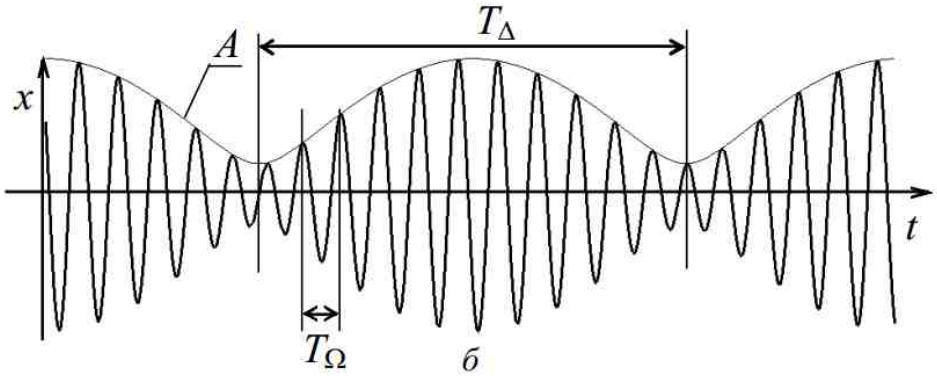


Рис. 2.2. Результуючий сигнал після складання двох сигналів

Тангенс φ залежить від часу, тому фаза коливань має складну залежність від часу:

$$\Phi(t) = \overline{\omega}t + \varphi_0 + \varphi(t). \tag{2.21}$$

Таким чином, результуючі коливання описуються рівнянням:

$$x = A(t)\cos(\overline{\omega}t + \varphi_0 + \varphi(t)), \tag{2.22}$$

де $A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos(\Delta\omega t)$,

$$tg\varphi = \frac{A_2 - A_1}{A_1 + A_2} tg\left(\frac{1}{2}\Delta\omega t\right). \quad (2.23)$$

Для визначення залежності додаткової фази φ від часу врахуємо, що частоти коливань, що складаються близькі ω1 ≈ ω2, різниця частот Δω - мала величина. Модуль відношення амплітуд менше одиниці $\left|\frac{A_2 - A_1}{A_1 + A_2}\right| < 1$.Отже, тангенс додаткової фази φ теж мала величина. Розкладемо тангенс в правій і лівій частині в ряд до першого порядку малості (tg x ≈ x) $\varphi \approx \frac{1}{2}\frac{A_2 - A_1}{A_1 + A_2}\Delta\omega t$.

Тоді повна фаза результуючого коливання лінійно залежить від часу:

$$\overline{\omega}t + \varphi(t) + \varphi_0 \approx \overline{\omega}t + \frac{1}{2}\frac{A_2 - A_1}{A_1 + A_2}\Delta\omega t + \varphi_0. \quad (2.24)$$

Результуюче коливання можна записати у вигляді $x = A(t)\cos(\Omega t + \varphi_0)$, де $A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos(\Delta\omega t)$, частота коливань $\Omega \approx \overline{\omega}\left(1 + \frac{1}{2}\cdot\frac{A_2 - A_1}{A_1 + A_2}\cdot\frac{\Delta\omega}{\overline{\omega}}\right)$. Залежно від співвідношення амплітуд частота Ω результуючих коливань може бути як менше, так і більше середньої частоти коливань, що складаються ω.

При додаванні однаково спрямованих гармонічних коливань з різними амплітудами A1 ≠ A2 та близькими частотами ω1 ≈ ω2 результуючі коливання (биття) здійснюються з частотою Ω, при цьому амплітуда коливань повільно змінюється з часом від різниці до суми амплітуд коливань по періодичному закону. Частота зміни амплітуди биття дорівнює різниці частот складених коливань Δω і називається частотою биття. Тоді величина $T_\Omega = \frac{2\pi}{\Omega}$ називається періодом коливань, а величина $T_\Delta = \frac{2\pi}{\Delta\omega}$ періодом биття.

Критерій спостереження биття можна записати у вигляді $\left|\frac{\Delta\omega}{\overline{\omega}}\right| \ll 1$ або $T_\Omega \ll T_\Delta$.

Іншими словами, биття спостерігаються, якщо за один період зміни амплітуди тіло здійснює багато коливань.

Окремий випадок, коли складаються коливання з однаковими амплітудами A1 = A2 (φ = 0), описується простішими рівняннями:

$$x = A(t)\cos(\overline{\omega}t + \varphi_0), \tag{2.25}$$

де $A^2 = 2A_1^2(1 + \cos(\Delta\omega t)) = 4A_1^2 cos^2(\frac{1}{2}\Delta\omega t), \Longrightarrow A = 2A_1 \cos\left(\frac{1}{2}\Delta\omega t\right)$.

З наведених виразів видно, що при додаванні однаково спрямованих гармонічних коливань з однаковими амплітудами A1 = A2 і близькими частотами ω1 ≈ ω2 результуючі коливання (биття) здійснюються з середньою частотою ω, при цьому амплітуда коливань повільно змінюється з часом від нуля до $2A_1$ по гармонічному закону. Частота биття дорівнює половині різниці частот коливань $\omega\Delta_2$ 1 (рис. 2.3).

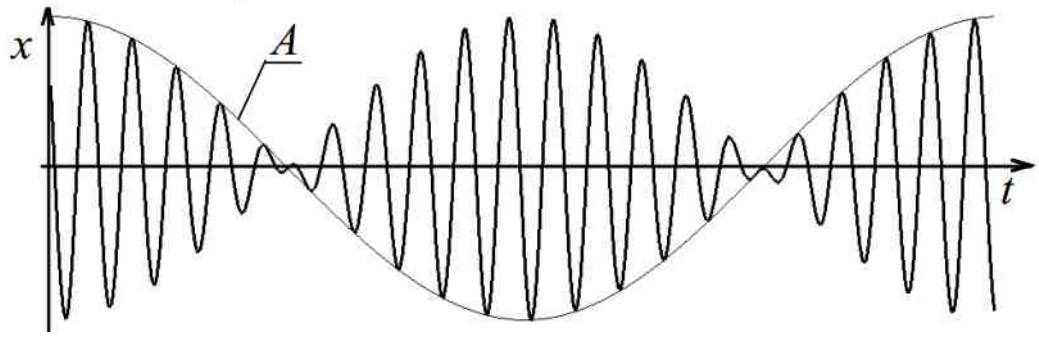


Рис. 2.3. Відображення ефекту «биття» частот

Як визначено раніше, биття відбувається тільки при певному відношенні частот. Для того щоб визначити, в якому діапазоні частот можна спостерігати биття, необхідно визначити, як змінюється характер результуючого коливання.

Було показано, що початкова фаза близьких коливань не впливає на частоту та амплітуду результуючих коливань. Тому за початок рахунку часу візьмем

момент t_0, коли фази обох складуючих коливань x_1 та x_2 співпадають; систему координат розмістим таким чином, щоб початкова фаза була рівна нулю.
Тоді закон виміру результуючого руху можна записати двома способами:

$$x = A_1 \cos(\omega_1 t) + A_2 \cos(\omega_2 t), \text{або } x = A(t) \cos(\overline{\omega} t + \varphi(t)), \qquad (2.26)$$

де $tg\varphi = \frac{A_2 - A_1}{A_1 + A_2} tg\left(\frac{1}{2}\Delta\omega t\right)$, $A^2 = A_1^2 + A_2^2 + 2A_1A_2 \cos(\Delta\omega t)$.

Вибір способу запису закону результуючого руху зв’язаний із зручністю аналізу характеру руху.

Зафіксуємо частоту ω_1 першого коливання. Розглянем, як змінюється характер результуючого руху в залежності від частоти другого коливання ω_2.

1. При умові:

$$\omega_2 = 0(|\Delta\omega| = \overline{\omega}). \qquad (2.27)$$

Рівняння руху:

$$\omega_2 = 0(|\Delta\omega| = \overline{\omega}). \qquad (2.28)$$

Гармонічний рух з постійною частотою ω_1 і з постійною амплітудою, положення рівноваги якого піднято на величину A_2 - гармонічні коливання (Рис. 2.4).

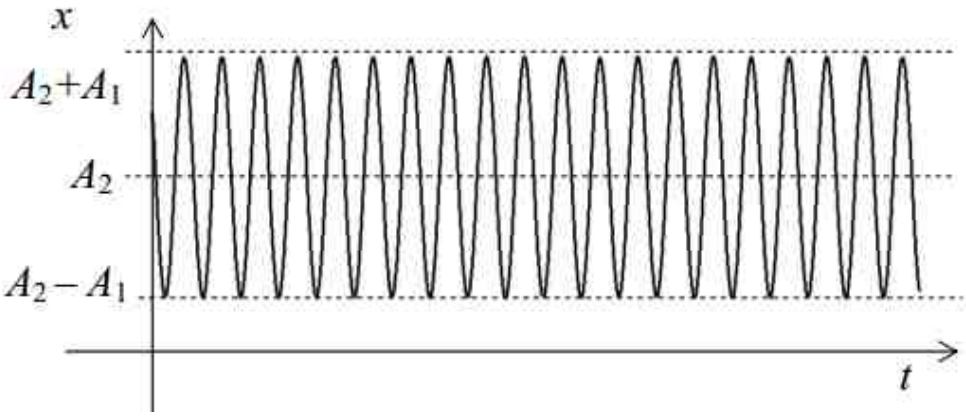


Рис. 2.4. Гармонічні коливання з постійною амплітудою

2. При умові:

$$\omega_2 > 0, \omega_2 \ll \omega_1 (|\Delta\omega| \approx \overline{\omega}). \quad (2.29)$$

Рівняння руху:

$$x = A_1 \cos(\omega_1 t) + A_2 \cos(\omega_2 t). \quad (2.30)$$

Період першого коливання менше періоду другого коливання. В період першого коливання друге коливання змінюється незначно. В період кожного періоду першого коливання результуючий рух можна розглядати, як гармонічне з зміщеним положенням рівноваги. Однак від періоду до періоду зміщення положення рівноваги змінюється.

Гармонічний рух з постійною частотою ω_1, положення рівноваги якого коливається за гармонічним законом від $-A_2$ до A_2 - коливання зі змінним положенням рівноваги (рис. 2.5).

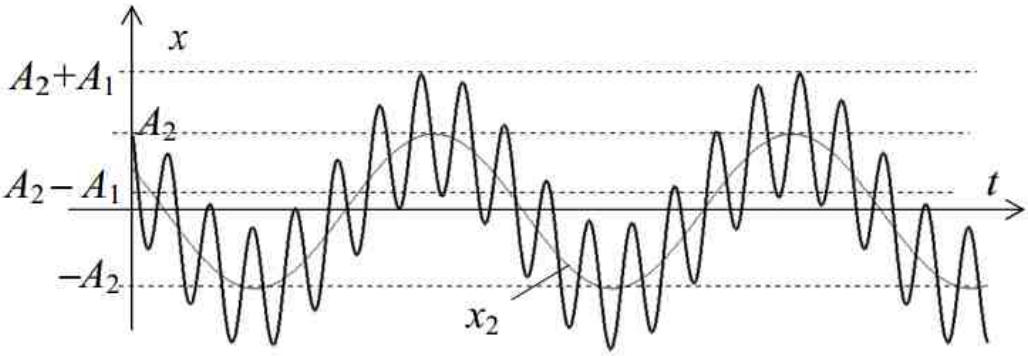


Рис. 2.5. Коливання зі змінним положенням рівноваги
з постійною частотою ω_1

3. При умові:

$$\omega_2 \gg \omega_1 (|\Delta\omega| \approx \overline{\omega}). \tag{2.31}$$

Рівняння руху:

$$x = A_1 \cos(\omega_1 t) + A_2 \cos(\omega_2 t)\,. \tag{2.32}$$

Період другого коливання багато менше періоду першого коливання. (Аналіз характеру руху аналогічний випадку 2.)

Гармонічний рух з постійною частотою ω_2, положення рівноваги якого коливається за гармонічним законом від $-A_1$ до A_1 - коливання з перемінним положенням рівноваги (Рис. 2.6).

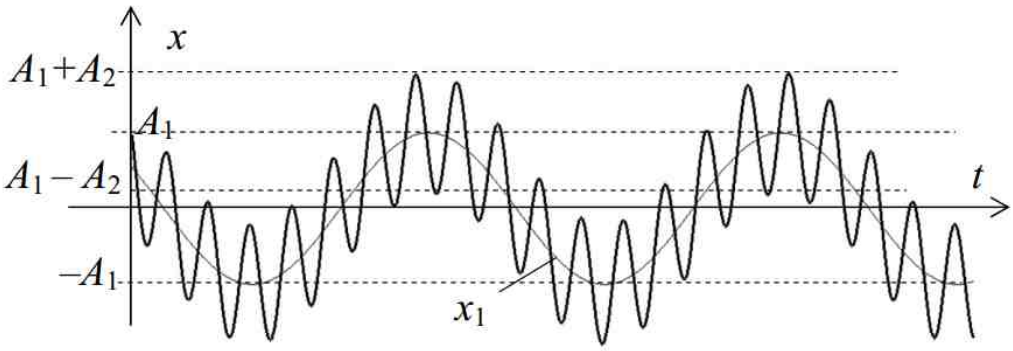


Рис. 2.6. Коливання зі змінним положенням рівноваги
з постійною частотою ω_2

4. При умові:

$$\omega_2 = \omega_1 (\Delta\omega = 0) \tag{2.33}$$

Рівняння руху:

$$x = (A_1 + A_2)\cos(\omega_1 t). \tag{2.34}$$

Складання когерентних коливань.

Гармонічний рух з постійною ω_1 і постійною амплітудою $A_1 + A_2$ - гармонічні коливання (Рис. 2.7).

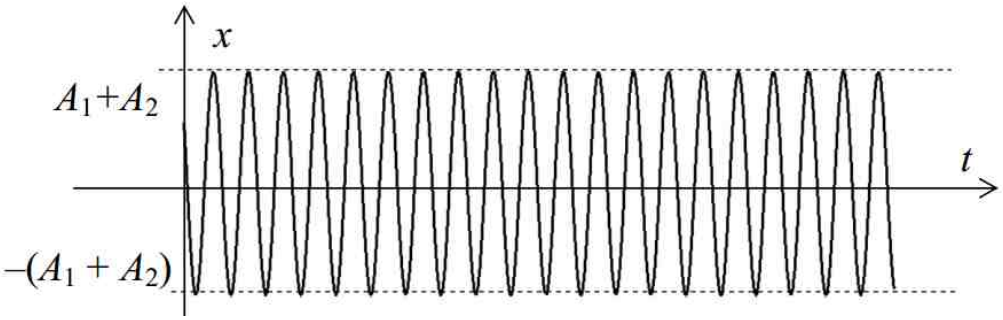


Рис. 2.7. Гармонічні коливання з постійною амплітудою $A_1 + A_2$

5. При умові:

$$\omega_2 \approx \omega_1 (|\Delta\omega| \to 0), |\Delta\omega| \ll \overline{\omega}. \tag{2.35}$$

Рівняння руху:

$$x = A(t)\cos(\Omega t)\,, A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos(\Delta\omega t), \tag{2.36}$$

$$\Omega \approx \overline{\omega} + \frac{1}{2} \cdot \frac{A_2 - A_1}{A_1 + A_2} \Delta\omega \tag{2.37}$$

Частота, а, отже, і період результуючих коливань не залежить від часу. Період зміни амплітуди багато більше періоду коливань.

Биття – гармонічний рух з постійною частотою Ω, амплітуда якого повільно змінюється від $|A_1 - A_2|$ до $A_1 + A_2$. (Рис. 2.9)

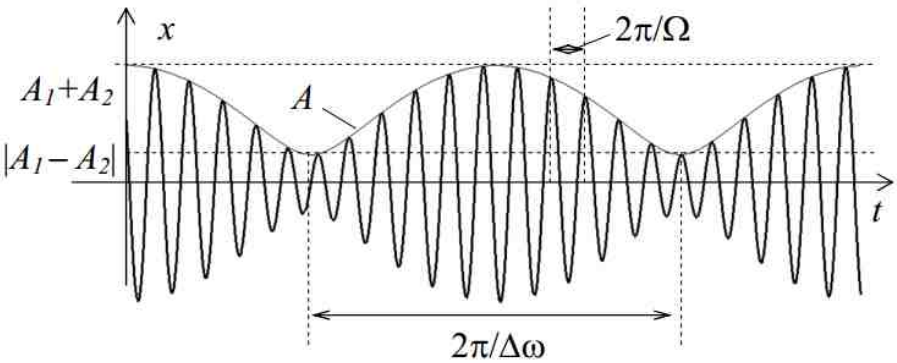


Рис. 2.8. Ефект утворення «биття» частот

6. При умові:

$$\omega_2 \neq \omega_1 \ (|\Delta\omega| > 0), \tag{2.38}$$

де $|\Delta\omega| < \overline{\omega}$ - всі види руху, що не відносяться до випадків 1-5.

Рівняння руху:

$$x = A(t)\cos\left(\overline{\omega}t + \varphi(t)\right), \tag{2.39}$$

$$A^2 = A_1^2 + A_2^2 + 2A_1A_2\cos(\Delta\omega t), \tag{2.40}$$

$$tg\varphi = \frac{A_2 - A_1}{A_1 + A_2} tg\left(\frac{1}{2}\Delta\omega t\right). \tag{2.41}$$

Різниця частот не нескінченно мала величина, тому для визначення додаткової фази $\varphi(t)$ не достатньо одного члена в розкладі в ряд тангенса

$tg\left(\frac{1}{2}\Delta\omega t\right)$. Розклад тангенса в ряд до другого порядку малості дозволяє отримати додаткову фазу у вигляді:

$$\varphi(t) \approx \frac{\Delta\omega}{2}\frac{A_2-A_1}{A_1+A_2}\left(1+\frac{1}{12}(\Delta\omega t)^2\right)\cdot t. \qquad (2.42)$$

Тобто частота коливань Ω залежить від часу:

$$\Omega \approx \overline{\omega} + \frac{\Delta\omega}{2}\frac{A_2-A_1}{A_1+A_2}\left(1+\frac{1}{12}(\Delta\omega t)^2\right). \qquad (2.43)$$

Період зміни амплітуди незначно більший періоду коливань.

Рух зі змінною частотою та змінною амплітудою – негармонічні коливання (Рис. 2.9).

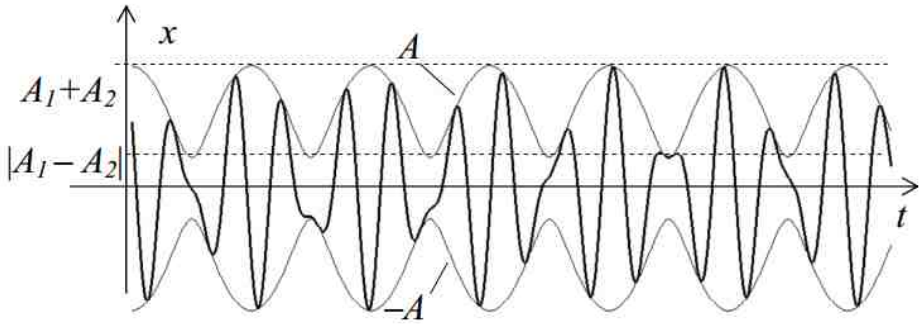


Рис. 2.9. Негармонічні коливання

Розглянуті випадки не мають чітко виражених границь на шкалі частот, а плавно переходять один в другий (рис. 2.9). Всі області частот, в яких виявляється рух одного виду, розміщені як справа, так і зліва від зафіксованої частоти ω_1 і залежать від значень цієї частоти (рис. 2.10).

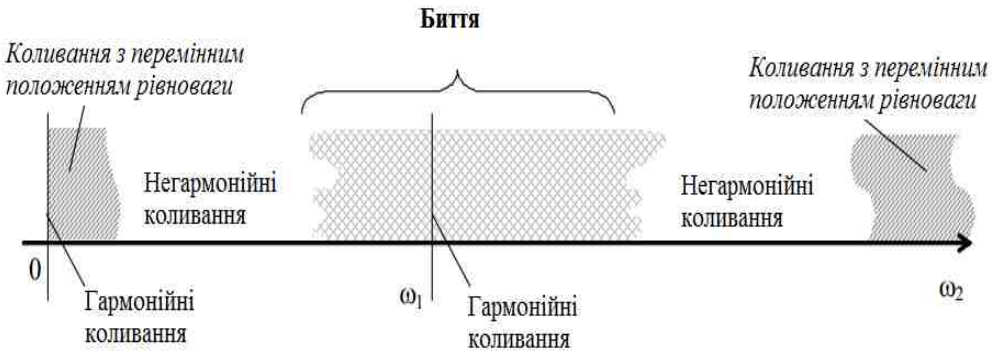


Рис. 2.10. Складання сигналів

2.3. Розробка моделі і методу захисту інформації інформації від витоку каналами високочастотного нав’язування

Виходячи з цього, запропонована нова концепція розробки методів захисту інформації від її перехоплення способами ВЧ-нав'язування – застосування захисного сигналу за допомогою «биття» і «качання» не тільки на основній, а й бічних гармоніках, за допомогою чого здійснюється погрішення параметрів та спотворення небезпечного сигналу [65-67].

Узагальнюючи вищезгадану інформацію, явище виникнення биття між двома близькими за частотою гармонічними коливаннями має вигляд:

$$s_{\Sigma}(t) = s_1(t) + s_2(t) = A_{m1}\sin\omega_1 t + A_{m2}\sin\omega_2 t = 2A_{m1}A_{m2}\cos\frac{\omega_1-\omega_2}{2}t\cdot\sin\frac{\omega_1+\omega_2}{2}t \quad (2.44)$$

В результаті взаємодії двох таких коливань виникають нові коливання з частотою

$$\omega = \frac{\omega_1+\omega_2}{2} \quad (2.45)$$

і змінною амплітудою, максимальні значення якої повторюються з частотою

$$\Omega = \omega_1 - \omega_2 . \qquad (2.46)$$

Це явище можна використовувати для захисту від ВЧ-нав'язування. Дійсно, якщо виміряти частоту зондуючого коливання, то завжди можна випромінити у простір (або направити в струмопровідне середовище) коливання з частотою, близькою до частоти зондуючого сигналу ВЧ-нав'язування. В результаті їх взаємодії утворюються биття, однією з властивостей яких є зміна фази результуючого коливання при переході обвідної через нуль.

Оскільки при перехопленні інформації даними способом можуть виникати як амплітудна, так частотна і фазова модуляція перевипроміненого сигналу, то необхідно вжити заходів до блокування можливості одержання інформації при використанні будь-якої з цих модуляцій. Завадою для сигналів з фазовою модуляцією буде зміна фази результуючого коливання в момент переходу його амплітуди через нуль. Але якщо такі моменти зберегти постійними (тобто вибрати постійну частоту захисного коливання), то систему перехоплення інформації можна легко адаптувати до такої завади. Тому має сенс частоту захисного коливання зробити хитною в певних невеликих межах, які забезпечують виникнення явища биття. Для цього можна хитати частоту вліво і вправо від середнього значення, наприклад, за лінійним законом. А для внесення хаотичності в процес хитання частоти, основний (задавальний) лінійний керуючий сигнал можна скласти з випадковим низькочастотним сигналом, що забезпечить захист і від частотно-модульованого, і амплітудно-модульованого перехоплення інформації [63, 64].

Для остаточного спотворення інформації, випромінюваний захисний сигнал можна скласти з іншим випадковим сигналом малого рівня (щоб зберегти основну частоту захисного гармонічного сигналу), що перекриває заданий діапазон частот [63, 64].

Розглянемо модель процесів, які при цьому відбуваються. Для зручності скористаємося методом суперпозиції, використовуючи в якості первісного співвідношення (2.28).

Позначимо захисний сигнал як $s_1(t)$, а небезпечний сигнал як $s_2(t)$ і розглянемо їх взаємодію.

Спочатку запишемо захисний сигнал, випромінюваний в середовище поширення зондуючого сигналу, як

$$s_1(t) = [A_{m1} + \eta(t)]\sin(\omega_1 + \omega_\mu + \omega_P)t \qquad (2.47)$$

де A_{m1} – амплітуда захисного коливання,

$\eta(t)$ – випадковий сигнал, просумований з вихідним захисним коливанням,

ω_μ – миттєве значення частоти випадкового сигналу, просумоване з лінійним сигналом управління зміщенням частоти генератора захисного коливання,

ω_P – частота першої гармоніки лінійного керуючого сигналу.

Виходячи з співвідношень (2.29) і (2.30) можна записати частоту коливання, що утворюється в результаті взаємодії сигналів $s_1(t)$ і $s_2(t)$, як

$$\omega = \frac{\omega_3 + \omega_2}{2}, \qquad (2.48)$$

де

$$\omega_3 = \omega_1 + \omega_\mu + \omega_P, \qquad (2.49)$$

а частоту повторення максимальних значень амплітуди результуючого коливання як

$$\Omega = \omega_3 - \omega_2. \qquad (2.50)$$

При цьому амплітуда результуючого коливання запишеться як

$$A_{\Sigma} = 2\left[A_{m1} + \eta(t)\right] \cdot A_{m2}, \tag{2.51}$$

а саме результуюче коливання як

$$s_{\Sigma}(t) = A_{\Sigma} \cos\frac{\omega_3 - \omega_2}{2} t \cdot \sin\frac{\omega_3 + \omega_2}{2} t. \tag{2.52}$$

Таким чином, в середовище, використовуване для подачі зондуючого коливання, буде введена активна завада, що перетворює сигнал ВЧ-нав'язування в сигнал, фаза, частота і амплітуда якого носять випадковий характер, і робить його непридатним для перехоплення сигналу та відтворення з нього корисної інформації [63, 64].

Відповідно, при певному виборі середньої частоти захисного коливання і діапазону її зміни можна досягти захоплення цієї частоти генератором ВЧ-нав'язування.

Задача формування радіоелектронних завад одночасно на декількох гармоніках несійної частоти та забезпечення на кожній з них заданих значень індексів модуляції є непростою для вирішення технічною задачею.

Спосіб формування радіосигналів з кутовою модуляцією без обмеження величин індексів модуляції одночасно на кількох гармоніках коливання несійної частоти викладено в [68]. Нами розглядається перспектива застосування квадратурних формувачів радіосигналів для удосконалення захисних впливів на сформовані високочастотним нав'язуванням небезпечні сигнали.

Перевагою квадратурних формувачів є можливість здійснення в них модуляції у досить широкому діапазоні зміни як модулюючих, так і несійних частот без перебудови схеми завдяки відсутності у ній керованих реактивних елементів та частотно-вибіркових кіл. Разом з тим, необхідна точність

формування завадових радіосигналів як з малими, так і з високими значеннями індексів модуляції напряму залежить від точності реалізації періодичних функцій $\cos(Msin\Omega t)$ і $\sin(Msin\Omega t)$ в низькочастотній області.

Спосіб підвищення індексу кутової модуляції одночасно на першій, другій та третій гармоніках коливання несійної частоти базується на обчисленні косинусної та синусної функцій модулюючої напруги, подвоєннях аргументів косинусної та синусної функцій, квадратурному множенні та квадратурному перемноженні і підсумовуванні.

На рис. 1 наведено структурну схему, що реалізує квадратурний спосіб підвищення індексу кутової модуляції. Для реалізації функціональних перетворювачів синуса та косинуса модулюючого сигналу в основному використовуються аналітичні, табличні, таблично-алгоритмічні методи, а також їх комбінації [69].

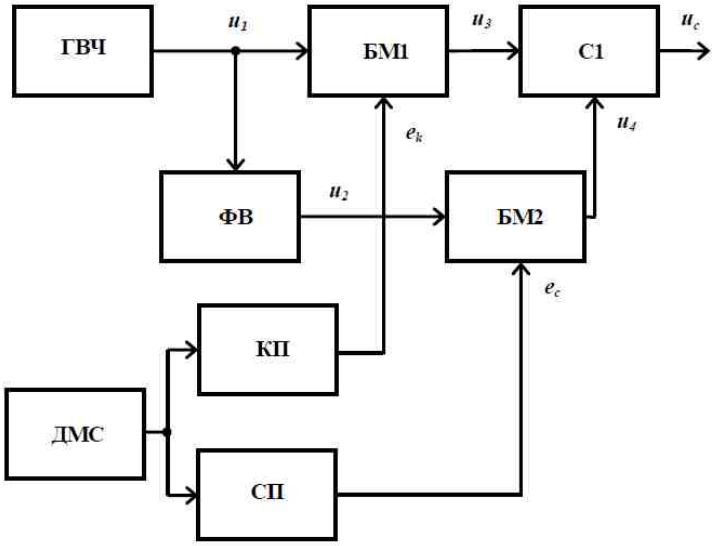


Рис. 2.11. Структурна схема, що реалізує квадратурний спосіб підвищення індексу кутової модуляції [68]: ГВЧ – генератор високої частоти; БМ1 та БМ2 – балансні модулятори; ФВ – високочастотний фазообертач на π/2; С1 – високочастотний лінійний суматор; ДМС – джерело модулюючого сигналу; КП – косинусний перетворювач; СП – синусний перетворювач.

Квадратурний спосіб включає:

формування за допомогою високочастотного генератора та фазообертача на π/2 квадратурних складових, що описуються, відповідно, виразами [69]:

$$u_1 = U_1 cos\omega t \tag{2.53}$$

$$u_2 = -U_1 cos\omega t \tag{2.54}$$

формування за допомогою косинусного та синусного перетворювачів модулюючої напруги, відповідно, керуючих сигналів:

$$e_k = E_y \cos\left[m_\varphi sin\Omega t\right] \tag{2.55}$$

$$e_c = E_y \sin\left[m_\varphi sin\Omega t\right] \tag{2.56}$$

квадратурне перемноження високочастотних та низькочастотних складових (2.53) з (2.55) і (2.54) з (2.56) у балансних модуляторах з коефіцієнтами

$k_{\text{БМ}} = 1$;

складання високочастотних квадратурних складових у лінійному суматорі, у результаті якого формується вихідний фазомодульований сигнал:

$$u_c = U_1 E_y\left[cos\omega t cos\left(m_\varphi sin\Omega t\right) - sin\omega t sin\left(m_\varphi sin\Omega t\right)\right] = U_{c1}\cos(\omega t + m_\varphi sin\Omega t)\ , \tag{2.57}$$

де $U_{c1} = U_1 E_y$ – постійна амплітуда.

З формул (2.53) - (2.57) випливає, що в структурній схемі на рис. 2.11 можливе отримання фазомодульованих сигналів з будь-якими довільно заданими індексами модуляції m_φ.

На 1-му та 2-му етапах виконують, відповідно, перше множення коливання несійної частоти (1-й вихід) та формування його квадратури:

$$u_{ус1} = (U_1 cos\omega t)^2 - (U_1 sin\omega t)^2 = U_1^2 cos2\omega t \quad (2.58)$$

$$u_{фв1} = -U_1^2 cos2\omega t \quad (2.59)$$

3-й та 4-й етапи реалізують перші синфазне та квадратурне перемноження 2-х гармонік коливань несійної частоти (2.58) та (2.59), відповідно, із складовими (2.55) та (2.56):

$$u_{сп1} = U_1^2 cos2\omega t \times E_1 \cos[m_\varphi sin\Omega t], \quad (2.60)$$

$$u_{кп1} = -U_1^2 sin2\omega t \times E_1 \sin[m_\varphi sin\Omega t], \quad (2.61)$$

На 5-му етапі виробляють перше лінійне алгебраїчне підсумовування результатів (2.60) та (2.61) (2-й вихід):

$$u_{с1} = U_1^2 cos2\omega t \times E_1 \cos\left[m_\varphi sin\Omega t\right] - U_1^2 sin2\omega t \times E_1 \sin\left[m_\varphi sin\Omega t\right] = \\ = U_{c1} \cos(2\omega t + m_\varphi sin\Omega t), \quad (2.62)$$

де U_{c1} — постійна амплітуда.

На 6-му та 7-му етапах проводять, відповідно, друге множення ФМС (3-й вихід) та формування його квадратури:

$$u_{ус2} = (U_{c1} \cos(\omega t + m_\varphi sin\Omega t))^2 - (U_{c1} \sin(\omega t + m_\varphi sin\Omega t))^2 = \\ = U_{c1}^2 \cos\left(2\omega t + +2m_\varphi sin\Omega t\right), \quad (2.63)$$

$$u_{фв2} = -U_{c1}^2 \sin\left(2\omega t + 2m_\varphi sin\Omega t\right). \quad (2.64)$$

8-й та 9-й етапи реалізують перші синфазне та квадратурне перемноження сигналів (2.63) та (2.64), відповідно, із складовими (2.55) та (2.56):

$$u_{\text{сп}2} = U_{c1}^2 \cos\left(2\omega t + 2m_\varphi sin\Omega t\right) \times E_1 \cos\left[m_\varphi sin\Omega t\right], \quad (2.65)$$

$$u_{\text{кп}2} = -U_{c1}^2 \sin\left(2\omega t + 2m_\varphi sin\Omega t\right) \times E_1 \sin\left[m_\varphi sin\Omega t\right]. \quad (2.66)$$

На 10-му етапі проводять друге лінійне алгебраїчне підсумовування результатів творів (2.65) та (2.66) (4-й вихід):

$$u_{c2} = U_{c1}^2 \cos\left(2\omega t + 2m_\varphi sin\Omega t\right) \times E_1 \cos\left[m_\varphi sin\Omega t\right] - U_{c1}^2 \sin\left(2\omega t + 2m_\varphi sin\Omega t\right) \times E_1 \sin\left[m_\varphi sin\Omega t\right] = U_{c2} \cos\left(2\omega t + 3m_\varphi sin\Omega t\right), \quad (2.67)$$

де U_{c2} — постійна амплітуда.

11-й та 12-й етапи реалізують треті синфазне та квадратурне перемноження 2-х гармонік коливань несійної частоти (2.58) та (2.59), відповідно, із складовими $e_{k3} = E_3 \cos[4m_\varphi sin\Omega t]$, $e_{c3} = E_3 \sin[4m_\varphi sin\Omega t]$, алгоритми отримання яких описані в [70]:

$$u_{\text{сп}3} = U_1^2 cos2\omega t \times E_3 \cos[4m_\varphi sin\Omega t], \quad (2.68)$$

$$u_{\text{кп}3} = -U_1^2 sin2\omega t \times E_3 \sin\left[4m_\varphi sin\Omega t\right]. \quad (2.69)$$

На 13-му етапі виробляють третє лінійне алгебраїчне підсумовування результатів творів (2.68) та (2.69) (5-й вихід):

$$u_{c3} = U_1^2 cos2\omega t \times E_3 \cos\left[4m_\varphi sin\Omega t\right] - U_1^2 cos2\omega t \times E_3 \sin\left[4m_\varphi sin\Omega t\right] =$$
$$= U_{c3} \cos\left(2\omega t + 4m_\varphi sin\Omega t\right), \quad (2.70)$$

де U_{c3} — постійна амплітуда.

На 14-му та 15-му етапах проводять, відповідно, третє множення коливання несійної частоти (6-й вихід) та формування його квадратури:

$$u_{yc3} = U_1 cos\omega t \times U_1^2 \cos 2\omega t - U_1 \sin\omega t \times U_1^2 \cos 2\omega t = U_{c4}^2 cos3\omega t, \quad (2.71)$$

$$u_{\text{фв3}} = -U_{c4}^2 sin3\omega t. \quad (2.72)$$

16-й та 17-й етапи реалізують четверті синфазне та квадратурне перемноження 2-х гармонік коливань несійної частоти (2.71) та (2.72), відповідно, із складовими (2.55) та (2.56):

$$u_{\text{сп4}} = U_{\text{c4}}^2 cos3\omega t \times E_1 cos\left[m_\varphi sin\Omega t\right], \quad (2.73)$$

$$u_{\text{кп4}} = -U_{\text{c4}}^2 sin3\omega t \times E_1 sin\left[m_\varphi sin\Omega t\right]. \quad (2.74)$$

На 18-му етапі проводять четверте лінійне алгебраїчне підсумовування результатів добутків (2.73) та (2.74) (7-й вихід):

$$u_{\text{c4}} = U_{\text{c4}}^2 cos3\omega t \times E_1 cos\left[m_\varphi sin\Omega t\right] - U_{\text{c4}}^2 sin3\omega t \times E_1 sin\left[m_\varphi sin\Omega t\right] =$$
$$= U_{c4} \cos\left(3\omega t + m_\varphi sin\Omega t\right), \quad (2.75)$$

де U_{c4} — постійна амплітуда.

19-й та 20-й етапи реалізують п'яті синфазне та квадратурне перемноження 2-х гармонік коливань несійної частоти (2.75) та (2.76),

відповідно, із складовими $e_{k2} = E_2 \cos\left[2m_\varphi sin\Omega t\right], e_{c2} = E_2 \sin\left[2m_\varphi sin\Omega t\right]$, алгоритми отримання яких описані в [70]:

$$u_{\text{сп}5} = U_{\text{c}4}^2 cos3\omega t \times E_2 \cos\left[2m_\varphi sin\Omega t\right], \tag{2.76}$$

$$u_{\text{кп}5} = -U_{\text{c}4}^2 sin3\omega t \times E_2 \sin\left[2m_\varphi sin\Omega t\right]. \tag{2.77}$$

На 21-му та 22-му етапах проводять п'яте лінійне алгебраїчне підсумовування результатів добутків (2.76) і (2.77) (8-й вихід) та формування квадратури отриманого ФМС:

$$u_{\text{c}5} = U_{\text{c}4}^2 cos3\omega t \times E_2 \cos\left[2m_\varphi sin\Omega t\right] - U_{\text{c}4}^2 sin3\omega t \times E_2 \sin\left[2m_\varphi sin\Omega t\right] = \\ = U_{c5} \cos\left(3\omega t + 2m_\varphi sin\Omega t\right), \tag{2.78}$$

де U_{c5} — постійна амплітуда,

$$u_{\text{фв}4} = -U_{c5} \sin(3\omega t + 2m_\varphi sin\Omega t). \tag{2.79}$$

23-й та 24-й етапи реалізують шості синфазне та квадратурне перемноження сигналів (2.78) та (2.79), відповідно, із складовими (2.55) та (2.56):

$$u_{\text{сп}6} = U_{c5} \cos(3\omega t + 2m_\varphi sin\Omega t) \times E_1 \cos\left[m_\varphi sin\Omega t\right], \tag{2.80}$$

$$u_{\text{кп}6} = -U_{c5} \sin(3\omega t + 2m_\varphi sin\Omega t) \times E_1 \sin\left[m_\varphi sin\Omega t\right]. \tag{2.81}$$

На 25-му етапі проводять шосте лінійне алгебраїчне підсумовування результатів творів (2.80) та (2.81) (9-й вихід):

$$u_{c6} = U_{c5}\cos\left(3\omega t + 2m_{\varphi}sin\Omega t\right) \times E_1 \cos\left[m_{\varphi}sin\Omega t\right] - U_{c5}\sin\left(3\omega t + \right.$$
$$\left. +2m_{\varphi}sin\Omega t\right) \times E_1 \sin\left[m_{\varphi}sin\Omega t\right] = U_{c6}\cos\left(3\omega t + 3m_{\varphi}sin\Omega t\right), \quad (2.82)$$

де U_{c6} — постійна амплітуда.

26-й та 27-й етапи реалізують сьомі синфазне та квадратурне перемноження сигналів (2.81) та (2.82), відповідно, із складовими$e_{k3} = E_3 \cos\left[4m_{\varphi}sin\Omega t\right], e_{c3} = E_3 \sin\left[4m_{\varphi}sin\Omega t\right]$, алгоритми отримання яких описані в [70, 71]:

$$u_{\text{сп}7} = U_{\text{c}4}^2\cos 3\omega t \times E_3 \cos\left[4m_{\varphi}sin\Omega t\right], \quad (2.83)$$

$$u_{\text{кп}7} = -U_{\text{c}4}^2 sin3\omega t \times E_3 \sin\left[4m_{\varphi}sin\Omega t\right]. \quad (2.84)$$

На 28-му етапі проводять сьоме лінійне алгебраїчне підсумовування результатів (2.85) та (2.86) (10-й вихід):

$$u_{c7} = U_{\text{c}4}^2\cos 3\omega t \times E_3 \cos\left[4m_{\varphi}sin\Omega t\right] - U_{\text{c}4}^2 sin3\omega t \times E_3 \sin\left[4m_{\varphi}sin\Omega t\right] =$$
$$= U_{c7}\cos\left(3\omega t + 4m_{\varphi}sin\Omega t\right), \quad (2.85)$$

де U_{c7} – постійна амплітуда.

Для N-кратного збільшення кількості етапів множень коливання несучої частоти у поєднанні з операціями квадратурних перемножень та алгебраїчних лінійних підсумовувань для вихідних ФМС можна записати:

$$u_{cN} = U_{cN}\cos(N\omega t + Nm_{\varphi}sin\Omega t), \quad (2.88)$$

де U_{cN} – постійна амплітуда.

З формул (2.58), (2.62), (2.63), (2.67), (2.70), (2.71), (2.75), (2.76), (2.80), (2.83) і (2.84) випливає, що пропорційно збільшенню кількості етапів множень коливання несучої частоти у поєднанні із збільшенням кількості етапів квадратурних перемножень та лінійних підсумовувань відбувається збільшення кількості гармонік коливання несійної частоти з одночасним збільшенням на них (гармоніках) значень індексів модуляції вихідних ФМС за відсутності прояву паразитних амплітудної і фазової модуляцій.

На Рис. 2.12 *а* – *д* наведені спектри на виходах етапів моделювання способу (етапи формування ФМС на 2-й і 3-й гармоніках коливання несійної частоти, в порівнянні з 1-й гармонікою, відзначені цифрами): рис. 2.12, *а* – відповідає 1-му та 14-му етапам; рис. 2.12, *б* – 5-му і 18-му етапам; рис. 2.12, *в* – 6-му та 21-му етапам; рис. 2.12, *г* – 10-му та 25-му етапам; рис. 2.12, *д* – 13-му і 28-му етапам.

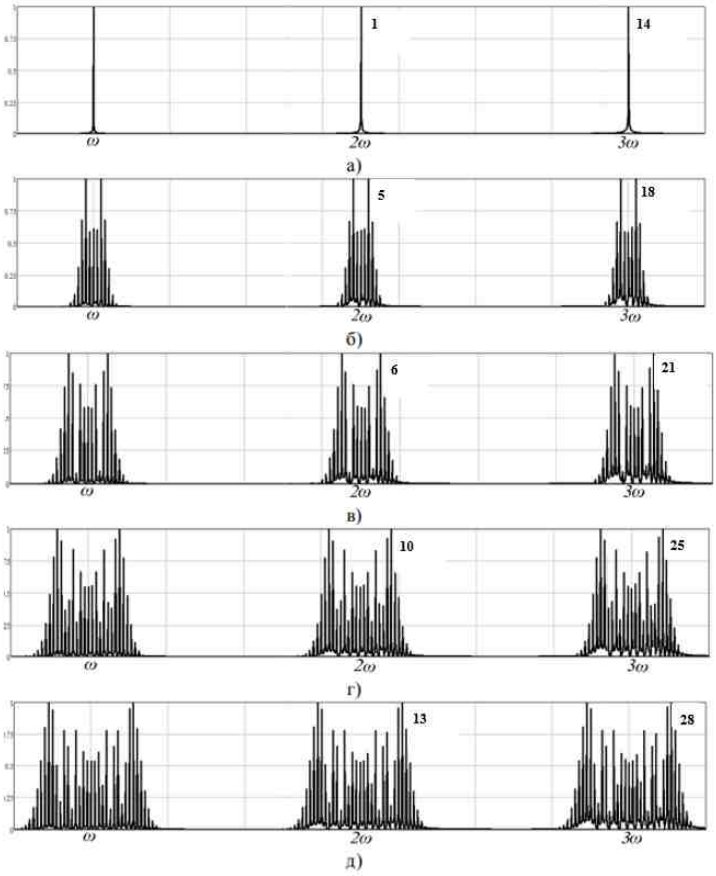


Рис. 2.12. [72] Етапи моделювання способу підвищення індексу кутової модуляції (цифрами від 1 до 28 позначені етапи формування вихідних фазомодульованих сигналів)

Отже, для підвищення ефективності захисту інформації від перехоплення пропонується метод високочастотного нав’язування, який буде здійснювати формування захисних сигналів не тільки відносно основної частоти, а й відносно гармонік небезпечного сигналу.

Висновки до розділу 2

1. Досліджено основні принципи блокування перехоплення інформації методами високочастотного нав’язування та принцип активного методу захисту інформації від витоку каналами високочастотного нав’язування. Виявлено залежність якості блокування перехоплення інформації від зміни параметрів захисного сигналу, який впливає на небезпечний, тим самим спотворюючи його. Явище «биття» коливань спостерігається при складанні двох гармонічних коливань з близькими частотами і полягає в амплітудній низькочастотній модуляції сумарного високочастотного коливання.

2. Вперше запропоновано модель блокування процесу перехоплення інформації каналами високочастотного нав’язування, яка забезпечує захист інформації від витоку каналами високочастотного нав’язування шляхом руйнування інформативних параметрів небезпечних сигналів.

3. Удосконалено модель захисту інформації від витоку каналами високочастотного нав’язування, яка, на відміну від існуючих, забезпечує руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках небезпечного зондуючого сигналу.

4. Запропоновано методу захисту інформації, який здійснює формування радіоелектронних завад одночасно на декількох гармоніках несійної частоти та забезпечує на кожній з них задані значення індексів модуляції, що дає основу для його використання при формуванні захисних впливів на сформовані високочастотним нав'язуванням небезпечні сигнали, де потрібно як підвищення коефіцієнта якості шумових завад з кутовою модуляцією, так і збільшення дистанції впливу.

РОЗДІЛ 3
СИНТЕЗ МОДЕЛЕЙ І МЕТОДІВ ІМІТАЦІЙНИХ ДОСЛІДЖЕНЬ

3.1. Розробка моделі і методики дослідження параметрів завадових сигналів шляхом математичного та імітаційного моделювання

Головними завданнями імітаційних досліджень є визначення оптимальних параметрів захисних сигналів, забезпечення максимального ступеню ефективності запропонованого методу, визначення максимального рівня цієї ефективності.

Питання організації постановки експерименту щодо визначення вихідних параметрів запропонованої авторами системи захисту інформації від її несанкціонованого перехоплення методами ВЧ-нав'язування розглянуто в [46].

Як було сказано вище, гармонічний небезпечний сигнал описується наступним рівнянням:

$$x_1 = Acos\omega_1 t \tag{3.1}$$

Відповідно захисний сигнал має вигляд:

$$x_2 = Acos\omega_2 t \tag{3.2}$$

Для проведення дослідження ефекту "биття" икористовуємо рівняння результуючого сигналу, яке має наступний вигляд:

$$x(t) = 2Acos\Delta\omega t cos\omega t, \tag{3.3}$$

де $\Delta\omega = \frac{\omega_1 - \omega_2}{2}$, $\omega = \frac{\omega_1 + \omega_2}{2}$.

Ефективне «биття» сигналів спостерігається тільки при певній різниці частот небезпечного та захисного сигналів, забезпечуючи спотворення параметрів небезпечного сигналу.

На Рис. 3.3 наведено зображення ефекту «биття» гармонічних коливань з близькими частотами (гармонічні коливання з постійною частотою Ω, амплітуда якого повільно змінюється від $|A_1 - A_2|$ до $A_1 + A_2$) [72 - 74].

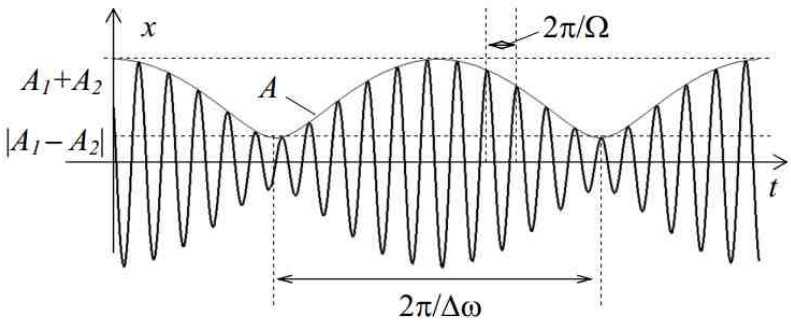


Рис. 3.1. Зображення ефекту «биття» гармонічних коливань з близькими частотами

За допомогою математичного моделювання в середовищі MathCad 14 [75] визначено оптимальний діапазон значень захисних сигналів для забезпечення явища «биття»: 0,001 МГц ≤ Δω ≤ 1 МГц, де Δω – різниця частот небезпечного та захисного сигналів [76, 77].

На наступних рисунках показано декілька варіантів взаємодії небезпечного та захисного сигналів:

Як видно з рис. 3.4, при |ω1 – ω2|>1 МГц, де ω1 = 800 МГц – частота небезпечного сигналу, а ω2 – частота захисного сигналу, "биття" частот практично відсутнє і руйнування інформативних параметрів небезпечного сигналу не забезпечується.

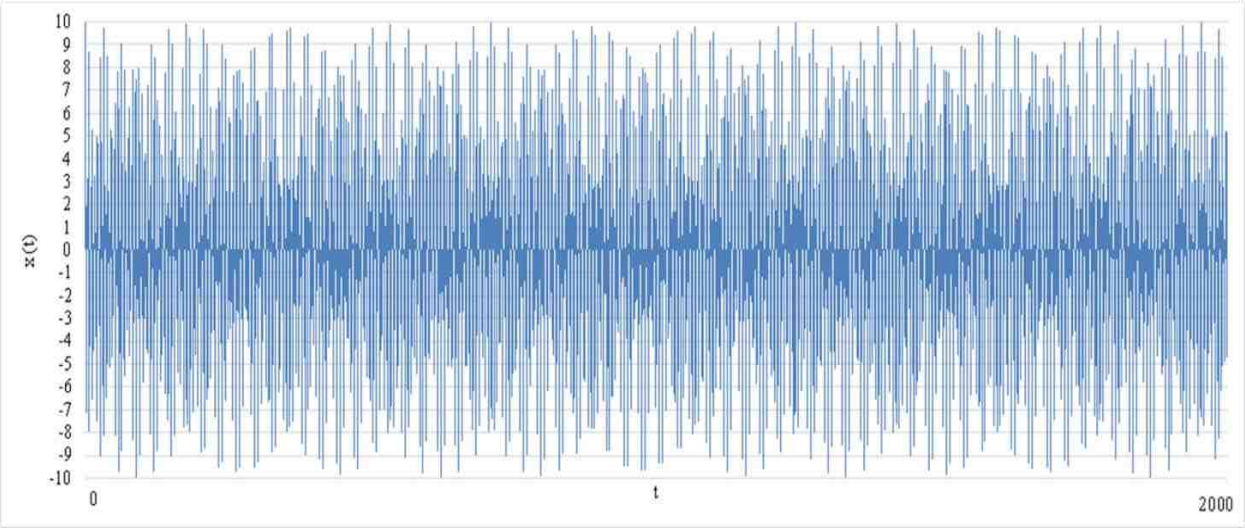


Рис. 3.2. Відсутність ефекту «биття» при умові |ω1 – ω2|=1.5 МГц

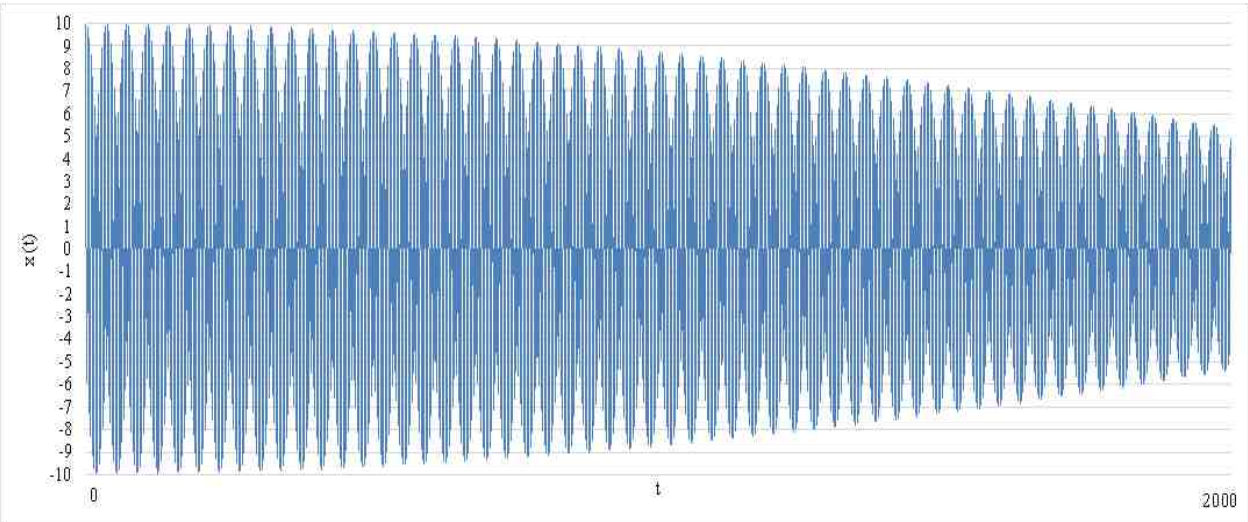


Рис. 3.3. Початок появи ефекту «биття» при умові |ω1 – ω2|=1 Гц

Натомість при |ω1 – ω2|=0,01 МГц можна чітко побачити "биття" частот, що чергу свідчить про забезпечення руйнації інформативних параметрів небезпечних сигналів (Рис. 3.4).

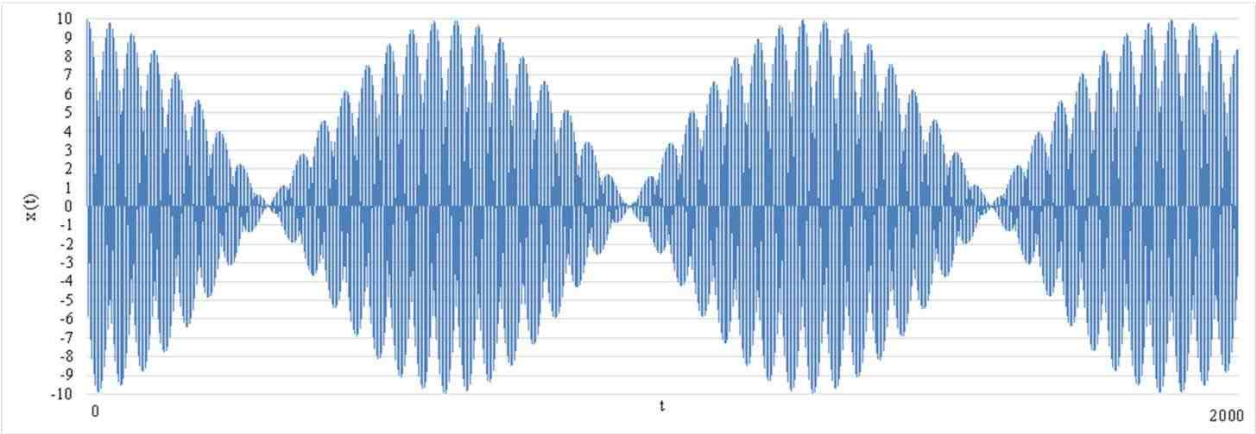


Рис. 3.4. Наявність ефекту «биття» при умові |ω1 – ω2|=10 кГц

За підсумками проведення математичного моделювання в середовищі MathCad 14 зроблено наступні висновки:

1. Підтверджено теоретичні відомості про утворення ефекту «биття» частот.

2. Досліджено утворення ефекту «биття» частот в діапазоні 0 – 2 ГГц.

3. Досліджено максимальну ефективність запропонованого методу та знайдено оптимальний діапазон (0,001 МГц ≤ Δω ≤ 1 МГц).

Також було проведено імітаційні дослідження для всіх видів модуляції з використанням пакету LabVIEW версії 20.0.1 [78 - 82].

Дослідження впливу захисних сигналів на амплітудно-модульований небезпечний сигнал: метою першого дослідження було перевірити ефективність впливу захисних сигналів на небезпечний сигнал з амплітудною модуляцією (Рис. 3.6.а). Дослідження виконувались за блок-схемою, поданою на Рис. 3.5.

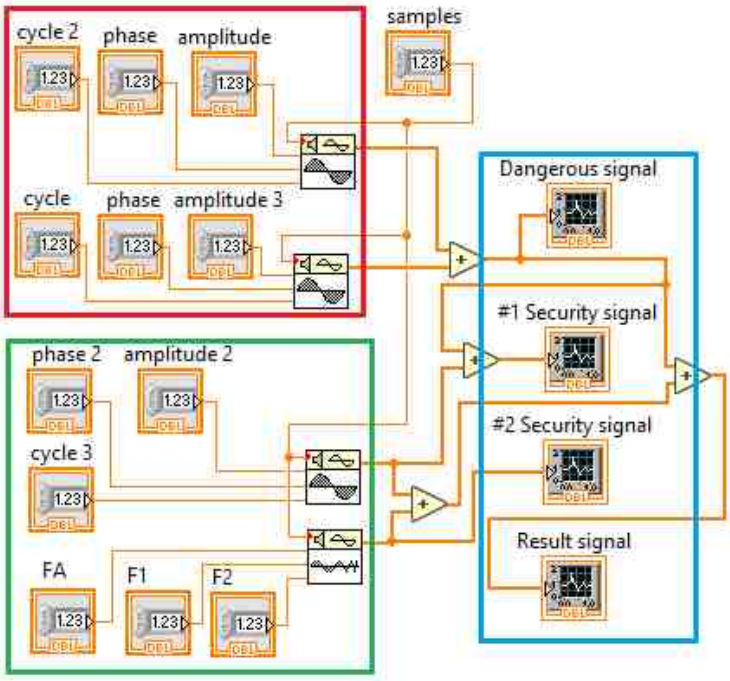


Рис. 3.5. Блок-схема дослідження впливу захисних сигналів на амплітудно-модульований небезпечний сигнал

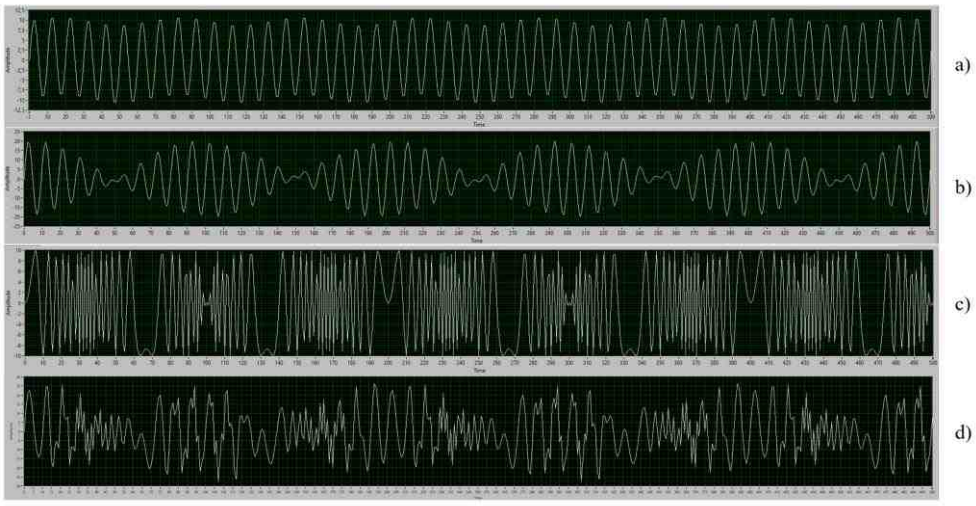


Рис. 3.6. Зображення сигналів дослідження впливу захисних сигналів на амплітудно-модульований небезпечний сигнал. (a – зображення небезпечного сигналу з амплітудною модуляцією, b – зображення результуючого небезпечного сигналу під впливом першого захисного сигналу, c – зображення другого захисного сигналу, d – зображення результуючого небезпечного сигналу)

Беручи до уваги дані, отримані в результаті дослідження, а саме – зображення результуючого сигналу (рис. 3.6.d), можна зробити висновок про ефективне руйнування інформаційної складової небезпечного сигналу з амплітудною модуляцією.

Дослідження впливу захисних сигналів на фазово-модульований небезпечний сигнал: метою другого дослідження було перевірити ефективність впливу захисних сигналів на небезпечний сигнал з фазовою модуляцією (Рис. 3.8.a).

Дослідження виконувались за блок-схемою, поданою на Рис. 3.7.

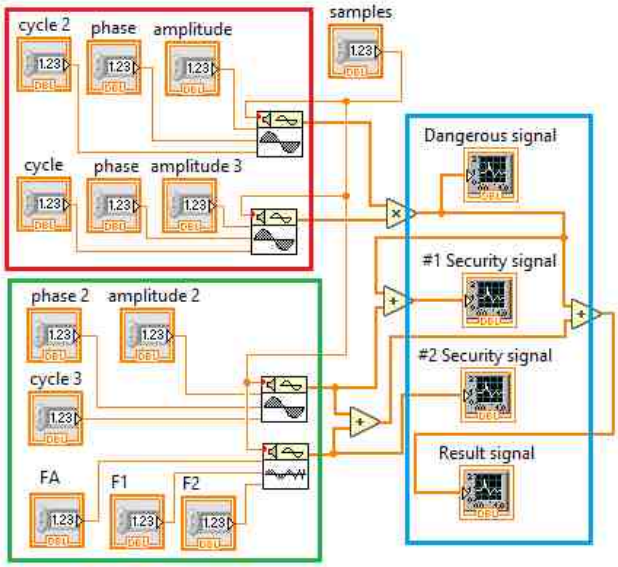


Рис. 3.7. Блок-схема дослідження впливу захисних сигналів на фазово-модульований небезпечний сигнал

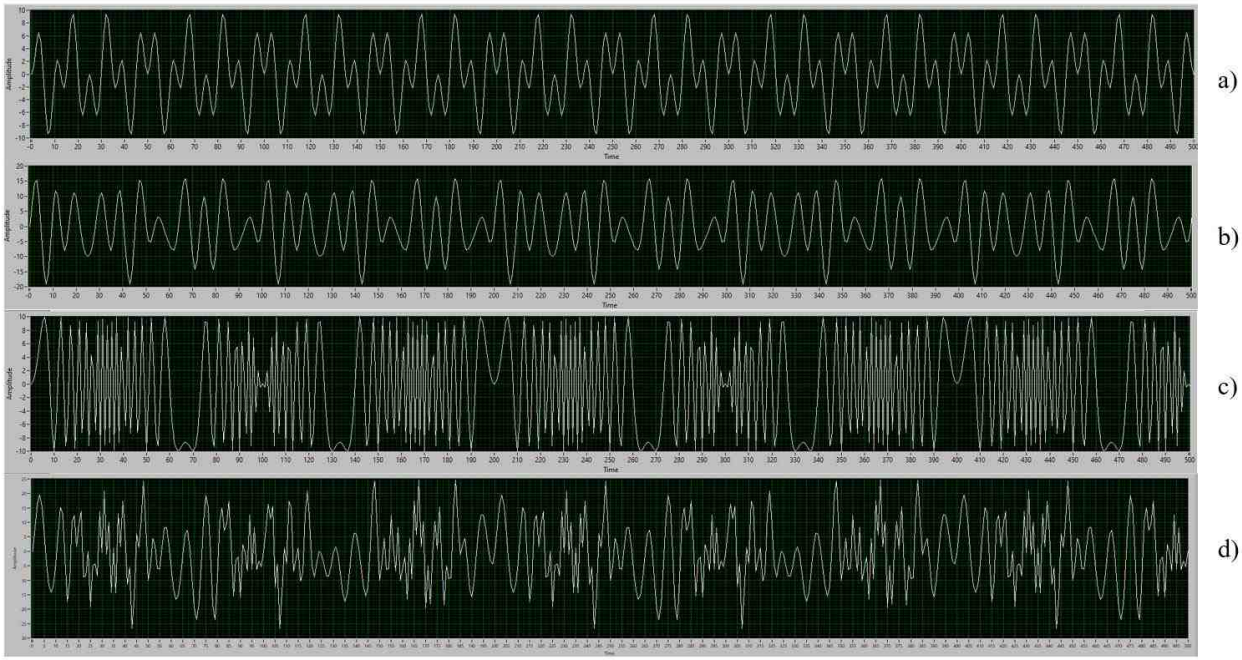


Рис. 3.8. Зображення сигналів дослідження впливу захисних сигналів на фазово-модульований небезпечний сигнал. (a – зображення небезпечного сигналу з фазовою модуляцією, b – зображення результуючого небезпечного сигналу та першого захисного сигналу, c – зображення другого захисного сигналу, d – зображення результуючого сигналу)

Беручи до уваги дані, отримані в результаті дослідження, а саме – зображення результуючого сигналу (рис. 3.8.d), можна зробити висновок про ефективне руйнування інформаційної складової небезпечного сигналу з фазовою модуляцією.

Дослідження впливу захисних сигналів на частотно-модульований небезпечний сигнал: метою третього дослідження було перевірити ефективність впливу захисного сигналу на частотно-модульований небезпечний сигнал (Рис. 3.10.a).

Дослідження виконувались за блок-схемою, поданою на Рис. 3.9.

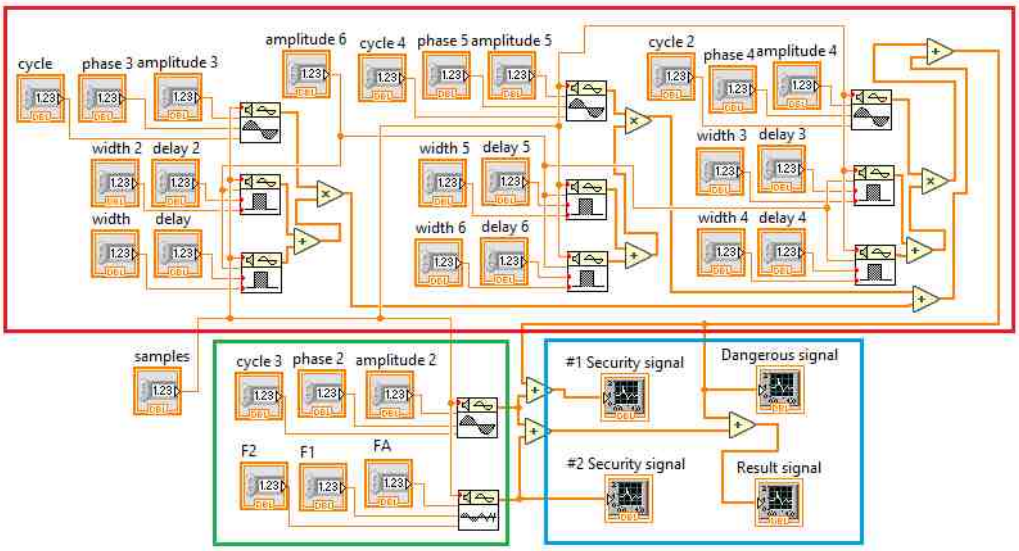


Рис. 3.9. Блок-схема дослідження впливу захисних сигналів на частотно-модульований небезпечний сигнал

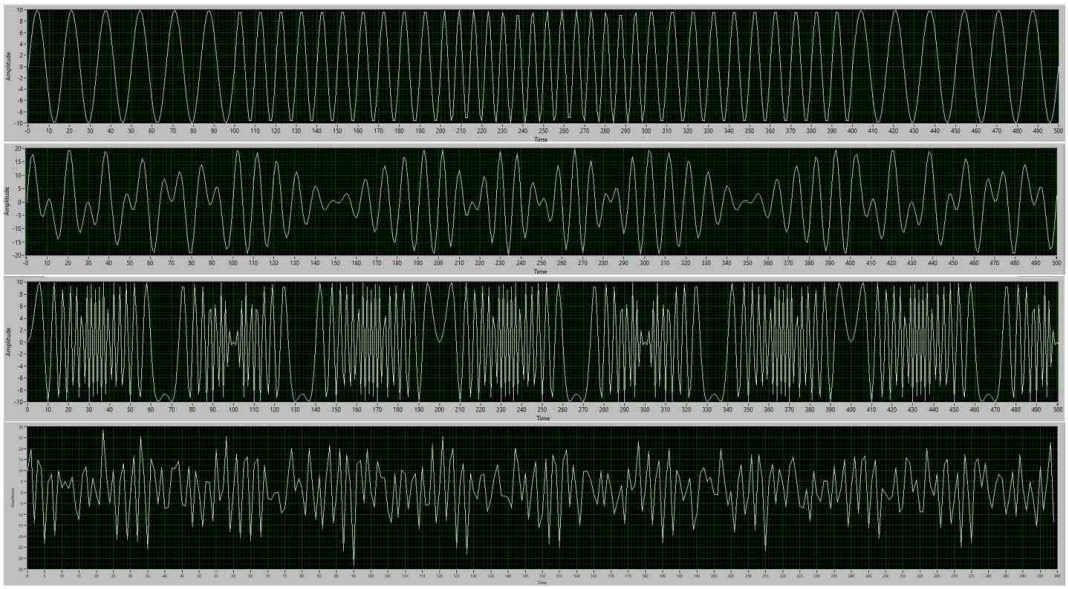


Рис. 3.10. Зображення сигналів дослідження впливу захисних сигналів на частотно-модульований небезпечний сигнал. (a – зображення небезпечного сигналу з частотною модуляцією, b – зображення результуючої небезпечного сигналу та першого захисного сигналу, c – зображення другого захисного сигналу, d – зображення результуючого сигналу)

Беручи до уваги дані, отримані в результаті дослідження, а саме зображення результуючого сигналу (рис. 3.10. d), можна зробити висновок, про ефективне руйнування інформаційної складової небезпечного сигналу з частотною модуляцією.

Дослідження впливу захисних сигналів на небезпечні сигнали з апмлітудною та кутовою модуляціями: мета четвертого дослідження було перевірити ефективність впливу захисного сигналу на небезпечний сигнал з амплітудною та кутовою модуляціями (Рис. 3.12.а).

Дослідження виконувались за блок-схемою, поданою на Рис. 3.11.

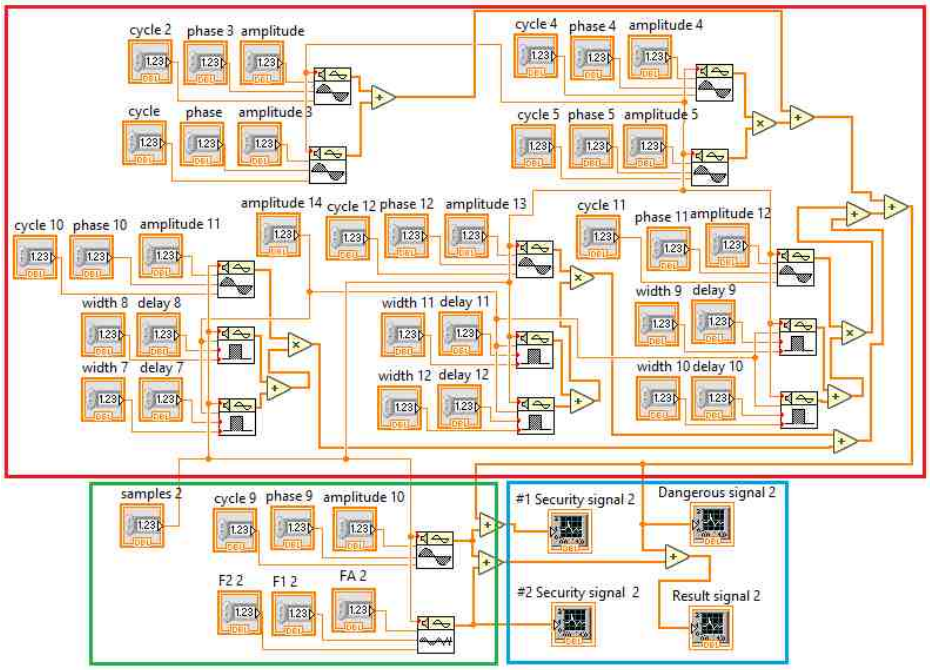


Рис. 3.11. Блок-схема дослідження впливу захисних сигналів на небезпечні сигнали з амплітудною та кутовою модуляціями

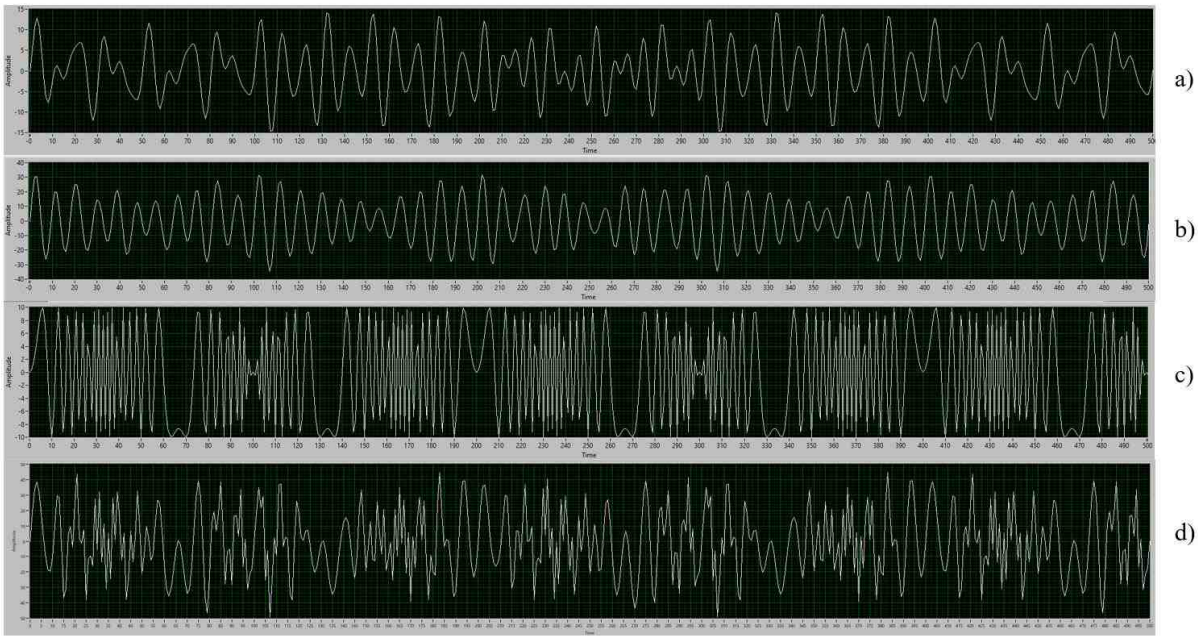


Рис. 3.12. Зображення сигналів дослідження впливу захисних сигналів на небезпечні сигнали з амплітудною та кутовою модуляціями. (a – зображення небезпечного сигналу з частотною модуляцією, b – зображення результуючої небезпечного сигналу та першого захисного сигналу, c – зображення другого захисного сигналу, d – зображення результуючого сигналу)

Беручи до уваги дані, отримані в результаті дослідження, а саме зображення результуючого сигналу (Рис. 3.12.d), можна зробити висновок, про ефективне руйнування (зменшення потужності результуючого сигналу на 17-48% в залежності від діапазону в порівнянні з небезпечним сигналом) інформаційної складової небезпечного сигналу з амплітудно-кутовою модуляцією.

Враховуючи, що перехоплення інформації може здійснюватись як на основній частоті, так і на гармоніках небезпечного сигналу, формування захисних сигналів слід здійснювати не тільки відносно основної частоти, а й відносно гармонік небезпечного сигналу [81]. Таким чином, явища «биття» і «качання» небезпечних сигналів буде прослідковуватись і на основній частоті, і на гармоніках, що унеможливить перехоплення інформації.

За підсумками проведення математичного моделювання в середовищі LabVIEW версії 20.0.1 зроблено наступні висновки:

1. Спираючись на результати досліджень, нами визначено параметри захисних сигналів, спрямованих на блокування небезпечних сигналів високочастотного нав'язування з різними видами модуляції несійної частоти.

2. Запропонований метод захисту інформації від перехоплення з використанням високочастотного нав'язування змінює властивості небезпечних сигналів і робить їх непридатними для використання за призначенням.

3. Отримані спотворення небезпечного сигналу унеможливлюють відтворення перехопленої інформації, що дозволяє забезпечити захист інформації від витоку каналами високочастотного нав'язування.

3.2. Удосконалення моделі оцінки оптимальних параметрів захисних сигналів шляхом експериментальних досліджень

Першочергове значення для оцінки ефективності впливу захисних сигналів на небезпечні сигнали ВЧН має вибір критеріїв ефективності. Практикою встановлено [83-85], що в якості критерія ефективності засобів радіозв’язку повинен бути обраний такий показник, який вдовольняє наступним основним вимогам: показник повинен відповідати меті досліджень і відображати основне призначення засобів радіозв’язку; показник повинен бути зв’язаний з характеристиками (параметрами) засобу радіозв’язку і чутливий до змін цих характеристик; показник повинен бути максимально простим.

Метою є обґрунтування ентропійно-інформаційного критерію та методики оцінки ефективності впливу захисних сигналів на небезпечні сигнали ВЧН.

Сучасна теорія оптимального приймання радіосигналів базується на апараті теорії імовірностей і математичної статистики. До основних обмежень

цього математичного апарату відносяться припущення про необмеженість часу оцінювання статистичного параметра, сталість закону його розподілу або про те, що вимірюваний в процесі досліджень параметр не змінює свого значення.

Ускладнення радіотехнічних засобів формування та обробки сигналів на тлі завад призводить до ситуації, коли практичні завдання оцінки якості приймання радіосигналів не можуть бути коректно вирішені методами математичної статистики і теорії імовірностей. Подолати обмеженість традиційної статистичної моделі приймання сигналів дозволяє перехід до інформаційних уявлень про кількість і якість інформації, яку містить сигнал.

Якщо розглядати поняття ентропії в якості міри невизначеності про що-небудь, то повідомлення, передане по каналу зв'язку, зменшує апріорну ентропію, а шум (завада) в каналі збільшує ентропію повідомлення.

Найбільший дезінформаційний вплив вносить завада з гауссовим законом розподілу.

Якщо завада в імовірнісному сенсі не залежить від сигналу, незалежно від закону розподілу і потужності сигналу дезінформаційна дія завади визначається її ентропією:

$$H(x) = -\int_{-\infty}^{\infty} p(x) \ln p(x) dx, \tag{3.4}$$

де $p(x)$ – одномірна густина розподілу імовірностей (ГРІ) оцінюваного інформативного параметра x, безрозмірна величина.

Важливою особливістю ентропії (3.38) є те, що її загальне поняття як міри невизначеності процесу зводиться до числового значення ГРІ і нею можна оперувати як фізичною величиною.

Ентропія нормального закону розподілу при рівних енергіях випадкових процесів максимальна і характеризується повною відсутністю кореляційних

зв'язків між формуючими процес випадковими флуктуаціями сигналу або складовими його процесами. Завада з таким законом розподілу є математичною ідеалізацією завади з найкращою дезінформаційною дією (білий шум).

Ентропія ГРІ досить просто обчислюється і вимірюється через ГРІ оцінюваної випадкової величини. Найбільш простим є метод вимірювання ГРІ за допомогою оцінювання відносного часу перебування випадкової величини в заданому інтервалі значень [83].

При однакових значеннях відносної похибки час вимірювання ентропії суттєво менший за час вимірювання одномірної ГРІ, що важливо при вимірюваннях короткочасних і швидкоплинних випадкових процесів. Якщо вимірюваний випадковий процес суттєво нестаціонарний, то оцінки ГРІ є випадковим процесом зі своїм законом розподілу. В цьому випадку необхідно оцінювати закон розподілу, що в ряді випадків дозволяє отримувати надійну інформацію і з істотно нестаціонарних процесів.

Показана принципова можливість вимірювання ентропії ГРІ через вимір кореляційної функції. Ця можливість обумовлена математично встановленим взаємозв'язком між кореляційною функцією, законом розподілу, моментними характеристиками і ентропією ГРІ випадкового процесу. Остання обставина спрощує вимір ентропії за допомогою мікропроцесорної техніки. В якості основних моделей ГРІ використовують розподіл Релея і узагальнений розподіл Релея (розподіл Райса).

Похідною від ентропії ГРІ характеристикою є коефіцієнт якості шуму, який визначається через ентропію ГРІ наступним чином [83, 84]:

$$\eta = \frac{1}{2\pi e}\exp\left[2H(x)\right] \tag{3.5}$$

Коефіцієнт якості шуму має ту ж розмірність, що і ентропія, але більш широко застосовується в радіотехніці для оцінки якості радіозавад.

Кількість інформації I визначається як різниця ентропій [84, 85]:

$$I = H(x) - H(x / x_n) \tag{3.6}$$

де $H(x)$ – ентропія оцінюваної величини до вимірювання;

$H(x / x_n)$ – умовна ентропія дійсного значення x вимірюваної величини після вимірювання.

Фізично (3.40) трактується як кількісна міра зменшення невизначеності при оцінюванні невідомого параметра x.

Інформаційні показники якості приймання сигналів мають простий і ясний фізичний зміст і можуть оцінюватися кількісно шляхом вимірювання параметрів законів розподілів амплітуд, фаз і частот сигналів.

Найбільш загальним критерієм оптимальності (якості) виявлення сигналів в статистичній радіотехніці є критерій мінімуму середнього ризику (середньої ціни наслідків помилок). Практичними важливими наслідками цього критерію є критерій Неймана-Пірсона (традиційно застосовується в радіолокації), критерій ідеального спостерігача, критерій мінімуму середньоквадратичної помилки (застосовується у вимірювальній практиці), ваговий критерій.

На практиці широко поширений критерій відношення правдоподібності:

$$l(x) = \frac{P_{СЗ}(x)}{P_З(x)}, \tag{3.7}$$

де $l(x)$ – відношення густин розподілу імовірностей однієї й тієї ж реалізації оцінюваного параметра x за двох умов: коли сигнал впливає на приймальний пристрій в сукупності з шумом (завадою) і коли на вході приймача діє тільки шум (завада). При використанні цього критерію роблять припущення, що апріорна ГРІ збігається з функцією правдоподібності. Після порівняння

чисельного значення критерію $l(x)$ з встановленим граничним значенням l_0 приймається рішення, яка з гіпотез щодо наявності сигналу в даному процесі є більш правдоподібною.

Застосування критерію відношення правдоподібності практично зводиться до обчислення відношення (3.7) і порівнянню його значення з порогом, величина якого відповідає заданій імовірності помилкової тривоги. Рішення про наявність корисного сигналу приймається, якщо значення відношення правдоподібності перевищує порогову величину l_0, в іншому випадку приймається рішення про відсутність сигналу в шумах або завадах.

Слід зазначити, що кореляційна обробка незмінно пов'язана з втратою корисної інформації, що міститься в зміні характеристик закону розподілу оцінюваного параметра корисного сигналу. Іншими словами, кореляційний приймач є оптимальним тільки в енергетичному сенсі; він покращує енергетичне відношення сигнал/шум, але при цьому втрачається корисна інформація про імовірнісних характеристиках сигналу. Із зазначеної причини кореляційний приймач не є оптимальним в інформаційному сенсі.

Як показано в [84], узагальненою характеристикою форми закону розподілу є ентропія його ГРІ. Ця характеристика враховує форму ГРІ, тому інформаційно-ентропійний критерій оптимального приймання виду:

$$I(x) = \frac{H_{СЗ}(x)}{H_З(x)}, \tag{3.8}$$

є більш універсальним, ніж енергетичний пороговий (заснований на обчисленні кореляційного інтеграла).

В (3.42) $I(x)$ – відносна кількість інформації, отримана внаслідок обробки сигналу разом з шумом (завадою); $H_{СЗ}(x)$, $H_З(x)$ – відповідно, ентропії ГРІ $P_{СЗ}(x)$ і $P_З(x)$.

Пряме вимірювання ГРІ $P_C(x)+P_З(x)$ і $P_З(x)$ і ентропій $H_C(x)+H_З(x)$ дозволяє отримувати корисну інформацію, що міститься в зміні параметрів форми законів розподілів переданих повідомлень.

Таким чином, інформаційно-ентропійний алгоритм оцінки якості захищеності сигналів у каналах радіозв'язку з зашумленням полягає у вимірі густини імовірностей $P_C(x)+P_З(x)$ і відповідних їм ентропій ГРІ$H_C(x)+H_З(x), H_З(x)$ з подальшим обчисленням відношення правдоподібності і прийняттям рішення про наявність корисного сигналу (або оцінці значення його параметра) шляхом порівняння з пороговим значенням ентропії H_0.

Інформаційне трактування процесів приймання радіосигналу і оцінювання його параметрів у порівнянні з традиційними статистичними підходами має переваги, які полягають у наступному:

- інформаційний показник якості приймання має простий фізичний зміст і можливість кількісної оцінки шляхом вимірювання імовірнісних характеристик сигналів;
- ентропійно-інформаційні показники якості виявлення і оцінювання сигналів інваріантні до зміни законів розподілів оцінюваного параметра, оскільки дозволяють враховувати вплив форми закону розподілу на якість оцінювання;
- інформаційний підхід до оптимізації якості прийому забезпечує отримання додаткової корисної інформації, що міститься в параметрах закону розподілу оцінюваного параметра, і дозволяє підвищити точність оцінок.

Ідеальні захисні сигнали повинні створювати такі умови, за яких апостеріорі, після прийому корисного сигналу, апріорна невизначеність в системі інформаційного забезпечення зберігалася б протягом тривалого часу. Чим більша невизначеність завадового сигналу при заданих обмеженнях, тим менше потенційних можливостей у супротивника для усунення його впливу.

Оцінка якості приймання радіосигналів здійснюється за інформаційно-ентропійним критерієм якості. Відмінністю нового критерію від традиційного

критерію відношення правдоподібності є заміна енергетичної процедури оптимального прийому на більш загальну інформаційно енергетичну процедуру. Інформаційно-ентропійний підхід базується на врахуванні відмінностей статистичних властивостей сигналів і захисних завад, а саме відмінності ентропій (форм) законів їх розподілу в технологічній процедурі розрізнення або оцінювання параметрів сигналів на тлі завад.

Структурну схему оцінки якості каналу з зашумленням наведено на Рис. 3.13.

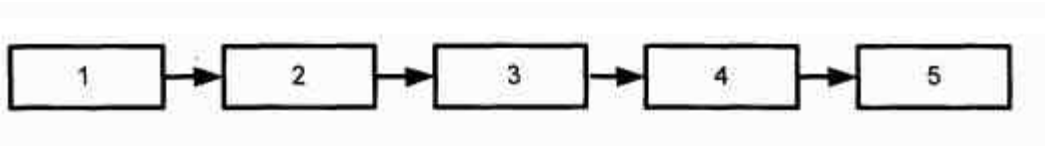


Рис. 3.13. Структурна схема оцінки якості каналу для фазо-модульованих і частотно-модульованих захисних завад:
1 - джерело захисної завади; 2 - вимірювальний приймач з частотним (фазовим), амплітудним демодулятором; 3 - вимірювач кореляційних характеристик; 4 - АЦП, 5 - персональний комп'ютер

В блоці 1 формується захисний фазо-модульована або частотно-модульована шумова сигнал, яка випромінюється в навколишній простір за допомогою антени. В блоці 2 прийнята завада демодулюється і формується електричний сигнал, який подається на вимірювач кореляційних характеристик (блок 3). В блоці 3 здійснюється дискретизація за часом прийнятого електричного сигналу, вимірюються рівні сигналу для дискретних моментів часу і будується гістограма густини розподілу імовірності значень електричного сигналу, яка після аналого-цифрового перетворення в блоці 4 поступає в персональний комп'ютер (блок 5), де обчислюється ентропія закону розподілу значень напруг електричного сигналу завади, ентропія еталонного рівномірного закону розподілу і ентропійний коефіцієнт якості завади.

Якщо блок 1 замінити джерелом корисного сигналу, то для оцінки його статистичних властивостей приймають сигнал, здійснюють дискретизацію відліків значень електричного сигналу, вимірюють для всіх дискретних моментів часу рівні напруг електричного сигналу $u_i(i=\overline{1,N})$, будують гістограму закону розподілу значень напруги електричного сигналу $p_i(u_i)\left(i=\overline{1,N}\right)$, обчислюють з використанням гістограми ентропію H закону розподілу значень напруг електричного сигналу за формулою:

$$H=-\sum_{i=1}^{N} p_i \ln p_i. \tag{3.9}$$

Порівняння ентропійних характеристик коефіцієнтів якості η захисної частотно-модульованої шумової завади і замаскованого сигналу дозволяє оцінювати якість каналу. При необхідності більш детального аналізу якості з використанням гістограми розраховують другий момент σ_0 закону розподілу значень напруги електричного сигналу або (і) завади за формулою:

$$\sigma_0=\sqrt{\sum_{i=1}^{N} u_i^2 p_i}. \tag{3.10}$$

З використанням гістограми розраховують також математичне очікування m натурального логарифма значень напруги електричного сигналу (завади) за формулою

$$m=\sum_{i=1}^{N} p_i \ln u_i, \tag{3.11}$$

обчислюють ентропію H^P еталонного релеєвського закону розподілу за формулою:

$$H^P = -m + 2\ln r + \frac{\sigma_0^2}{2r^2}, \qquad (3.12)$$

де $r = \sqrt{2}e^{\left[1+m+\frac{1}{2}\left(c-\sigma_0^2\right)\right]}$ - параметр релєєвського закону розподілу; $c = 0.577$ - постійна Ейлера.

Ентропійний коефіцієнт якості η^0 захисного сигналу обчислюють за формулою:

$$\eta^0 = \frac{e^H}{e^{H^P}} = e^{\left[H+m-2\ln r-\frac{\sigma_0^2}{2r^2}\right]}. \qquad (3.13)$$

Отримане значення η^0 ентропійного коефіцієнта якості використовують для оцінки якості захисного сигналу в конкретному каналі.

Головними завданнями експериментальних досліджень є досягнення максимальної точності в розрахунках діапазону максимального ступеню ефективності запропонованого методу, визначення максимального рівня цієї ефективності і визначення оптимальних параметрів захисних сигналів задля забезпечення цієї ефективності.

Питання організації постановки експерименту щодо визначення вихідних параметрів запропонованої авторами системи захисту інформації від її несанкціонованого перехоплення методами ВЧ-нав'язування розглянуто в наступному розділі.

Вважається доцільним будувати експеримент, використовуючи обладнання, яке за своїми характеристиками буде максимально відповідати умовам реального часу та дозволить максимально ефективно оцінити можливості захисту інформації від витоку каналами ВЧН, використовуючи запропонований метод .

Програми, методики, схеми проведення та результати проведення експериментальних досліджень детально представлені в наступному розділі.

Висновки до розділу 3

1. Введення ентропійного коефіцієнта як характеристики якості завадових сигналів дозволяє оцінювати потенційні можливості завад незалежно від способів їх обробки в каналах зв'язку.

2. Основні параметри системи захисту, що підлягають визначенню в результаті експерименту:

- визначення діапазону частот коливання захисного сигналу з метою забезпечення максимально ефективного впливу для кожного виду модуляції, що використовується при перехопленні інформації;

- визначення рівнів захисних сигналів максимально ефективного впливу для кожного виду модуляції.

Схема побудови експерименту залежить від вибраного критерію ступеню ефективності запропонованого методу. При цьому критерій повинен відповідати вимогам простоти проведення експерименту з використанням стандартизованих радіовимірювальних приладів і однозначності отриманих результатів.

3. Удосконалено модель блокування інформації від перехоплення каналами високочастотного нав’язування шляхом утворення ефекту «биття» частот не тільки на основній частоті, а й на комбінаційних гармоніках зондуючого сигналу.

За підсумками проведення математичного моделювання в середовищі LabVIEW версії 20.0.1 зроблено наступні висновки:

- спираючись на результати досліджень, нами визначено параметри захисних сигналів, спрямованих на блокування небезпечних сигналів високочастотного нав'язування з різними видами модуляції несійної частоти;

- запропонований метод захисту інформації від перехоплення з використанням високочастотного нав'язування змінює властивості небезпечних сигналів і робить їх непридатними для використання за призначенням;

- отримані спотворення небезпечного сигналу унеможливлюють відтворення перехопленої інформації, що дозволяє забезпечити захист інформації від витоку каналами високочастотного нав'язування.

4. Запропоновано модель захисту інформації від витоку каналами високочастотного нав’язування шляхом руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках зондуючого сигналу, що забезпечує більш ефективний захист інформації з обмеженим доступом від перехоплення. Ця модель згідно імітаційних досліджень забезпечує ефективне руйнування (зменшення потужності результуючого сигналу на 17-48% в залежності від діапазону в порівнянні з небезпечним сигналом) інформаційної складової небезпечного сигналу з амплітудно-кутовою модуляцією.

РОЗДІЛ 4
ПРОВЕДЕННЯ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ПАРАМЕТРІВ ЗАВАДОВИХ ЗАХИСНИХ СИГНАЛІВ

4.1. Постановка задач і розробка методик експериментальних досліджень

При проведенні експериментальних досліджень параметрів захисного сигналу поставлено наступні задачі [78, 80, 81, 87-89]:

1. Дослідити основні параметри захисного і небезпечного сигналів.
2. Виявити залежність утворення ефекту «биття» частот від зміни параметрів захисного і небезпечного сигналів.
3. Знайти умови, при яких забезпечується утворення ефекту «биття» частот.
4. Оцінити умови, при яких забезпечується утворення ефекту «биття» частот.
5. Узагальнити отримані результати та вивести загальний параметр, який дозволить однозначно оцінити рівень захисту інформації від витоку.

Схема побудови експерименту залежить від вибраного критерію ступеню ефективності запропонованого методу. При цьому критерій повинен відповідати вимогам простоти проведення експерименту з використанням стандартизованих радіовимірювальних приладів і однозначності отриманих результатів [90].

Оскільки поставлені завдання необхідно вирішити для всіх видів модуляції, що виникають при ВЧН, пропонується застосувати метод суперпозиції для кожного з них, що забезпечить однозначність трактування отриманих результатів і достатню для подальшого проектування повноту досліджень.

Узагальнену схему проведення експериментальних досліджень подано на рис. 4.1 [91].

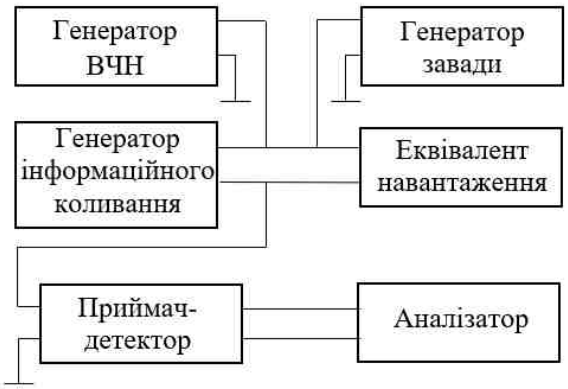


Рис. 4.1. Узагальнена схема проведення експериментальних досліджень

Функції генератора завади:

1. Формувати і змінювати частоту основного коливання впливу на сигнал ВЧН.

2. Змінювати діапазон управління частотою хитання і рівнем основної частоти.

3. Змінювати діапазон швидкості хитання основної частоти.

4. Формувати і змінювати параметри шумових сигналів.

5. Змінювати загальний рівень сигналу завади.

6. Здійснювати ці зміни незалежно одне від одного.

7. Використовувати кожний з видів зміни сигналу завади при відключенні решти факторів впливу.

Для вимірювання параметрів зондуючого сигналу і сигналу завади можуть бути використані стандартні осцилограф, частотомір і вольтметр (на схемі ці прилади не показано).

Еквівалент навантаження повинен забезпечувати три різні види модуляції зондуючого коливання небезпечними сигналами.

Основні вимоги до еквіваленту навантаження:

1. Забезпечення можливості перетворення небезпечного сигналу в АМ, ЧМ та ФМ незалежно один від одного.

2. Забезпечення можливості регулювання рівня глибини модуляції для кожного з її видів.

Очевидно, що найбільш прийнятним шляхом реалізації такого пристрою буде створення трьох окремих перетворювачів, що забезпечить простоту проведення експерименту.

Такі ж вимоги та методи побудови слід віднести і до побудови схем приймачів-детекторів.

Враховуючи, що перехоплення інформації може здійснюватись як на основній частоті, так і на гармоніках небезпечного сигналу, формування захисних сигналів слід здійснювати не тільки відносно основної частоти, а й відносно гармонік небезпечного сигналу [9]. Таким чином, явища «биття» і «качання» небезпечних сигналів буде прослідковуватись і на основній частоті, і на гармоніках, що унеможливить перехоплення інформації.

4.1.1. Розробка програми і методики експериментальних досліджень параметрів захисних сигналів

ПРОГРАМА ПРОВЕДЕННЯ

експериментальних досліджень параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА ОБ'ЄКТ ДОСЛІДЖЕНЬ

1.1. Об’єктом досліджень є комплекс приладів та пристроїв (далі – Комплекс-1):

1. Генератор сигналів довільної форми Tektronix AFG 3252.
2. Аналізатор спектру та сигналів ROHDE&SCHWARZ FSW 13 (Signal&Spectrum Analyser, 2 Hz – 13.6 GHz).
3. Осцилограф Tektronix DPO 7254 (Digital Phosphor Oscilloscope).
4. Комплекс антен дипольних Tuned Dipole Antenna FCC.
5. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 MHz – 7000 MHz.
6. Антена електрична ЕМА-2000 0.009 – 2000 МГц.

7. Стаціонарний комп’ютер стаціонарного типу (монітор, системний блок, маніпулятор типу «Миша», клавіатура) (далі - ПК).

1.2. Комплекс-1 створено з метою проведення експериментальних досліджень параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів.

2. МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕНЬ

2.1. Експериментальні дослідження проводяться з метою:

– визначення параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів;

– визначення діапазону ефективності захисного сигналу;

– підтвердження або спростування ефективності, достатності та надійності дії захисного сигналу задля забезпечення захисту інформації від витоку.

2.2. Завданням експериментальних досліджень є об'єктивна оцінка здатності захисного сигналу забезпечувати руйнацію інформативних параметрів небезпечних сигналів:

– забезпечення захисту інформації від витоку блокуванням каналів перехоплення методом високочастотного нав'язування;

– ефективність руйнування інформативного сигналу завдяки утворенню ефекту «биття» з небезпечним сигналом високочастотного нав’язування;

– знаходження параметрів захисних сигналів, здатних забезпечити максимально можливу руйнацію інформативних параметрів небезпечних сигналів на основній частоті та на комбінаційних гармонікахзондуючого сигналу, і, як результат, створенні протидії перехопленню інформації з обмеженим доступом заловмисниками.

3. ОБСЯГ ДОСЛІДЖЕНЬ

3.1. Експериментальні дослідження в обсязі:

3.1.1. Проведення інженерного аналізу схемної та конструктивної побудови обладнання Комплексу-1 з метою:

– формування вимог до режимів роботи обладнання;

– визначення переліку обладнання, яке необхідно підключати до Комплексу-1 при проведенні вимірювань;

– визначення особливих умов проведення вимірювань (вплив електромагнітних полів та інше);

– формування переліку спеціальних параметрів і характеристик сигналів

3.1.2. Проведення робіт щодо метрологічного забезпечення вимірювань з метою:

– визначення складу та режимів роботи метрологічного обладнання;

– визначення вимог до розташування обладнання Комплексу-1 та метрологічного обладнання при проведенні вимірювань;

– визначення схем підключення метрологічного обладнання, обладнання Комплексу-1 та допоміжних засобів;

– визначення вимог до нестандартного приладдя, виготовлення нестандартного приладдя, його калібрування (за потреби).

3.1.3. Проведення вимірювань спеціальних параметрів і характеристик сигналів обладнання Комплексу-1 з метою підготовки вихідних даних щодо визначення параметрів захисного сигналу у такій послідовності:

– перевірка функціонування обладнання Комплексу-1;

– інструментальний контроль параметрів тестових сигналів обладнання Комплексу-1 для визначеного режиму роботи;

– реєстрація параметрів тестового сигналу (у часовій області) та спектральних характеристик (у частотній області) при підключенні засобів вимірювань до кіл формувачів тестових сигналів та встановлення метрологічного обладнання у режими роботи, що відповідають встановленням при вимірюваннях компонент тестових сигналів у відповідних каналах витоку інформації;

– визначення зон локального випромінювання складових частин обладнання Комплексу-1, вихідних вимог щодо їх орієнтації по відношенню до метрологічного обладнання, уточнення діапазонів частот, у яких потрібно проводити виміри для кожного з тестових режимів роботи;

– проведення вимірювань параметрів та характеристик сигналів обладнання Комплексу-1, на підставі яких розраховуються параметри захисного сигналу.

3.1.4. Обробка результатів вимірювань, визначення параметрів захисного сигналу, а саме:

– визначення параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів;

– визначення діапазону ефективності захисного сигналу;

– підтвердження або спростування ефективності, достатності та надійності дії захисного сигналу задля забезпечення захисту інформації від витоку.

3.2. Оформлення звітної документації за результатами Досліджень, а саме:

– звіту за результатами експериментальних досліджень обладнання Комплексу;

– висновку за результатами експериментальних досліджень обладнання Комплексу-1.

МЕТОДИКА

проведення експериментальних досліджень параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ОБ’ЄКТ ДОСЛІДЖЕНЬ

Комплекс-1 побудований з метою проведення досліджень параметрів сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів.

2. МЕТА ДОСЛІДЖЕНЬ

Метою досліджень є експериментальна перевірка комплексу для підтвердження теоретичної інформації або її спростування щодо здатності сигналу з певними заданими параметрами забезпечити руйнацію інформативних параметрів небезпечних сигналів.

3. ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1. Дослідження проводяться у відповідності до Програми проведення експериментальних досліджень.

3.2. Дослідження даного об’єкта проводяться вперше.

3.3. Місце проведення досліджень – екрановане приміщення II класу (згідно [92]). Ефективність екранування згідно [92] екранованого приміщення II класу складає від 30 до 80 дБ.

4. УМОВИ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ

4.1. Усі види досліджень проводяться в нормальних умовах.

Нормальним умовам відповідає:

- температура навколишнього середовища ..... (25 ± 10)°С;

- відносна вологість повітря ..... від 45 до 80%;

- атмосферний тиск ..... від 84,0 до 106,7 кПа (від 630 до 800 мм.рт.ст.).

4.2. Якщо пристрої, що надані на дослідження, до початку вимірювань знаходились в кліматичних умовах, які відрізняються від нормальних, то їх необхідно витримати в нормальних кліматичних умовах не менше 12 годин.

5. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДОСЛІДЖЕНЬ

Для проведення досліджень дозволяється використовувати прилади та пристрої, вказані у складі Комплексу-1 або інші прилади, що за своїми технічними характеристиками являються ідентичними.

6. ПОРЯДОК ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ

6.1. Проведення експериментальних досліджень проводиться згідно з структурною схемою, представленою на рис. 4.2.

6.1.1. Підготувати контрольно-вимірювальні прилади до роботи згідно з їх інструкціями по експлуатації.

6.1.2. З’єднати та ввімкнути вимірювальне обладнання згідно до

керівництв з експлуатації. Забезпечити надійне заземлення.

6.1.3. Через 15-30 хвилин після ввімкнення перевірити функціонування складового обладнання Комплексу-1.

6.1.4. Розташувати вимірювальні антени на відстані 1 м від ПК. Антени повинні знаходитись в паралельній площині до фронтальної частини ПК. При цьому необхідно забезпечити, щоб геометричні центри рамкової антени та ПК знаходилися на одній осі.

6.1.5. За допомогою генератору сигналів створити захисний сигнал та небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину), вибравши довільну початкову частоту сигналу. Різниця між сигналами повинна бути $\Delta\omega$= 400-600 kHz.

6.1.6. При встановленій смузі пропускання (RBW) вимірювального обладнання 30 Гц та смузі огляду частоти (Frequency span) 500 кГц, встановити на аналізаторі спектру детектор пікових значень (PK, PEAK).

6.1.7. На генераторі встановити частоти для К1 та К2 (К1 – небезпечний сигнал, К2 – захисний сигнал). Дослідним шляхом визначити різницю між К1 та К2, при якій можливе забезпечення руйнації інформативних параметрів небезпечних сигналів.

6.1.8. Зафіксувати $\Delta\omega$ сигналів на аналізаторі спектру.

6.1.9. Зафіксувати $\Delta\omega$ сигналів на екрані осцилографа.

6.1.10. Зробити відповідні висновки стосовно підтвердження або спростування теоретичної частини, зафіксувати параметри захисного сигналу, які задавались під час проведення експериментальних досліджень: частота, потужність, фаза.

6.1.11. За допомогою генератору сигналів створити захисний сигнал та

небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину). Різниця між сигналами повинна бути Δω= 200 kHz.

6.1.12. Повторити дії відповідно до п. 6.1.6 – 6.1.11.

6.1.13. За допомогою генератору сигналів створити захисний сигнал та небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину). Різниця між сигналами повинна бути Δω= 100 kHz.

6.1.14. Повторити дії відповідно до п. 6.1.6 – 6.1.11.

6.1.15. За допомогою генератору сигналів створити захисний сигнал та небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину). Різниця між сигналами повинна бути Δω= 10-20 kHz.

6.1.16. Повторити дії відповідно до п. 6.1.6 – 6.1.11.

6.1.17. За допомогою генератору сигналів створити захисний сигнал та небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину). Різниця між сигналами повинна бути Δω= 5-10 kHz.

6.1.18. Повторити дії відповідно до п. 6.1.6 – 6.1.11.

6.1.19. За допомогою генератору сигналів створити захисний сигнал та небезпечний сигнал (під захисним та небезпечним сигналом мається на увазі такі сигнали, які визначені виконавцем експериментальних досліджень і можуть підтвердити або спростувати теоретичну частину). Різниця між сигналами повинна бути Δω= 0 Hz.

6.1.20. Повторити дії відповідно до п. 6.1.6 – 6.1.11.

7. ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

За результатами випробувань розробляється Звіт за результатами експериментальних досліджень.

4.1.2. Розробка програми і методики експериментальних досліджень оцінки ефективності завадових захисних сигналів

ПРОГРАМА ПРОВЕДЕННЯ
експериментальних досліджень оцінки ефективного впливу захисних сигналів на небезпечні сигнали

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА ОБ'ЄКТ ДОСЛІДЖЕНЬ

1.1. Об’єктом досліджень є комплекс приладів та пристроїв (далі – Комплекс-2):

1. Генератор сигналів довільної форми Tektronix AFG 3252.
2. Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B 2 Hz-26.5 GHz.
3. Комплекс антен дипольних Tuned Dipole Antenna FCC.
4. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 MHz – 7000 MHz
5. Антена електрична ЕМА-2000 0.009 – 2000 МГц.
6. Стаціонарний комп’ютер стаціонарного типу (монітор, системний блок, маніпулятор типу «Миша», клавіатура) (далі - ПК).

1.2. Комплекс-2 створено з метою проведення експериментальних досліджень оцінки ефективного впливу захисних сигналів на небезпечні сигнали.

2. МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕНЬ

2.1. Експериментальні дослідження проводяться з метою:

– дослідити ефективний вплив захисних сигналів на небезпечні сигнали та руйнацію інформативних параметрів небезпечних сигналів;

– визначення оцінки ефективного впливу захисних сигналів на небезпечні сигнали.

2.2. Завданням експериментальних досліджень є об'єктивна оцінка ефективного впливу захисних сигналів на небезпечні сигнали:

– забезпечення захисту інформації від витоку блокуванням каналів перехоплення методом високочастотного нав'язування;

– ефективність руйнування інформативного сигналу завдяки утворенню ефекту «биття» з небезпечним сигналом високочастотного нав’язування.

3. ОБСЯГ ДОСЛІДЖЕНЬ

3.1. Експериментальні дослідження в обсязі:

3.1.1. Проведення інженерного аналізу схемної та конструктивної побудови обладнання Комплексу-2 з метою:

– формування вимог до режимів роботи обладнання;

– визначення переліку обладнання, яке необхідно підключати до Комплексу при проведенні вимірювань;

– визначення особливих умов проведення вимірювань (вплив електромагнітних полів та інше);

– формування переліку спеціальних параметрів і характеристик сигналів

3.1.2. Проведення робіт щодо метрологічного забезпечення вимірювань з метою:

– визначення складу та режимів роботи метрологічного обладнання;

– визначення вимог до розташування обладнання Комплексу та метрологічного обладнання при проведенні вимірювань;

– визначення схем підключення метрологічного обладнання, обладнання Комплексу та допоміжних засобів;

– визначення вимог до нестандартного приладдя, виготовлення нестандартного приладдя, його калібрування (за потреби).

3.1.3. Проведення вимірювань спеціальних параметрів і характеристик сигналів обладнання Комплексу-2 з метою підготовки вихідних даних щодо визначення параметрів захисного сигналу у такій послідовності:

– перевірка функціонування обладнання Комплексу-2;

– інструментальний контроль параметрів тестових сигналів обладнання Комплексу-2 для визначеного режиму роботи;

– реєстрація параметрів тестового сигналу (у часовій області) та спектральних характеристик (у частотній області) при підключенні засобів вимірювань до кіл формувачів тестових сигналів та встановлення метрологічного обладнання у режими роботи, що відповідають встановленням при вимірюваннях компонент тестових сигналів у відповідних каналах витоку інформації;

– визначення зон локального випромінювання складових частин обладнання Комплексу-2, вихідних вимог щодо їх орієнтації по відношенню до метрологічного обладнання, уточнення діапазонів частот, у яких потрібно проводити виміри для кожного з тестових режимів роботи;

– проведення вимірювань параметрів та характеристик сигналів обладнання Комплексу-2, на підставі яких розраховуються параметри захисного сигналу.

3.1.4. Обробка результатів вимірювань, визначення параметрів захисного сигналу, а саме:

– визначення параметрів захисного сигналу, здатного забезпечити руйнацію інформативних параметрів небезпечних сигналів;

– визначення діапазону ефективності захисного сигналу;

– підтвердження або спростування ефективності, достатності та надійності дії захисного сигналу задля забезпечення захисту інформації від витоку.

3.2. Оформлення звітної документації за результатами Досліджень, а саме:

– звіту за результатами експериментальних досліджень обладнання Комплексу-2;

– висновку за результатами експериментальних досліджень обладнання Комплексу-2.

МЕТОДИКА

проведення експериментальних досліджень оцінки ефективного впливу захисних сигналів на небезпечні сигнали

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ОБ’ЄКТ ДОСЛІДЖЕНЬ

Комплекс-2 побудований з метою проведення досліджень оцінки ефективного впливу захисних сигналів на небезпечні сигнали.

2. МЕТА ДОСЛІДЖЕНЬ

Метою досліджень є експериментальна перевірка комплексу для підтвердження теоретичної інформації та оцінки ефективного впливу захисних сигналів на небезпечні сигнали.

3. ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1. Дослідження проводяться у відповідності до Програми проведення експериментальних досліджень.

3.2. Дослідження даного об’єкта проводяться вперше.

3.3. Місце проведення досліджень – екрановане приміщення II класу (згідно [92]). Ефективність екранування згідно [92] екранованого приміщення II класу складає від 30 до 80 дБ.

4. УМОВИ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ

4.1. Усі види досліджень проводяться в нормальних умовах.

Нормальним умовам відповідає:

- температура навколишнього середовища ..... (25 ± 10)^{o}C;

- відносна вологість повітря ..... від 45 до 80%;

- атмосферний тиск ..... від 84,0 до 106,7 кПа (від 630 до 800 мм.рт.ст.).

4.2. Якщо пристрої, що надані на дослідження, до початку вимірювань знаходились в кліматичних умовах, які відрізняються від нормальних, то їх необхідно витримати в нормальних кліматичних умовах не менше 12 годин.

5. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДОСЛІДЖЕНЬ

Для проведення досліджень дозволяється використовувати прилади та пристрої, вказані у складі Комплексу-2 або інші прилади, що за своїми технічними характеристиками являються ідентичними.

6. ПОРЯДОК ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ

6.1. Проведення експериментальних досліджень проводиться згідно з структурною схемою, представленою на рис. 4.3.

6.1.1. Підготувати контрольно-вимірювальні прилади до роботи згідно з їх інструкціями по експлуатації.

6.1.2. З’єднати та ввімкнути вимірювальне обладнання згідно до керівництв з експлуатації. Забезпечити надійне заземлення.

6.1.3. Через 15-30 хвилин після ввімкнення перевірити функціонування складового обладнання Комплексу-2.

6.1.4. Розташувати вимірювальні антени на відстані 1 м від ПК. Антени повинні знаходитись в паралельній площині до фронтальної частини ПК. При цьому необхідно забезпечити, щоб геометричні центри рамкової антени та ПК знаходилися на одній осі.

6.1.5. На ПК запускається тестова програма, яка імітує максимальну навантаженість роботи по заданому інтерфейсу. Для проведення експерименту вибрано інтерфейс монітору (з роз’ємом VGA (DE-15)), адже на моніторі може відображатись інформація з обмеженим доступом, яка може бути перехоплена.

6.1.6. В діапазоні 0 – 2 ГГц зафіксувати частоти згідно тактової з

максимальним рівнем сигналу, після чого обираємо одну $\omega 1$, яка має найкраще співвідношення якість/рівень та на цій самій частоті вмикаємо перший канал генератора, який підсилює корисний сигнал, встановивши рівень сигналу 30 dBμV.

6.1.7. Включити другий канал генератора, встановивши рівень сигналу 30 dBμV на частоту $\omega 1 - 100$ кГц.

6.1.8. Додати до сигналу з 2 каналу генератора ефект «качання» частоти, почергово додаючи та віднімаючи 400 кГц (вибрано приблизно середнє значення з оптимального діапазону різниці частот захисного та небезпечного сигналів, який забезпечує ефект «биття» частот згідно п. 3.2.).

7. ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

За результатами випробувань розробляється Звіт за результатами експериментальних досліджень.

4.2. Опис схеми і апаратних засобів для проведення експериментальних досліджень

4.2.1. Опис схеми і апаратних засобів для проведення експериментальних досліджень параметрів захисних сигналів

Об’єктом досліджень є комплекс приладів та пристроїв (далі – Комплекс-1):

1. Генератор сигналів довільної форми Tektronix AFG 3252.
2. Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B 2 Hz-26.5 GHz.
3. Осцилограф Tektronix DPO 7254 (Digital Phosphor Oscilloscope).
4. Комплекс антен дипольних Tuned Dipole Antenna FCC.

5. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 MHz – 7000 MHz.

6. Антена електрична EMA-2000 0.009 – 2000 МГц.

7. Персональний комп’ютер стаціонарного типу (монітор, маніпулятор типу «Миша», клавіатура, системний блок) (далі - ПК).

Перелік обладнання комплексу для проведення експериментальних досліджень представлена на рис. 4.2.

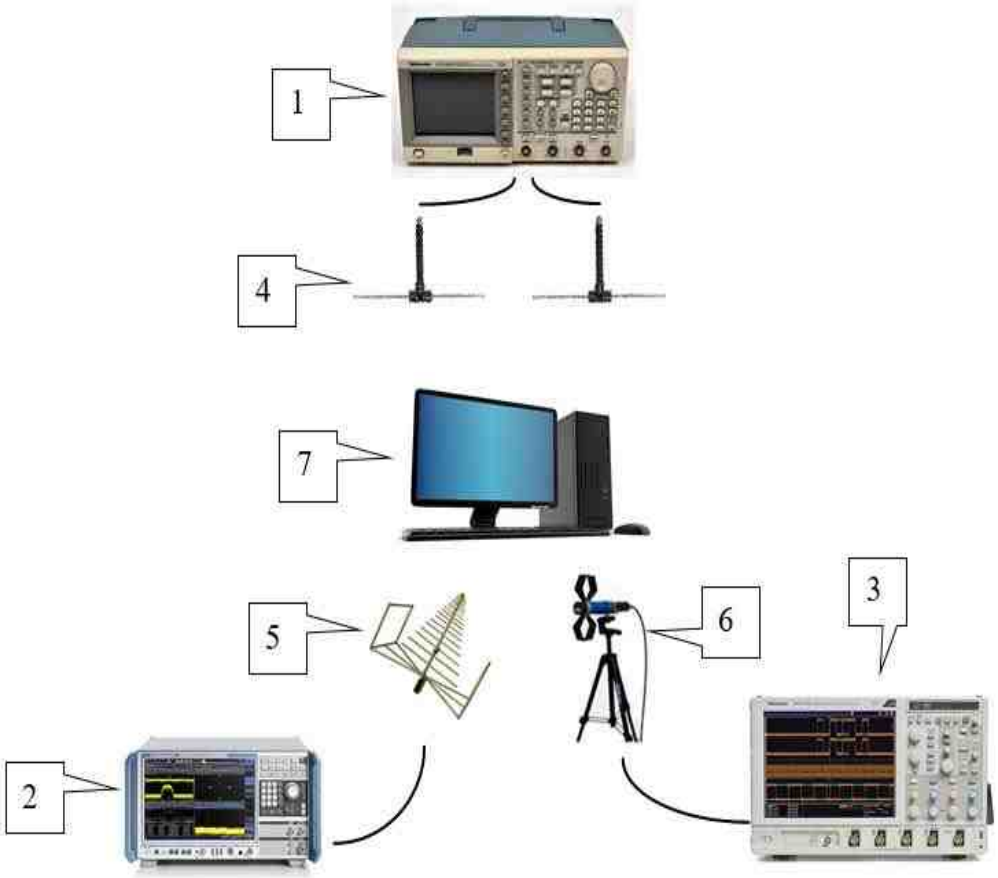


Рис. 4.2. Перелік обладнання для проведення експериментальних досліджень у складі: 1 – Генератор сигналів довільної форми Tektronix AFG 3252; 2 – Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B; 3 – Осцилограф Tektronix DPO 7254; 4 – Комплекс антен дипольних Tuned Dipole Antenna FCC; 5 – Антена білогоперіодична SAS-521F-7; 6 - Антена електрична EMA-2000; 7 – Персональний комп’ютер стаціонарного типу.

Детальний опис переліку обладнання для проведення експериментальних досліджень:

1. Генератор сигналів довільної форми Tektronix AFG 3252.

Основні технічні характеристики:

- сигнали синусоїндної форми частотою до 10 МГц, 25 МГц, 100 МГц або 240 МГц;
- сигнали довільної форми з роздільною здатністю 14 розрядів, 250 Мвиб/с, 1 Гвиб/с или 2 Гвиб/с.
- амплітуда до 20 Впік-пік на навантаженні 50 Ом.

2. Аналізатор спектру та сигналів ROHDE&SCHWARZ FSW 13 (Signal&Spectrum Analyser, 2 Hz – 13.6 GHz).

Основні технічні характеристики:

- діапазон частот - 2 Hz – 13.6 GHz;
- відхилення частоти опорного генератора за рахунок старіння - 1 × 10-7/год;
- смуги розширення - від 1 Гц до 10 МГц;
- канальний фільтр - від 100 Гц до 5 МГц;
- смуга демодуляції - I/Q - 10 МГц.

3. Осцилограф Tektronix DPO 7254 (Digital Phosphor Oscilloscope).

Основні технічні характеристики:

- частота дискретизації в режимі реального часу до 40 Гвиб./с по одному каналу, до 20 Гвиб./с по двох каналах;
- довжина запису осцилограм з використанням функції MultiView Zoom™ - до 500 млн точок;
- максимальна швидкість захоплення вхідного сигналу з використанням функції FastAcq™ >250 000 осцилограм в секунду;
- швидкість захоплення в режимі FastFrame™ з використанням сегментованої пам’яті FastFrame™ >310 000 осцилограм в секунду;
- можливість вибору користувачем фільтрів обмеження смуги рпопускання для підвищення точності виміру низькочастотних сигналів.

4. Комплекс антен дипольних Tuned Dipole Antenna FCC.

Основні технічні характеристики:

- діапазон частоти - 325 МГц – 1 ГГц;
- втрати - 0 до 2 дБі;
- фактор антени - 20 – 29 дБ/м;
- максимальа потужність - 60 Вт;
- імпеданс – 50 Ом;
- тип роз’єму - N-Type, female.

5. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 МГц – 7000 МГц.

Основні технічні характеристики:

- діапазон частоти - 25 МГц – 7000 МГц;
- фактор антени - 7 – 47 дБ/м;
- підсилення - 27 до 7 дБі;
- максимальна потужність - 400 Вт;
- максимальне випромінювання поля - 100 В/м;
- імпенданс - 50 Ом;
- роз’єм антени типу N-Type, Female;
- база для монтажу - ¼ x 20 Thread, Female.

6. Антена електрична ЕМА-2000 0.009 – 2000 МГц.

Основні технічні характеристики:

- діапазон частоти - 0,009…2000 МГц;
- коефіцієнт калібрування антени - 30,0;
- номінальне значення, дБ 1/м;
- відхилення від номінального значення на частоті 10 МГц, не більше, дБ - ± 2;
- нерівномірність частотної характеристики, не більше, дБ – 10;
- похибка коефіцієнта калібрування, не більше, дБ - ± 2;

- найбільша вимірювана напруженість електричного поля, дБ мкВ/м – 120;
- вихідний опір антени (номінальне значення), Ом – 50.

2. Персональний комп’ютер стаціонарного типу (монітор, маніпулятор типу «Миша», клавіатура, системний блок).

4.2.2. Опис схеми і апаратних засобів для проведення експериментальних досліджень оцінки ефективності завадових захисних сигналів

Об’єктом досліджень є комплекс приладів та пристроїв (далі – Комплекс-2):

1. Генератор сигналів довільної форми Tektronix AFG 3252.
2. Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B 2 Hz-26.5 GHz.
3. Осцилограф Tektronix DPO 7254 (Digital Phosphor Oscilloscope).
4. Комплекс антен дипольних Tuned Dipole Antenna FCC.
5. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 MHz – 7000 MHz.
6. Антена електрична ЕМА-2000 0.009 – 2000 МГц.
7. Персональний комп’ютер стаціонарного типу (монітор, маніпулятор типу «Миша», клавіатура, системний блок) (далі - ПК).

Перелік обладнання комплексу для проведення експериментальних досліджень представлена на Рис. 4.3.

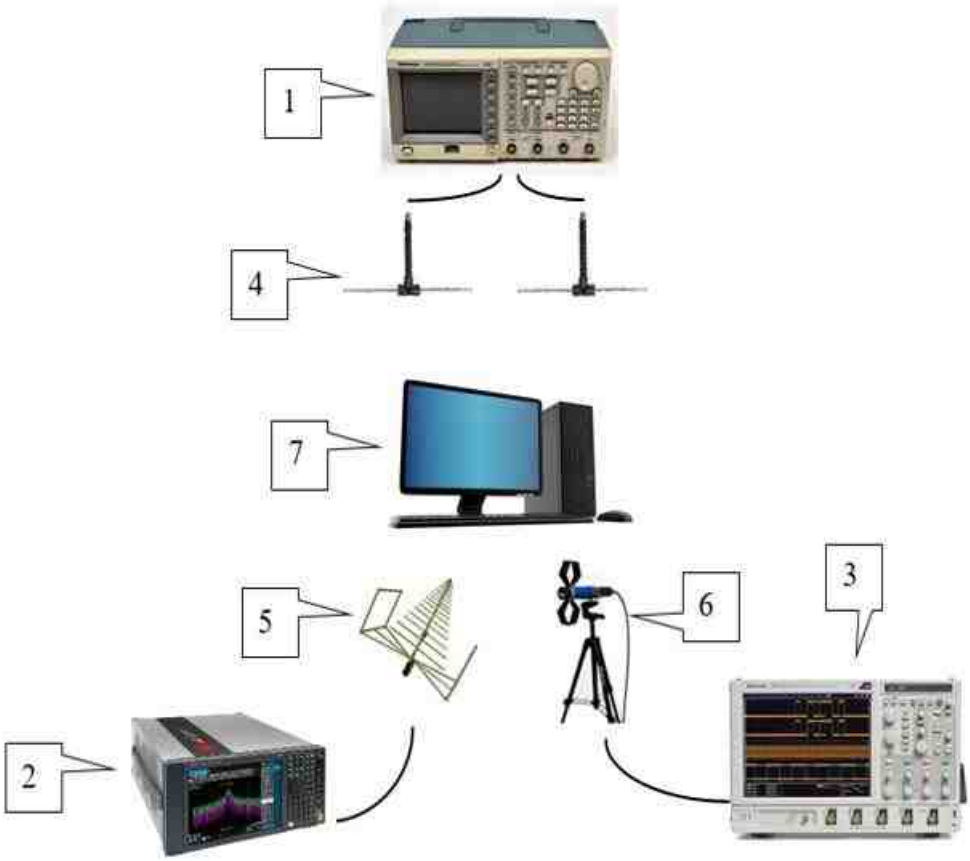


Рис. 4.3. Перелік обладнання для проведення експериментальних досліджень у складі: 1 – Генератор сигналів довільної форми Tektronix AFG 3252; 2 – Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B; 3 – Осцилограф Tektronix DPO 7254; 4 – Комплекс антен дипольних Tuned Dipole Antenna FCC; 5 – Антена білогоперіодична SAS-521F-7; 6 - Антена електрична EMA-2000; 7 – Персональний комп’ютер стаціонарного типу.

Детальний опис переліку обладнання для проведення експериментальних досліджень:

1. Генератор сигналів довільної форми Tektronix AFG 3252.

Основні технічні характеристики:

- сигнали синусоїндної форми частотою до 10 МГц, 25 МГц, 100 МГц або 240 МГц;

- сигнали довільної форми з роздільною здатністю 14 розрядів, 250 Мвиб/с, 1 Гвиб/с или 2 Гвиб/с;
- амплітуда до 20 Впік-пік на навантаженні 50 Ом.

2. Аналізатор спектру та сигналів Keysight PXA Signal Analyzer N9030B 2 Hz-26.5 GHz.

Основні технічні характеристики:

- стандартний діапазон аттенюатора: 70 дБ;
- стандартний крок аттенюатора: 2 дБ;
- параметри смуги пропускання в реальному часі: 85, 160, 255, 510 МГц;
- DANL на 1 ГГц: -174 дБм;
- максимальна смуга пропускання аналізу: 510 МГц;
- фазовий шум при 1 ГГц (зсув 1 МГц): -146 дБн/Гц;
- фазовий шум при 1 ГГц (зсув 10 кГц): -136 дБн/Гц;
- фазовий шум при 1 ГГц (зсув 30 кГц): -136 дБн/Гц;

3. Осцилограф Tektronix DPO 7254 (Digital Phosphor Oscilloscope).

Основні технічні характеристики:

- частота дискретизації в режимі реального часу до 40 Гвиб./с по одному каналу, до 20 Гвиб./с по двох каналах;
- довжина запису осцилограм з використанням функції MultiView Zoom™ - до 500 млн точок;
- максимальна швидкість захоплення вхідного сигналу з використанням функції FastAcq™ >250 000 осцилограм в секунду;
- швидкість захоплення в режимі FastFrame™ з використанням сегментованої пам’яті FastFrame™ >310 000 осцилограм в секунду;
- можливість вибору користувачем фільтрів обмеження смуги рпопускання для підвищення точності виміру низькочастотних сигналів.

4. Комплекс антен дипольних Tuned Dipole Antenna FCC.

Основні технічні характеристики:

- діапазон частоти - 325 МГц – 1 ГГц;
- втрати балуна - 0 до 2 дБі;
- фактор антени - 20 – 29 дБ/м;
- максимальа потужність - 60 Вт;
- імпеданс – 50 Ом;
- тип роз’єму - N-Type, female.

5. Антена білогоперіодична SAS-521F-7 (Folding Bilogical Antenna SAS-521F-7) 25 МГц – 7000 МГц.

Основні технічні характеристики:

- діапазон частоти - 25 МГц – 7000 МГц;
- фактор антени - 7 – 47 дБ/м;
- підсилення - 27 до 7 дБі;
- максимальна потужність - 400 Вт;
- максимальне випромінювання поля - 100 В/м;
- імпенданс - 50 Ом;
- роз’єм антени типу N-Type, Female;
- база для монтажу - ¼ x 20 Thread, Female.

6. Антена електрична ЕМА-2000 0.009 – 2000 МГц.

Основні технічні характеристики:

- діапазон частоти - 0,009…2000 МГц;
- коефіцієнт калібрування антени - 30,0;
- номінальне значення, дБ 1/м;
- відхилення від номінального значення на частоті 10 МГц, не більше, дБ - ± 2;
- нерівномірність частотної характеристики, не більше, дБ – 10;
- похибка коефіцієнта калібрування, не більше, дБ - ± 2;
- найбільша вимірювана напруженість електричного поля, дБ мкВ/м – 120;
- вихідний опір антени (номінальне значення), Ом – 50.

7. Персональний комп’ютер стаціонарного типу (монітор, маніпулятор типу «Миша», клавіатура, системний блок).

4.3. Проведення експериментальних досліджень параметрів захисних сигналів

4.3.1. Визначення різниці частот між захисним та небезпечним сигналами

Для експерименту було встановлено небезпечний сигнал на рівні 181 МГц.

За результатами проведення експериментальних досліджень отримано наступні результати:

1. Дослідження ефекту биття частот у випадку, коли захисний сигнал кардинально відрізняється від небезпечного, $\Delta\omega = 225$ МГц:

Рис. 4.4. Фотографічне зображення сигналів на екрані аналізатора

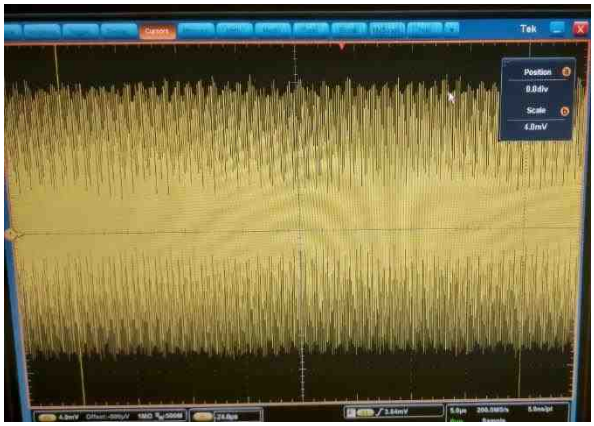


Рис. 4.5. Фотографічне зображення сигналів на екрані осцилографа

Результат: ефект биття не спостерігається при такій великій різниці між небезпечним та захисним сигналом.

2. Дослідження аналогічні до п. 1, але зменшена різниця між сигналами, становить Δω =30 МГц:

Рис. 4.6. Фотографічне зображення сигналів на екрані аналізатора

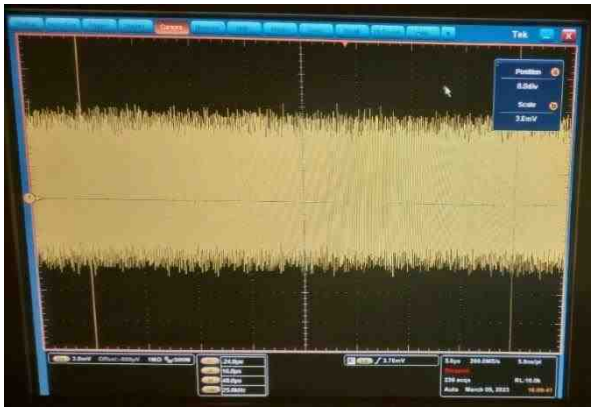


Рис. 4.7. Фотографічне зображення сигналів на екрані осцилографа

Результат: аналогічно з п. 1, ефекту биття частот не спостерігається.

3. Дослідження утворення ефекту биття частот у випадку, якщо небезпечний та захисний сигнали мають однакову частоту:

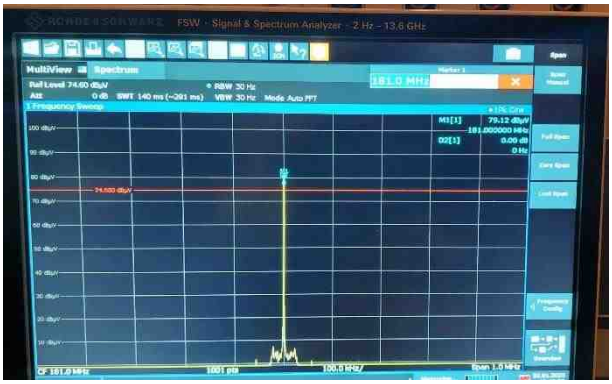


Рис. 4.8. Фотографічне зображення сигналів на екрані аналізатора

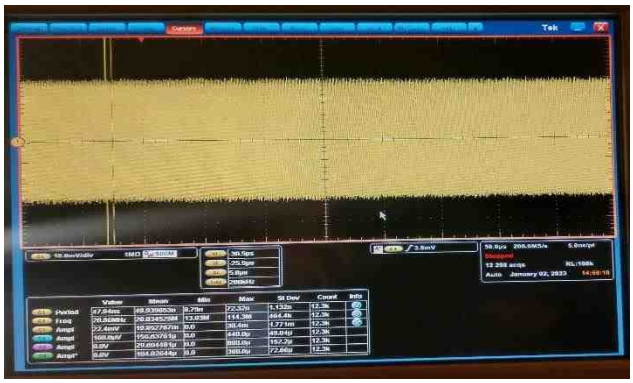


Рис. 4.9. Фотографічне зображення сигналів на екрані осцилографа

Результат: аналогічно з п. 1, ефекту биття частот не спостерігається.

4. Дослідження моменту, коли починається утворення ефекту биття частот шляхом мінімального збільшення частоти захисного сигналу:

Рис. 4.10. Фотографічне зображення сигналів на екрані аналізатора

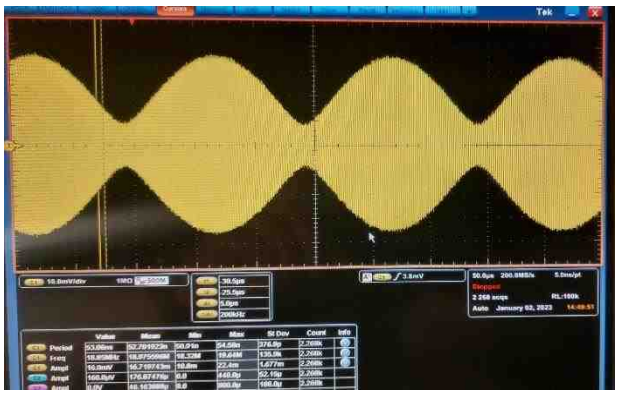


Рис. 4.11. Фотографічне зображення сигналів на екрані осцилографа

Результат: виявлення ознак ефекту биття при різниці між небезпечним та захисним сигналами Δω=6 кГц.

5. Дослідження допустимої різниці частот між небезпечним та захисним сигналом, при якому зберігається ефект биття частот. Також перевіка дзеркальності ефекту, чи зберігається він, якщо зондуючий сигнал бути по частоті меншим за небезпечний. Збільшення різниці, Δω=9 кГц:

Рис. 4.12. Фотографічне зображення сигналів на екрані аналізатора

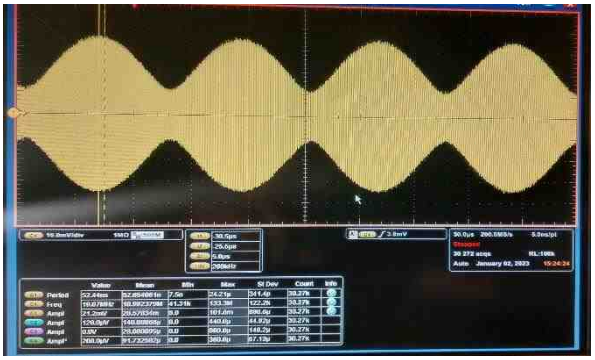


Рис. 4.13. Фотографічне зображення сигналів на екрані осцилографа

Результат: ефект биття частот зберігається. Також підтверджено дзеркальність, що означає, що зондуючий сигнал може бути більш варіативним.

6. Дослідження відповідно до п.5, пошук перших ознак втрати ефекту биття частот. Збільшення різниці, Δω=16 кГц:

Рис. 4.14. Фотографічне зображення сигналів на екрані аналізатора

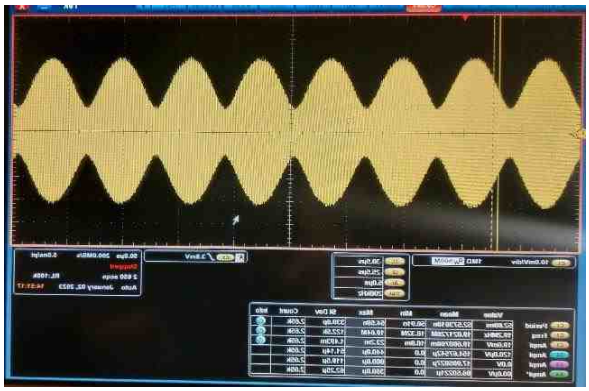


Рис. 4.15. Фотографічне зображення сигналів на екрані осцилографа

Результат: ефект биття частот зберігається. Також підтверджено дзеркальність, що означає, що зондуючий сигнал може бути більш варіативним.

7. Дослідження відповідно до п. 5, пошук перших ознак втрати ефекту биття частот. Збільшення різниці, Δω=100 кГц:

Рис. 4.16. Фотографічне зображення сигналів на екрані аналізатора

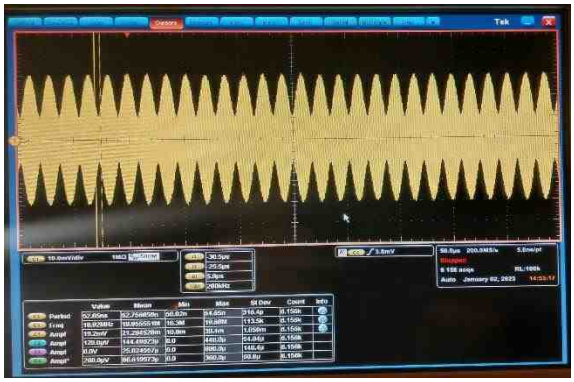
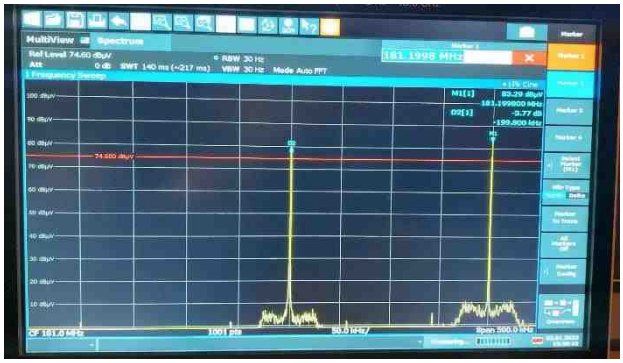


Рис. 4.17. Фотографічне зображення сигналів на екрані осцилографа

Результат: ефект биття частот зберігається, але його якість втрачається.

8. Дослідження відповідно до п.5, пошук перших ознак втрати ефекту биття частот. Збільшення різниці, Δω=200 кГц:



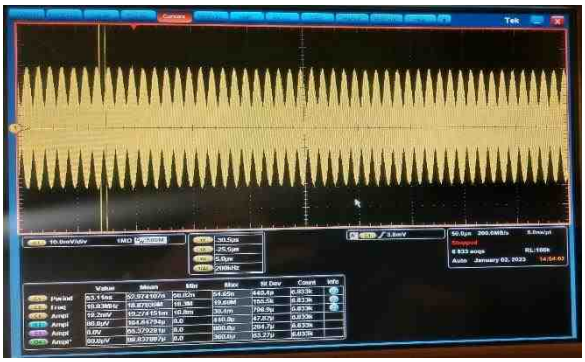


Рис. 4.18. Фотографічне зображення сигналів на екрані аналізатора

Рис. 4.19. Фотографічне зображення сигналів на екрані осцилографа

Результат: ефект биття частот зберігається, але його якість втрачається.

9. Дослідження відповідно до п.5, пошук перших ознак втрати ефекту биття частот. Збільшення різниці, Δω=1 МГц:

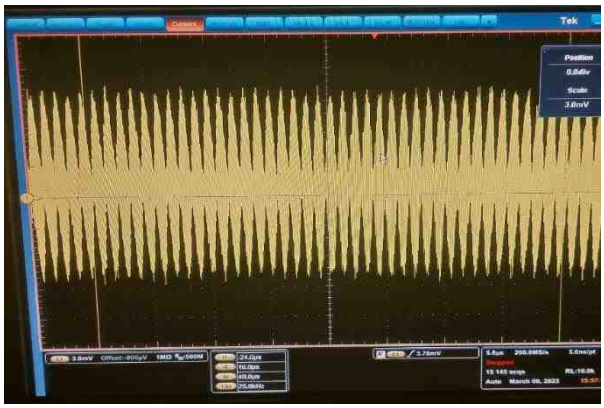


Рис. 4.20. Фотографічне зображення сигналів на екрані аналізатора

Рис. 4.21. Фотографічне зображення сигналів на екрані осцилографа

Результат: при різниці Δω=1 МГц спостерігається практично крайній варіант ефекту биття, який вже не настільки якісний. Після цієї різниці ефекту не спостерігається.

Висновки проведення експериментальних досліджень щодо пошуку ріхниці частот $\Delta\boldsymbol{\omega}$, в межах якого забезпечується захищеність інформації від витоку каналами високочастотного нав'язування: експериментальним методом знайдено наступну різницю частот небезпечного та захисного сигналу, яка складає -1 МГц $< \Delta\omega <$ 1МГц за виключенням $\Delta\omega = 0$.

4.3.2. Дослідження впливу зміни фази захисного сигналу на захищеність інформації

Експериментальні дослідження проводяться задля виявлення залежності якості захисного сигналу від зміни фази зондуючого захисного сигналу. Для цього використаємо різницю частот 40 кГц, при якій відповідно до п. 4.3.1 спостергіається явище биття частот:

1. Зміщення фази захисного сигналу на 10 °:

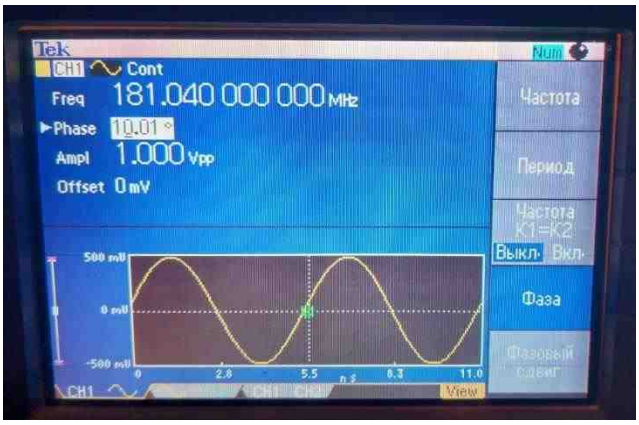


Рис. 4.22. Фотографічне зображення зміщення фази на екрані генератора

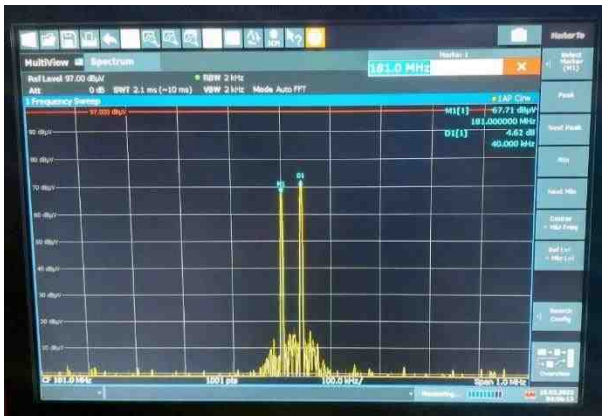


Рис. 4.23. Фотографічне зображення сигналів на екрані аналізатора

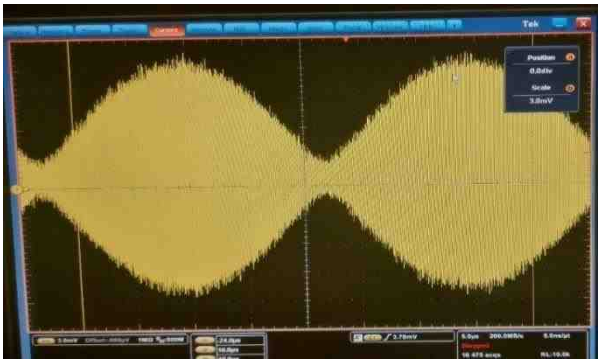


Рис. 4.24. Фотографічне зображення сигналів
на екрані осцилографа

Результат: зміщення фази захисного сигналу на 10 ° не впливає на загальну якість захисного сигналу.

2. Зміщення фази захисного сигналу на 30 °:

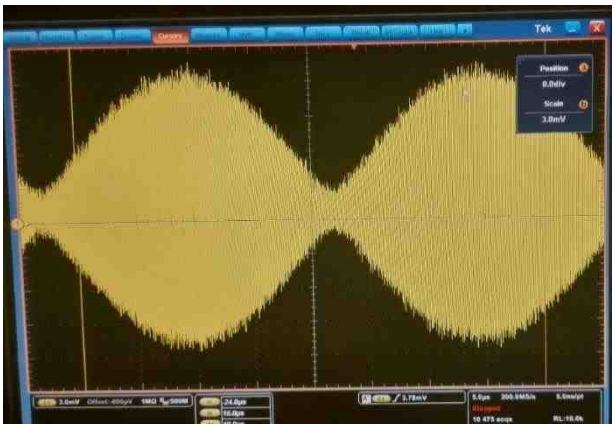
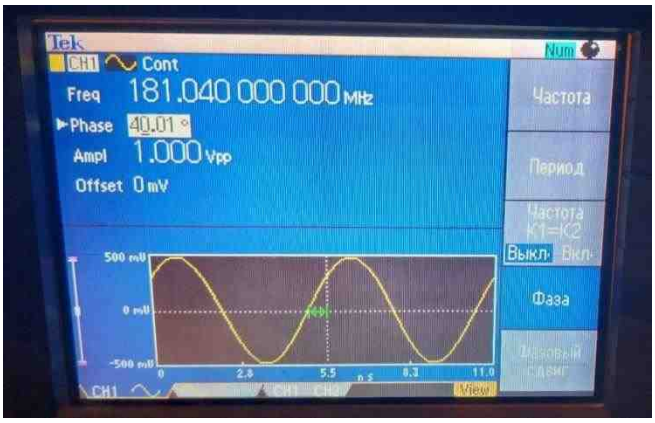


Рис. 4.25. Фотографічне зображення зміщення фази на екрані генератора

Рис. 4.26. Фотографічне зображення сигналів на екрані осцилографа

Результат: зміщення фази захисного сигналу на 30 ° не впливає на загальну якість захисного сигналу.

3. Зміщення фази захисного сигналу на 40 °:



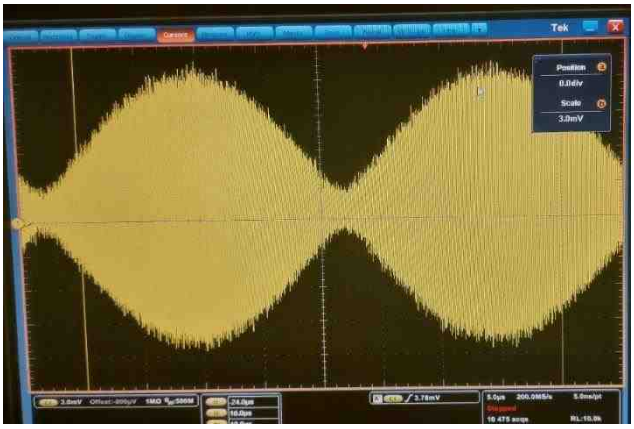
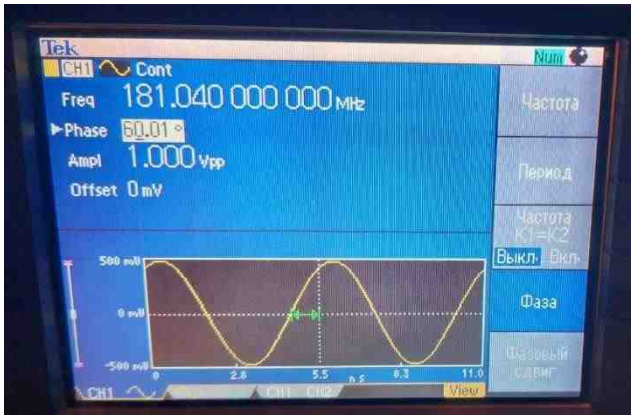


Рис. 4.27. Фотографічне зображення зміщення фази на екрані генератора

Рис. 4.28. Фотографічне зображення сигналів на екрані осцилографа

Результат: зміщення фази захисного сигналу на 40 ° не впливає на загальну якість захисного сигналу.

4. Зміщення фази захисного сигналу на 60 °:



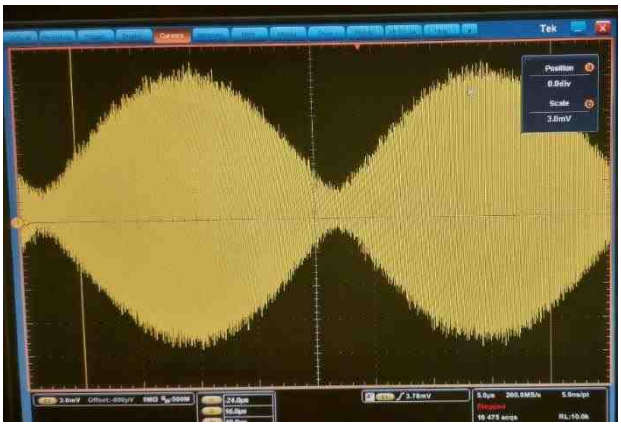
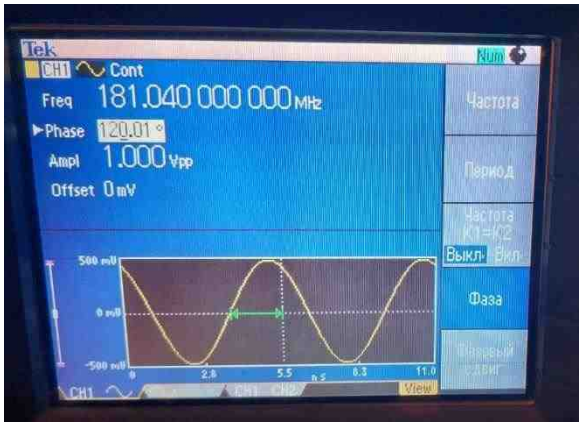


Рис. 4.29. Фотографічне зображення зміщення фази на екрані генератора

Рис. 4.30. Фотографічне зображення сигналів на екрані осцилографа

Результат: зміщення фази захисного сигналу на 60 ° не впливає на загальну якість захисного сигналу.

5. Зміщення фази захисного сигналу на 120 °:



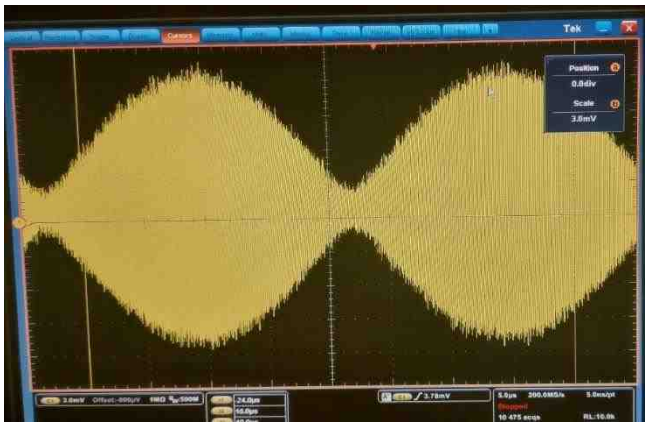
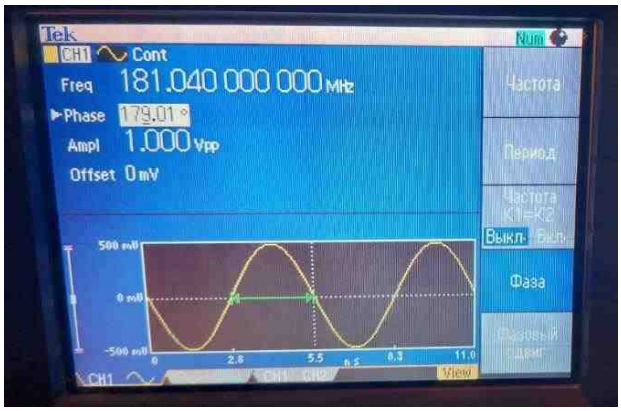


Рис. 4.31. Фотографічне зображення зміщення фази на екрані генератора

Рис. 4.32. Фотографічне зображення сигналів на екрані осцилографа

Результат: зміщення фази захисного сигналу на 120 ° не впливає на загальну якість захисного сигналу.

6. Зміщення фази захисного сигналу на 179 °:



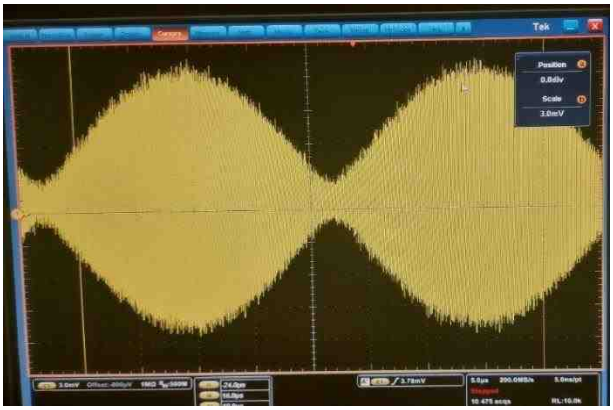


Рис. 4.33. Фотографічне зображення зміщення фази на екрані генератора

Рис. 4.34. Фотографічне зображення сигналів на екрані осцилографа

Результат: зміщення фази захисного сигналу на 179 ° не впливає на загальну якість захисного сигналу.

Висновки щодо проведення експериментальних досліджень залежності якості захисного сигналу від зміни фази зондуючого захисного сигналу: зміна

фази захисного сигналу не впливає на його здатність утворювати ефект биття частот із небезпечним сигналом.

4.4. Експериментальна оцінка ефективності завадових захисних сигналів

Для проведення екпериментальних досліджень на ПК запускається тестова програма, яка імітує максимальну навантаженість роботи по заданому інтерфейсу. Для проведення експерименту вибрано інтерфейс монітору (з роз’ємом VGA (DE-15)), адже на моніторі може відображатись інформація з обмеженим доступом, яка може бути перехоплена.

Моделюємо ідеальні умови, коли у зловмисника є можливості для перехоплення інформації методом ВЧН, а саме: йому відоме місце встановлення ПК, на якому обробляється інформація з обмеженим доступом, в наявності засоби, які дозволяють здійснити перехоплення.

Дослідним шляхом визначено тактову частоту монітору/інтерфейсу монітору.

1. В діапазоні 0 – 2 ГГц фіксуємо частоти згідно тактової з максимальним рівнем сигналу, після чого обираємо одну (1812,5255 МГц), яка має найкраще співвідношення якість/рівень та на цій самій частоті вмикаємо перший канал генератора, який підсилює корисний сигнал, встановивши рівень сигналу 30 dBμV:

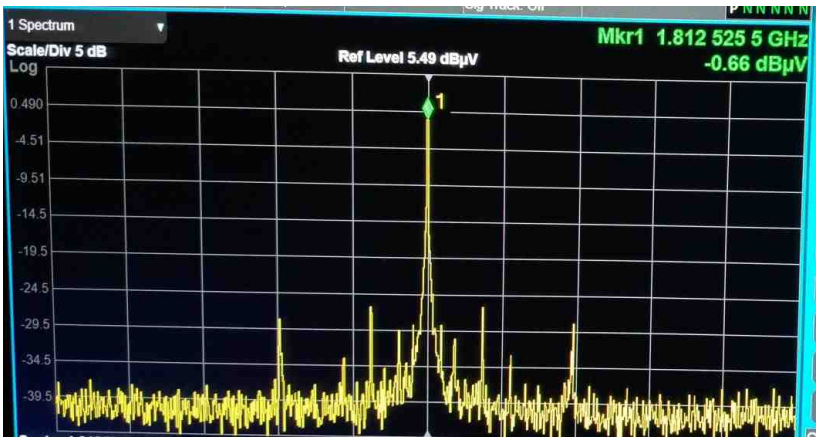


Рис. 4.35. Фотографічне зображення сигналу на екрані аналізатора

Результат: спостерігаємо корисний сигнал з рівнем -0.66 dBµV.

2. Включаємо другий канал генератора, встановивши рівень сигналу 30 dBµV на частоту 1812,4255 МГц і отримуємо наступний результат:

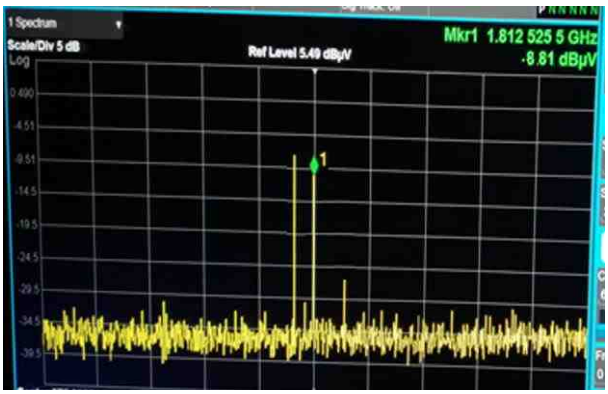


Рис. 4.36. Фотографічне зображення сигналів на екрані аналізатора

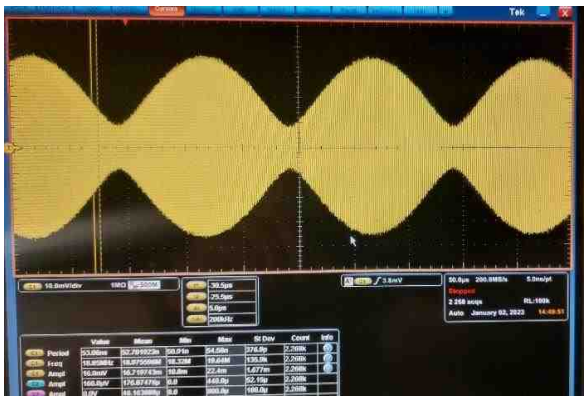


Рис. 4.37. Фотографічне зображення сигналів на екрані осцилографа

Результат: спостерігаємо суттєве зниження рівня корисного сигналу до позначки -8.81 dBµV (Рис. 4.36) завдяки ефекту «биття» (Рис. 4.37), яке відбувається за участі корисного сигналу (який ще підсилений сигналом з 1 каналу генератора) та сигналу з 2 каналу генератора. Ймовірність перехоплення інформації зменшується вже після проведення такої процедури, тому що менший рівень корисного сигналу зменшує ймовірність того, що зловмисник зможе перехопити інформацію якісно та без спотворень.

3. Додаємо до сигналу з 2 каналу генератора ефект «качання» частоти, додаючи та віднімаючи 400 кГц (діапазон від 1812,0255 МГц до 1812,8255 МГц):

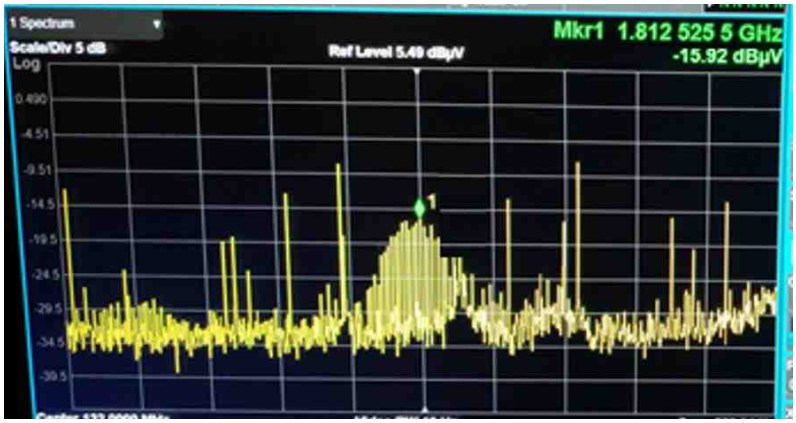


Рис. 4.38. Фотографічне зображення сигналу на екрані аналізатора

Результат: спостерігаємо ефект так званого зашумлення та спотворення корисного сигналу разом із зменшенням загального рівня всіх сигналів (максимальний рівень сигналу серед цього зашумлення складає -15.92 dBµV) (Рис. 4.38). Таким чином ймовірність перехоплення зловмисником інформації знову зменшується. За допомогою «качання» здійснюється часткова руйнація інформативних параметрів небезпечного сигналу (зниження рівня сигналу, спотворення сигналу, зашумлення діапазону в межах здійснення «качання» частот).

4.5. Визначення коефіцієнту захищеності інформації від витоку та можливості відтворення

Експериментальні дослідження проводились з метою підтвердження теоретичних відомостей та здійснення загальної оцінки ефективності запропонованого методу з дотриманням відповідних вимог щодо достовірності.

Для оцінки ефективності завадових захисних сигналів потрібно використовувати поняття коефіцієнту захищеності, під яким розуміється мінімально необхідне відношення потужності завади до потужності сигналу

на вході приймача в межах смуги пропускання його лінійної частини, що забезпечує задану втрату інформації.

Величина коефіцієнту захищеності радіолінії зв’язку визначається видом завади і її спектральними характеристиками, розладом завади відносно резонансної частоти завадового приймаючого приладу, видом модуляції, який застосовується в радіолінії.

Найважливішим питанням визначення коефіцієнта захищеності є поняття завданої втрати інформації.

Умова визначення коефіцієнта захищеності за мінімально необхідним відношенням потужності завади до потужності сигналу пов'язана з тим, що коефіцієнт захищеності має бути пороговим значенням цього відношення, щоб за його допомогою можна було визначати межу зони захищеності.

Коефіцієнт захищеності розраховується за формулою:

$$K_{\text{з}} = \frac{U_{\text{г}}}{U_{\text{с}}}, \tag{4.1}$$

де:

$K_{\text{з}}$ – коефіцієнт захищеності, який показує якість спотворення небезпечного сигналу;

$U_{\text{г}}$ – енергетична складова сигналу, виміряна в смузі, яка необхідна для перехоплення сигналу, при включеному генераторі з ефектом «биття» та «качання» частоти з врахуванням коефіцієнту поправки антени (дані з сертифікату калібрування/повірки або заводської документації);

$U_{\text{с}}$ – енергетична складова сигналу, виміряна в смузі, яка необхідна для перехоплення сигналу, небезпечного сигналу з впливом на нього генератора противника / або чистий сигнал з врахуванням коефіцієнту поправки антени (дані з сертифікату калібрування/повірки або заводської документації).

Згідно проведених експериментів було розраховано коефіцієнти захищеності для наступних випадків:

1. При умові включеного обладнання, запущеної тестової програми, яка імітує максимальну навантаженість роботи по заданому інтерфейсу та без роботи захисного обладнання. Відповідно у зловмисника є можливість безперешкодно перехопити сигнал, який містить інформацію з обмеженим доступом, використовуючи ВЧН.

$$K_{з1} = \frac{10^{\frac{-3}{20}}}{10^{\frac{-7}{20}}} = 0.63 \tag{4.2}$$

2. При умові включеного обладнання, запущеної тестової програми, яка імітує максимальну навантаженість роботи по заданому інтерфейсу та з роботи захисного обладнання.

$$K_{з2} = \frac{10^{\frac{3}{20}}}{10^{\frac{-7}{20}}} = 4.42 \tag{4.3}$$

Експериментальні дослідження були проведені емпіричним шляхом. Були зроблені висновки, що при умові $К_з \geq 2$ виділення зі спектру частот корисного сигналу зі збереженням неспотворених параметрів сигналу задля подальшого виділення корисної інформації буде ускладненим.

На Рис. 4.39 продемонстровано порівняльну характеристику енергетичних складових сигналів в діапазоні 0 – 2 ГГц в трьох випадках:

1. $U_ш$ – сигнал по рівню шумів, без включеного обладнання, на якому обробляється інформація з обмеженим доступом.

2. $U_с$ – корисний сигнал з впливом на нього генератора противника / або чистий сигнал.

3. $U_г$ – сигнал при включеному генераторі з ефектом «биття» та «качання» частоти.

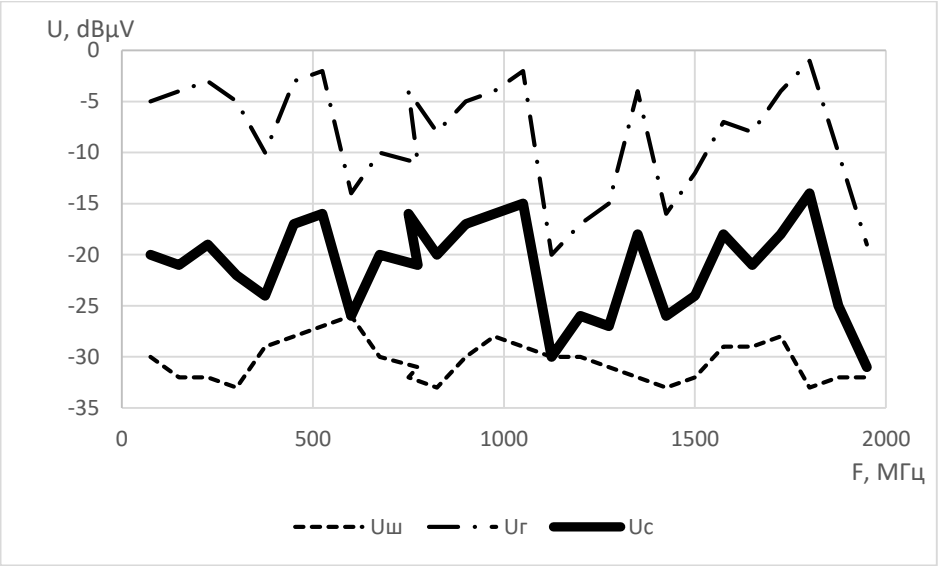


Рис. 4.39. Порівняльна характеристика енергетичних складових сигналу для різних умов захисту в діапазоні 0 – 2 ГГц

На Рис. 4.40 продемонстровано значення коефіцієнтів захищеності на фіксованих частотах в діапазоні 0 – 2 ГГц для різних умов захисту:

1. $K_{з1}$ – при умові відсутнього захисту інформації від витоку та роботи зловмисника щодо її перехоплення.

2. $K_{з2}$ – при умові використання методу ВЧН для захисту інформації від витоку та роботи зловмисника щодо її перехоплення.

3. $K_{з3}$ – при умові використання запропонованого методу ВЧН (з використанням ефектів «биття» та «качання») для захисту інформації від витоку та роботи зловмисника щодо її перехоплення.

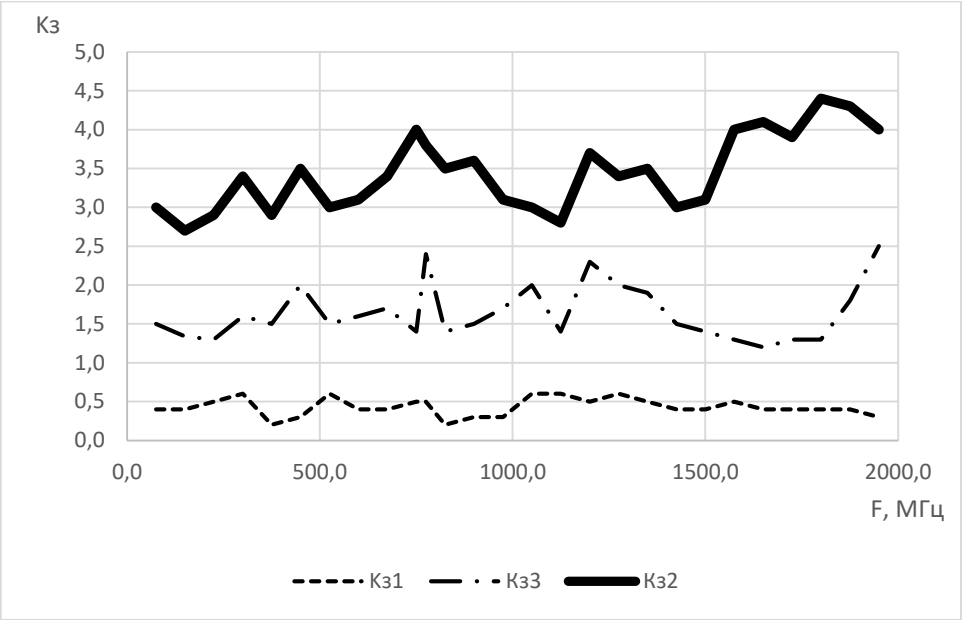


Рис. 4.40. Значення коефіцієнтів захищеності на фіксованих частотах для різних умов захисту в діапазоні 0 – 2 ГГц

Відповідно застосування запропонованого активного методу із застосуванням ефекту «биття» та «качання» частот зменшує ймовірність перехоплення інформації та її відтворення в 1,5-3 рази в порівнянні з використанням звичайного активного методу.

Ефективність методу високочастотного нав'язування загалом визначається як результат взаємодії наступних технічних систем:

- системи перехоплення інформації;
- системи передачі, обробки і зберігання інформації;
- системи зв’язку.

Апріорні результати взаємодії цих систем можуть оцінюватися проведенням системного аналізу функціонування складної технічної системи, що складається з трьох зазначених складових частин.

Застосування активних методів захисту – так званих систем руйнування інформації – може бути рекомендовано лише в сукупності з добре виконаним

пасивним захистом, захистом екрануванням, фільтрацією та розв'язками, для подальшого підвищення ступеня ефективності захисту.

Як міра кількісної оцінки ступеня захищеності інформації в технічних засобах, які безпосередньо обробляють інформацію з обмеженим доступом, може бути прийнята ймовірність витоку інформації.

При проведенні експериментальних досліджень встановлено:

- Задля досягнення ефекту «биття» частот потрібно використовувати максимально схожі за вихідними характеристиками генератори сигналів.
- При різниці частот більшій, ніж 1 МГц між небезпечним сигналом та зондуючим сигналом ефект «биття» частот не спостерігається.
- Зміна фази одного із сигналів ніяким чином не впливає на виникнення ефекту «биття» частот.
- За допомогою оцінки ефективності встановлено, що при умові, якщо коефіцієнт захищеності при застосуванні запропонованого методу становить $K_з \geq 2$, що дозволяє збільшити ефективність захисту інформації в 1,5-3 рази в залежності від діапазону.

Висновки до розділу 4

Розроблено активний метод захисту інформації від витоку каналами високочастотного нав’язування.

Поданий метод забезпечує захист інформації шляхом руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках зондуючого сигналу.

1. Встановлено, що застосування активних методів захисту – так званих систем руйнування інформації – може бути рекомендовано лише в сукупності з добре виконаним пасивним захистом, захистом екрануванням,

фільтрацією та розв'язками, для подальшого підвищення ступеня ефективності захисту.

2. Показано, що величина коефіцієнту захищеності, як міра оцінки ефективності завадових захисних сигналів, визначається видом завади і її спектральними характеристиками, розладом завади відносно резонансної частоти завадового приймаючого приладу, видом модуляції, який застосовується в радіолінії. Найважливішим питанням визначення коефіцієнта захищеності є поняття завданої втрати інформації.

3. Запропоновані програми і методики експериментальних досліджень параметрів захисного сигналу дозволяють якісно дослідити ефективність запропонованого методу.

4. Подано параметри захисних сигналів, які дозволяють максимально ефективно розрахувати коефіцієнт захищеності:

- задля досягнення ефекту «биття» частот потрібно використовувати максимально схожі за вихідними характеристиками генератори сигналів;
- при різниці частот більшій, ніж 1 МГц між небезпечним сигналом та зондуючим сигналом ефект «биття» частот не спостерігається;
- зміна фази одного із сигналів ніяким чином не впливає на виникнення ефекту «биття» частот.

5. Удосконалено оцінку ефективності захисту інформації від витоку каналами високочастотного нав’язування та встановлено, що при умові, якщо коефіцієнт захищеності при застосуванні запропонованого методу становить $K_з \geq 2$, дозволяє збільшити ефективність захисту інформації в 1,5-3 рази в залежності від діапазону.

ВИСНОВКИ

В результаті дисертаційних досліджень, виконаних автором, вирішено наукове завдання щодо розробки методу захисту інформації від високочастотного нав’язування як на основних, так і на комбінаційних гармоніках зондуючого сигналу. Дане наукове завдання має важливе значення для теорії і практики технічного захисту інформації, створення та забезпечення функціонування інформаційних систем і технологій на об’єктах інформаційної діяльності та критичних інфраструктур сфери кібербезпеки та захисту інформації. Відсутність аналогічних рішень в нашій країні і закордоном робить результати досліджень пріоритетними.

Отримані результати мають важливе значення для модернізації існуючих та в процесі розробки нових методів захисту інформації від витоку каналами високочастотного нав’язування.

На підставі проведених досліджень зроблені наступні висновки:

1. Аналіз відомих методів захисту інформації від витоку каналами високочастотного нав’язування показав, що на сьогоднішній день існуючі методи не враховують загрози перехоплення інформації на комбінаційних гармоніках зондуючого сигналу. Відтак необхідним є розробка методу захисту інформації від високочастоного нав’язування як на основних, так і на комбінаційних гармоніках сигналу.

2. Вперше запропоновано модель блокування процесу перехоплення інформації каналами високочастотного нав’язування, яка на основі процесу суперпозиції близьких по частоті гармонічних коливань дозволяє забезпечити ефект «биття» частот шляхом руйнування інформативних параметрів небезпечних сигналів і блокує витік інформації каналами високочастотного нав’язування.

3. Удосконалено модель захисту інформації від витоку каналами високочастотного нав’язування, яка, на відміну від існуючих, побудована на

основі навмисного «качання» частоти і забезпечує руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування не тільки на основній частоті, а й на комбінаційних гармоніках небезпечного зондуючого сигналу.

4. Удосконалено модель розрахунку коефіцієнта оцінки захищеності інформації, яка, на відміну від існуючих, побудована на основі порівняння енергетичних складових, виміряних в смугах, достатніх для перехоплення, небезпечних та захисних сигналів і забезпечує кількісну оцінку захищеності на основі встановленого значення коефіцієнта з врахуванням параметрів та значень небезпечного зондуючого сигналу.

5. Вперше розроблено метод захисту інформації від витоку каналами високочастотного нав’язування, який базується на основі алгоритму блокування та руйнування інформативних параметрів небезпечного сигналу високочастотного нав’язування, що забезпечує захист інформації по заданих значеннях коефіцієнта захищеності.

6. Застосування запропонованого методу та моделей дозволяє підвищити значення коефіцієнта захищеності з врахуванням параметрів та значень небезпечного зондуючого сигналу в 1.5-3 рази. Удосконалена модель захисту інформації дозволяє покращити ефективність захисту інформації від витоку каналами високочастотного нав’язування на 17-48%.

7. Мета дослідження щодо підвищення ефективності захисту інформації від витоку каналами високочастотного нав’язування досягнута і всі часткові завдання вирішені повністю. Наукові результати можуть бути використані дослідно-конструкторськими організаціями та державними структурами при розробці та удосконаленні оцінки захищеності інформації під час проведення інструментального контролю різнотипних об’єктів інформаційної діяльності критичної інфраструктури та вирішення комплексних проблем щодо захисту інформації на об’єктах інформаційної діяльності критичної інфраструктури.

8. Напрямками подальших досліджень у зазначеній галузі можуть бути:

- удосконалення критеріїв оцінки захищеності інформації різнотипних об’єктів інформаційної діяльності критичної інфраструктури;
- розробка рекомендацій щодо удосконалення існуючих методик спеціальних досліджень для оцінки захищеності інформації від витоку каналами високочастотного нав’язування;
- дослідження підходів щодо технічної реалізації запропонованого методу захисту інформації від витоку каналами високочастотного нав’язування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Боднар І. Р. "Інформаційна безпека як основа національної безпеки." Mechanism of Economic Regulation 1 (2014): с. 68-75.

2. Ніщименко О. А. "Інформаційна безпека України на сучасноиу етапі розвитку держави і суспільства." Наше право 1 (2016): с. 17-23.

3. Хмелевський Р. М. "Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності." Сучасний захист інформації 4 (2016): с. 65-70.

4. Степко О. М. "Аналіз головних складових інформаційної безпеки держави." Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм 1.3 (2011): с. 90.

5. Бахтіяров Д. І. "Оцінка можливості перехоплення семантичної інформації за рахунок побічних електромагнітних випромінювань у відеосистемі персонального комп’ютера" Colloquium-journal. No. 26 (78). Голопристанський міськрайонний центр зайнятості, 2020.

6. Габрусенко Євген, Валерій Павлов, Інна Михальчук. "Запобігання витоку інформації у бездротових мереж." Безпека інформації. - 2014. - Т. 20, № 1. - С. 17-20.

7. Котерлін І. Б. (2022). "Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод information security in martial law in terms of ensuring information rights and freedoms." Актуальні проблеми вітчизняної юриспруденції, 1.

8. Opyrskyy I., Sovyn Y., Datsenko Y., & Usyk M. (2021). Аналіз методів та засобів протидії лазерним системам розвідки. Ukrainian Scientific Journal of Information Security, *27*(3), с. 142-149.

9. Yemelyanov V., & Bondar H. (2019). Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. Public Administration and Regional Development, (5), с. 493-523.

10. Гнатюк С. О., Рябий М. О., & Лядовська В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв'язок, (4), с. 3-7.

11. Бірюков Д. С., & Кондратов С. І. (2012). Стратегія захисту критичної інфраструктури в системі національної безпеки держави. Стратегічні пріоритети, (3), с. 24.

12. Перевалова Л. В. Захист конфіденційної інформації: проблеми та шляхи вирішення / Л. В. Перевалова, С. В. Кваша // Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип. : Актуальні проблеми розвитку українського суспільства. – Харків : НТУ "ХПІ". – 2011. – № 30. – С. 55-61.

13. Водоп’ян С. В., Д. В. Пясковський, О. М. Романов. "Алгоритм цифрової еквівалентної комбінованої системи фазового автопідстроювання частоти для демодуляції сигналів з фазовою маніпуляцією." // Вісник ЖДТУ. 2013. № 1 (64) (2010).

14. Ткаченко В. В. Особливості практичного використання методів високочастотного" навязування". Захист інформації, 11(1 (42)), с. 75-78.

15. Цибуляк Б. З. (2013). Захист інформації від витоку каналами телефонного зв’язку. Вісник Національного технічного університету України Київський політехнічний інститут. Серія: Радіотехніка. Радіоапаратобудування, (55).

16. Yelchenkov, V., & Smyrnov, O. (2020). Сучасні підходи до класифікації загроз безпеці інформації, яка циркулює на об’єктах інформаційної діяльності національної гвардії україни. Честь і Закон, 2(73), с. 27-32.

17. Якубенко В. В. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Актуальні проблеми кібербезпеки, с. 179.

18. Конахович Г. Ф., Голубничий О. Г., & Пузиренко О. Ю. (2007). Оцінка ефективності систем захисту інформації в телекомунікаційних системах. Проблеми інформатизації та управління, *3*(21), с. 75-83.

19. Стащук А. А., & Кочкін В. Г. (2023). Організація безпеки та захисту об’єктів критичної інфраструктури україни. Актуальні проблеми забезпечення державної безпеки: матеріали, с. 241.

20. Єрменчук О. (2018). Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки. Jurnalul juridic national: teorie şi practică, 34(6), 50-54.

21. Gnatyuk S., Sydorenko V., & Sotnichenko Y. (2020). Базові аспекти захисту конфіденційної інформації на об’єктах критичної інформаційної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(9), с. 170-181.

22. Цурко Ю. В. Фактори, які впливають на стан кібербезпеки об’єктів критичної інфраструктури. Актуальні проблеми управління інформаційною безпекою держави, с. 229.

23. Сидоренко В., Єременко С., Пруський А., & Демків А. (2021). Оцінка уразливості критично важливих об’єктів. Kolegium redakcyjne, с. 177.

24. Прокофьєв М. І., & Стеченко В. М. (2015). Особливості мережі електроживлення як каналу витоку побічних випромінювань від електронно-обчислювальної техніки. Вісник Національного університету Львівська політехніка. Автоматика, вимірювання та керування, (821), с. 100-104.

25. Досенко, С. Д. (2021). Технічний захист інформації. Основні проблеми та способи їх вирішення. Вісник ЛТЕУ. Технічні науки, (27), с. 27-32.

26. Степанов М., Бойко Ю., & Павленко Є. (2023). Визначення необхідного рівня сигналу та маскуючого шуму для захисту інформації в умовах її перехоплення технічними засобами. Measuring and computing devices in technological processes, (2), с. 21-27.

27. Шокало В. М., Усін В. А., Грецьких Д. В., Хорошко В. О., & Крючкова Л. П. (2012). Поля і хвилі в системах технічного захисту інформації. Харків: ХНУРЕ.

28. Kataiev V. C., Grycak A. V., Leontiev V. O., & Liahovchenko N. V. (2016). Проблеми активного захисту інформації від витоку через віброакустичні канали. Реєстрація, зберігання і обробка даних, 18(3), с. 54-58.

29. Шатило, Я. Л. (2015). Підвищення ефективності функціонування комплексів технічного захисту інформації. Імперативи розвитку цивілізації, с. 116.

30. Форощук, І. В. (2010). Загроза витоку інформації в умовах впливу надширокосмугових сигналів. Захист інформації, 12(1) с. 46.

31. Слободян В. Г. Активні та пасивні методи захисту приміщень від витоку інформації віброакустичним каналом / В. Г. Слободян, О. П. Живков // XIX Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Україна, м. Київ, 13–14 травня 2021 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2021. – С. 164–165. – Бібліогр.: 2 назви.

32. Досенко, С. Д. (2021). Технічний захист інформації. Основні проблеми та способи їх вирішення. Вісник ЛТЕУ. Технічні науки, (27), с. 27-32.

33. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року № 1229. https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення – 01.11.2023).

34. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення – 02.11.2023).

35. Лізунов, С. І.,., Кадулін, М. О.(2019). Використання аналізаторів спектра для захисту інформації. Запорізький національний технічний університет. Тиждень науки-2019. Факультет радіоелектроніки та телекомунікацій. Збірник тез доповідей щорічної науково-практичної конференції. 15–19 квітня 2019 року. С. 110-112.

36. Наконечний Т. А., & Євграфов Д. В. (2018). Перехоплення сигналу витоку інформації з екрану монітора. Захист інформації, том 23, №3, липень-вересень 2021. С. 160-167.

37. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-tr-pemvn-95.pdf.

38. Radio Monitoring: Problems, Methods, and Equipment / Anatoly Rembovsky, Alexander Ashikhmin, Vladimir Kozmin, and Sergey Smolskiy – Springer Science+Business Media, LLC 2009. – 507 p.

39. Blintsov V., Nuzhniy S. Improving the method of assessing the level of protection speech information // Eastern-European Journal Of Enterprise Technologies. 2019. 6 (9 (102)).

40. Нужний С. М. Удосконалена технологія оцінки ступеня захисту мовної інформації // Сучасний захист інформації. 2018. №1(33). С. 66–73.

41. Крючкова Л. П., Пліс Ю. А., Овсійчук І. П., Тарасенко Д. О. Методичні аспекти оцінювання технічної захищеності мовленнєвої інформації у виділених приміщеннях // Київ, Зв’язок № 3 2022, с. 12-15.

42. Особливості захисту інформації від витоку по каналу, створеному за рахунок застосування методу високочастотного «нав’язування» / О.П. Провозін, В.К. Железняк, В.А. Хорошко // Сучасні інформаційно-телекомунікаційні технології: Матеріали міжнародної науково-технічної конференції. Том IV. Сучасні технології інформаційної безпеки. – Київ: ДУТ, 17–20 листопада 2015. С.28 – 30.

43. Крючкова Л.П., Провозін О.П. Перехоплення мовленнєвої інформації методами високочастотного «нав’язування»// Сучасний захист інформації – 2017. – №3 (31), С.74-80.

44. В.М. Шокало, В.А. Усін, Д.В. Грецьких, В.О. Хорошко, Л.П. Крючкова. Поля і хвилі в системах технічного захисту інформації: ХНУРЕ ; Колегіум, 2013. – 456 с.

45. Ярутіч А. О. Захист інформації від витоку технічними каналами. Наука онлайн: Міжнародний електронний науковий журнал. 2019. №1.

46. Сергієнко, С. ., Крижановський, В. ., Чернов, Д. ., & Загоруйко, Л. . (2021). Використання нестаціонарних шумових завад для протидії пасивним радіозакладкам. Радіотехніка, 4(207), с. 132–138.

47. Gorbenko I.D., Zamula A. A., Morozov V. L., Rodionov S.V. Mathematical model of orthogonal frequency distribution and multiplexing (OFDM) signals. Радіотехніка. 2019. Вип. 198. С. 32-44.

48. Горбенко, І., Семенко, Є., & Замула, О. (2020). Methods and means of synthesis and generation of signals – physical carriers of data in modern information and communication systems. Radiotekhnika, 3(202), 87–98.

49. Горбенко І.Д., Замула О.А. Дослідження структури спектрів сигналів з лінійною частотною модуляцією. Радіотехніка. 2018. Вип. 193. С.192 -199.

50. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп’ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

51. Лізунов С.І., Кадулін М.О. Використання аналізаторів спектра для захисту інформації. Тиждень науки-2019. Факультет радіоелектроніки та телекомунікацій. Тези доповідей науково-практичної конференції, Запоріжжя, 15–19 квітня 2019 р. Редкол. :В. В. Наумик (відпов. ред.). Запоріжжя: ЗНТУ, 2019. С.110-112.

52. Лізунов С. І., Розумовський К.І. Застосування екрануючих конструкцій для захисту інформації. Тиждень науки-2019. Факультет радіоелектроніки та телекомунікацій. Тези доповідей науково-практичної конференції, Запоріжжя, 15–19 квітня 2019 р. Редкол. :В. В. Наумик (відпов. ред.). Запоріжжя: ЗНТУ, 2019. С.112-115.

53. Gorbenko Ivan, Zamula Alexander, Morozov Vladyslav. Information and communication systems based on signal systems with improved properties building concept. Workshop Proceedings 2019 CEUR.

54. Mykhailo Mozhaiev, Oleksandr Mozhaiev, Yurii Gnusov, Volodymyr Strukov, Petro Klimushin, Dmytro Yevstrat. Analysis of acoustic information protection methods in critical applications. No. 1 (23) (2023): Innovative technologies and scientific solutions for industries. P. 96-107.

55. С. Нужний. Нові підходи до розробки систем запобігання витоку мовної інформації за межі контрольованої зони. Конференція: Інформаційні системи та технології. IST-2021 10-та Міжнародна науково-технічна конференція 13-19 вересня 2021 р. за адресою: Харків – Одеса, Україна. С. 293-299.

56. Єрмошин В.В., Ткаченко В.В. Модель сигналу високочастотного нав’язування. Науково-технічний журнал «Сучасний Захист Інформації». 2010. № 2. С. 68-72.

57. Хома В. В. Методи і засоби технічного захисту інформації на абонентських телефонних лініях. Автоматика, вимірювання та керування. Л.: Вид-во Нац. ун-ту «Львів. Політехніка», 2009. № 639. С. 87-93.

58. Kriuchkova Larysa, Tsmokanych Ivan. (2021) Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions. International Journal of Innovative Technologies in Social Science. 3(31).

59. Volodymyr Blintsov, Sergey Nuzhniy, Yurii Kasianov, Viktor Korytskyi. Mathematical model of the system of active protection against eavesdropping of speech information on the scrambler generator. EUREKA Physics and Engineering 3(3):p. 11-22.

60. Іванченко С. О., Гавриленко О. В., Липський О. А. [та ін.]. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Київ : НТУУ «КПІ», 2016. 104 с.

61. Володимир Блінцов, Сергій Нужний, Юрій Касьянов, Віктор Корицький. Розробка математичної моделі генератора мовних перешкод типу скремблера для системи запобігання витоку мовної інформації по акустичних та вібраційних каналах. Технологічний аудит і виробничі резерви 5(2(49)): с. 19-26.

62. Buye Xu, Tony Miller. Selective active noise cancellation based on directional reference signals. The Journal of the Acoustical Society of America 146(4): p. 2794-2794.

63. Патент 95365 Україна, МПК (2011.01) H04K 3/00. Метод захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; оголошено 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.

64. Патент 103546 Україна, МПК (2013.01) H04K 3/00. Метод захисту інформації / Рибальський О.В., Хорошко В.О., Грищук Р.В.; заявник та патентовласник Грищук Р.В. - № a201202038; оголошено 22.02.2012; опубл. 25.10.2013, Бюл. № 20.

65. Рибальський О.В., Хорошко В.А., Крючкова Л.П. Экспериментальные исследования нового метода защиты от ВЧ-навязывания // Вісник Східноукраїнського національного університету ім. В. Даля №6 (136). Частина 1, 2009. – С. 94 – 96.

66. Сергієнко, В. Д., Попов, А. О., Зібін, С. Д., Бичков, А. М., & Підгородецький, М. М. (2017). Аналіз сучасного стану розвитку багатофункціональних засобів та комплексів радіоелектронної боротьби. Сучасні інформаційні технології у сфері безпеки та оборони, (1), с. 135-143.

67. Заславець, В. П., Долина, М. П., & Чечуй, О. В. (2020). Особливості розрахунку завадозахищеності ліній радіозв’язку в умовах радіоподавлення (радіоелектронного конфлікту). Системи озброєння і військова техніка, (1 (61)), с. 7-12.

68. Сорокін, А. Ю. (2010). Оптимальні параметри розширення спектра радіосигналу на основі швидких стрибків частоти з безперервною фазою. Вісник Чернігівського державного технологічного університету. Серія: Технічні науки, (42), с. 242-246.

69. Кубрак, О. М. (2010). Методика формування радіоперешкод для подавлення широкосмугових ліній радіозв’язку. Вісник ЖДТУ. Серія "Технічні науки", 1(2 (53)).

70. Бугайов, М. В., Нагорнюк, О. А., Клязника, В. В., Рикун, В. Л., & Гаврилюк, О. С. (2021). Реалізація підходів до імітування динамічної радіоелектронної обстановки в широкій смузі частот. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем, (21), с. 4-15.

71. Pevtsov, G. V., Yatsutsenko, A. Y., Karlov, D. V., & Trofimenko, Y. V. (2011). Теоретичні основи енергетичного виявлення-оцінювання параметрів радіолокаційних сигналів. Військово-технічний збірник, (5), с. 50-58.

72. Бондарєв, А. П., & Мандзій, Б. А. (2007). Підвищення завадостійкості приймання сигналу з глибокою кутовою модуляцією. Вісник Вінницького політехнічного інституту, с. 119-123.

73. Якобінчук, О. В. (2009). Методика оцінки завадозахищеності системи зв’язку, радіотехнічного забезпечення та автоматизації управління. Системи озброєння і військова техніка, (1), с. 144-146.

74. Larysa Kriuchkova, Maksym Vovk, Ivan Tsmokanych, and Denys Tarasenko. Parameters of Aiming Interfering Signals for Information Protection from Leaks by High-Frequency Channel Imposition, CEUR Workshop Proceedings CPITS-II-2 2021, pp. 265-272. (**Scopus**)

75. Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни “Обчислювальна техніка в розрахунках електромеханічних систем ” (пакет MathCAD) для студентів напряму 0922 Електромеханіка / Упоряди.: В.А. Бородай, В.Е. Воскобойник. – Дніпропетровськ: Національний гірничий університет, 2003 – 64 с.

76. Kriuchkova, L., Tsmokanych, I., & Vovk, M. (2022). Advanced Method Of Protection Of Confidential Information From Interception By High-Frequency Imposition Methods. Computer Systems and Information Technologies, (3), 14–20.

77. Крючкова Л.П., Цмоканич І.В. Удосконалений метод захисту інформації від витоку каналами високочастотного нав'язування // Збірник тез доповідей XIII Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2021), м. Київ, 15–17 квітня 2021 р., Національний авіаційний університет. – К.: НАУ, 2021. – С. 62 – 63.

78. Статюха, Г. О., Складанний, Д. М., & Бондаренко, О. С. (2011). Вступ до планування оптимального експерименту. Навч. посібн. для студ. спец. 092502 – Комп'ютерно-інтегровані технологічні процеси і виробництва / Уклад.: Г.О. Статюха, Д.М. Складанний, О.С. Бонаренко – К.: ІВЦ «Політехніка», 2011.

79. Ленков С.В., Рибальский О.В., Хорошко В.А., Крючкова Л.П. Принципи блокування зняття інформації методами ВЧ-навязування // Науковий вісник Національного університету ім. Т. Шевченко. – К., № 22, 2009. – С. 36–39.

80. Л.П. Крючкова, І.В. Цмоканич / Удосконалений метод захисту інформації від перехоплення методом високочастотного нав'язування // Науково-практична інтернет-конференція «Цифрова трансформація кібербезпеки». – Державний університет телекомунікацій. Навчально-науковий інститут захисту інформації, 2020. – С. 146 – 149.

81. Крючкова, Л., & Цмоканич, І. (2022). Методичні аспекти визначення параметрів захисних впливів на зондувальні сигнали високочастотного нав'язування. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 197–204.

82. H. V. Lutsenko, "Application of Labview during the processing of experimental data by statistical methods", ITLT, vol. 35, no. 3, pp. 120–134, may 2013.

83. Чесановський, І. І., Іванов, А. В., & Гурман, І. В. (2013). Підвищення завадостійкості обробки сигналів в некогерентних радіолокаційних системах. Вісник Національного технічного університету України Київський політехнічний інститут. Серія: Радіотехніка. Радіоапаратобудування, (54).

84. Ципоренко, В. Г. (2009). Аналіз ширини спектра радіосигналу з невідомим фазовим спектром. Вісник ЖДТУ. Серія" Технічні науки", (1 (48)), 127-130.

85. Кононов, В. Б. (2011). Види та методи оцінювання результатів вимірювання засобами вимірювальної техніки. Системи обробки інформації, (5), с. 45-49.

86. Кононова, В. О., Харкянен, О. В., & Грибков, С. В. (2014). Оцінка засобів захисту інформаційних ресурсів. Вісник Національного університету Львівська політехніка. Комп’ютерні системи та мережі, (806), с. 99-105.

87. Крючкова, Л., & Цмоканич, І. (2023). Удосконалення захисних впливів на небезпечні сигнали високочастотного нав’язування. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 243–253.

88. Л.П. Крючкова, І.В. Цмоканич / Захист інформації від високочастотного нав’язування на об’єктах критичної інфраструктури // IV Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” – Київський національний університет імені Тараса Шевченка. – Київ, 2021. – С. 37 – 38.

89. Крючкова Л.П., Вовк М.О. Метод блокування каналів активних радіозакладних пристроїв // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез IV Міжнародної науково-практичної конференції (PCSITS); м.Київ, 15-16 квітня 2021 року; Київський національний університет імені Тараса Шевченка. – К.: ВПЦ "Київський університет" 2021. – С. 48 – 49.

90. Смирний М. Ф. Основи наукових досліджень; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 111 с.

91. Larysa Kriuchkova, Ivan Tsmokanych, Svitlana Shevhenko, Oleksandr Bohdanov, and Nataliia Mazur. Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, *CEUR Workshop Proceedings CPITS-II-2 2023*, pp. 261-268. (**Scopus**)

92. ГОСТ 30373-95. Сумісність технічних засобів електромагнітна. Устаткування для випробувань. Камери екрановані. Класи, основні параметри, технічні вимоги та методи випробувань.

Додаток А

ЗАТВЕРДЖУЮ

Начальник
Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації

Володимир КОЗАК

"06" 12 2023 р.

АКТ

про впровадження результатів дисертаційної роботи здобувача наукового ступеня доктора філософії (PhD) ЦМОКАНИЧА Івана Володимировича на тему «Методи та алгоритми захисту інформації від високочастотного нав'язування»

Комісія у складі:

голови комісії – начальника 2 науково-дослідного центру ДержНДІ технологій кібербезпеки Лисенка Сергія Станіславовича,

членів комісії – заступника начальника 2 науково-дослідного центру ДержНДІ технологій кібербезпеки Страха Сергія Миколайовича, начальника 1 науково-дослідного відділу 2 науково-дослідного центру ДержНДІ технологій кібербезпеки Скиби Віктора Миколайовича, провідного наукового співробітника 1 науково-дослідного відділу 2 науково-дослідного центру ДержНДІ технологій кібербезпеки, кандидата технічних наук Голішевського Анатолія Васильовича встановила, що І.В. Цмоканичем отримані наукові результати, а саме:

- запропоновано метод захисту інформації від витоку каналами високочастотного нав'язування шляхом руйнування інформативних параметрів небезпечних сигналів високочастотного нав'язування окрім основної частоти також на комбінаційних гармоніках зондуючого сигналу;
- запропоновані імітаційні моделі та методика для визначення параметрів захисних сигналів;
- розроблені програма, методика і схеми експериментальних досліджень для визначення параметрів захисних сигналів. Вищезгадані програма, методика і схеми експериментальних досліджень були використані для прийняття обґрунтованих технічних рішень щодо удосконалення існуючих методик спеціальних досліджень для оцінки захищеності інформації від витоку каналами високочастотного нав'язування на об'єктах інформаційної діяльності.

Запропоновані автором наукові результати дозволяють підвищити рівень захищеності інформації на об'єктах інформаційної діяльності від її перехоплення методами високочастотного нав'язування та в подальшому можуть використовуватись для вирішення комплексних проблем щодо захисту інформації на об'єктах інформаційної діяльності.

Запропоновані імітаційні моделі та створена на їх основі методика може стати основою для визначення параметрів захисних сигналів на об'єктах інформаційної діяльності та виконання імітаційних досліджень конфліктної взаємодії електромагнітних сигналів.

Запропоновані програма, методика і схеми експериментальних досліджень можуть застосовуватись для визначення параметрів захисних сигналів, спрямованих на руйнування інформативних параметрів небезпечних сигналів лазерних систем акустичної розвідки або ПЕМВН.

Економічний ефект від впровадження не розраховувався у зв'язку з науковим призначенням результатів.

Акт складено для представлення у разову спеціалізовану вчену раду і не є підставою для фінансових зобов'язань.

Голова комісії: Сергій ЛИСЕНКО

Члени комісії: Сергій СТРАХ

Віктор СКИБА

Анатолій ГОЛІШЕВСЬКИЙ

"05" 12 2023 р.

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка
кандидат фізико-математичних наук, старший науковий співробітник
_____ **Оксана ЛИТВИН**
«11» 12 2023 р.

А К Т
про впровадження результатів наукових досліджень
Цмоканича Івана Володимировича
в освітній процес
кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики
Київського університету імені Бориса Грінченка

Комісія у складі:

Голова комісії:	завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, кандидат технічних наук, доцент ***Павло СКЛАДАННИЙ***;
члени комісії:	професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, доктор технічних наук, професор ***Геннадій ГУЛАК***;
	професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, доктор технічних наук, професор ***Наталія КОРШУН.***

Комісія встановила, що результати наукових досліджень *Цмоканича Івана Володимировича* на тему: «Методи та алгоритми захисту інформації від високочастотного нав'язування» за спеціальністю 125 – Кібербезпека та захист інформації, є актуальними для впровадження в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Отримані наукові результати, а саме:

- метод захисту інформації від витоку каналами високочастотного нав'язування шляхом руйнування інформативних параметрів небезпечних сигналів високочастотного нав'язування окрім основної частоти також на комбінаційних гармоніках зондуючого сигналу;
- імітаційна модель та методика для визначення параметрів захисних сигналів;
- розроблена програма, методика і схеми експериментальних досліджень для визначення параметрів захисних сигналів.

Зазначені наукові розробки були впроваджені в освітній процес Університету в робочих програмах навчальних дисциплін «Компонентна база та елементи схемотехніки в системах захисту інформації», «Теорія кіл і сигналів в інформаційному та кіберпросторах», «Системи технічного захисту інформації» та «Комплексні системи захисту інформації: проектування, впровадження, супровід» першого (бакалаврського) рівня освіти, вони також були ефективно використані і впроваджені у програмне апаратне забезпечення «Центру дослідження технології захисту інформаційних активів» при розгортанні Лабораторії систем криптографічного та технічного захисту інформації (навчальний кіберполігон).

Даний акт не є підставою для фінансових взаєморозрахунків.

Голова комісії _____ Павло СКЛАДАННИЙ

Члени комісії: _____ Геннадій ГУЛАК

_____ Наталія КОРШУН

Документ підписано у сервісі Вчасно (початок)
ЦМОКАНИЧ_І_В_ДИСЕРТАЦІЯ_28_12_фінальна.pdf

Документ підписано у сервісі Вчасно (продовження)
ЦМОКАНИЧ_І_В_ДИСЕРТАЦІЯ_28_12_фінальна.pdf

Документ відправлено: 10:35 28.12.2023

Власник документу

Електронний підпис
10:35 28.12.2023
Ідентифікаційний код: 3525009750
ЦМОКАНИЧ ІВАН ВОЛОДИМИРОВИЧ
Власник ключа: ЦМОКАНИЧ ІВАН ВОЛОДИМИРОВИЧ
Час перевірки КЕП/ЕЦП: 10:35 28.12.2023
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 5E984D526F82F38F040000007BF539016F01AB04
Тип підпису: удосконалений