МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЕЛЕКТРИЧНИМИ КАНАЛАМИ**

Студент групи СЗЗ-51 Аношко Володимир Русланович _____
(підпис)

Науковий керівник: д.т.н., проф., Ахрамович Володимир Миколайович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Аношко Володимиру Руслановичу

1.Тема роботи: Захист інформації від витоку електричними каналами, затверджено наказом від « 24» лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту передачі та прийому інформації по електричним каналам.

4. Предметом дослідження: технології захисту, які забезпечують безпеку передачі інформації, прийому та обробки інформації в інформаційних системах через електричні канали.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту інформації через електричні канали.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій захисту інформації через електричні канали;
- аналіз та дослідження існуючих методів захисту інформації через електричні канали;
- створення рекомендацій щодо застосування технологій захисту інформації через електричні канали.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Ахрамович В.М.

(підпис)

Завдання прийняв до виконання _____Аношко В.Р.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «____» _____2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 20.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗЗ -51 Аношко В.Р. _____

(підпис)

Науковий керівник: д.т.н., проф. Ахрамович В.М. _____

(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____

(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 51 сторінку, 36 рисунків, 1 таблицю.

Інформація відіграє величезну роль у життєдіяльності кожної особи, підприємства, держави, які є суб'єктами інформаційного поля. У зв'язку зі стрімким розвитком інформаційних технологій відбувається неймовірний стрибок зростання конкурентної боротьби компаній за вихід на лідируючі позиції, внаслідок чого виникає загроза витоку значущої для підприємств та установ інформації.

Одним з основних інструментів забезпечення розвідувальних заходів є отримання доступу до каналів передачі інформації, якими користуються опоненти. Серед усього різноманіття способів несанкціонованого перехоплення інформації є прослуховування телефонних переговорів за допомогою електричних каналів.

Об’єктом дослідження є процеси захисту передачі та прийому інформації по електричним каналам.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі інформації, прийому та обробки інформації в інформаційних системах через електричні канали.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації через електричні канали.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій захисту інформації через електричні канали;

- аналіз та дослідження існуючих методів захисту інформації через електричні канали;
- створення рекомендацій щодо застосування технологій захисту інформації через електричні канали.

ABSTRACT

The thesis contains 51 pages, 36 figures, and 1 tables.

Information plays a huge role in the life of every person, enterprise, and state that are subjects of the information field. Due to the rapid development of information technology, there is an incredible jump in the growth of competition between companies to take leading positions, which leads to the threat of leakage of information important to enterprises and institutions.

One of the main tools for ensuring intelligence activities is gaining access to information transmission channels used by opponents. Among all the various ways of unauthorized interception of information is listening to telephone conversations through electrical channels.

Object of research: processes for protecting the transmission and reception of information through electrical channels.

The subject is security technologies that ensure the security of information transmission, reception and processing of information in information systems through electrical channels.

The purpose of the work is improvements and recommendations on the use of methods for protecting information through electrical channels.

To achieve this goal, the following main tasks are performed:

• analysis of implemented technologies for protecting information through electrical channels;

• analysis and research of existing methods of protecting information through electrical channels;

• creating recommendations for the use of information security technologies through electrical channels.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОІД	Об`єкт інформаційної діяльності	Object of information activity
ТКВІ	Технічні канали витоку інформації	Technical channels of information leakage
ПЕМВ	Побічне електромагнітне випромінювання	Indirect electromagnetic radiation
EEPROM	Постійний запам’ятовувач що програмується та очищується за допомогою електрики	Electrically Erasable Programmable Read-Only Memory
NIST	Національний інститут стандартизації та технологій	The National Institute of Standards and Technology
PKI	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	

ІТС	Інформаційно-телекомунікаційна система
ОЗП	Оперативний запам’ятовувальний пристрій
УВЧ	Ультра високі частоти

ВСТУП

Наявність спеціального (відокремленого) приміщення для обробки, зберігання та передачі конфіденційної та таємної інформації, таких як кімнати перемовин, на теперішній час є нормою не тільки у великих корпораціях, а й в організаціях середнього рівня. Для виявлення технічних каналів витоку інформації проводиться спеціальне дослідження, а перед ним будується модель загроз.

Актуальність теми полягає в тому, що спеціальна кімната для переговорів є одним з головних місць наради з конфіденційних питань співробітників не тільки у великих корпораціях, а й у середніх підприємствах через істотне зниження вартості обладнання, яке дає змогу вести несанкціоноване знімання конфіденційної інформації. Спеціальне дослідження, яке проводиться в обов'язковому порядку для таких приміщень, дає спроможність виявити вразливі точки, які можуть призвести до витоку інформації. Після проведення спеціального дослідження та отримання його підсумків формуються пропозиції щодо встановлення або модернізації вже наявної системи захисту інформації.

Спеціальне дослідження є складним комплексом заходів, які передбачають виявлення за допомогою контрольно-вимірювального обладнання можливих технічних каналів витоку інформації, що захищається, від основних і допоміжних технічних засобів та оцінку відповідності рівня захисту інформації вимогам нормативних документів.

Одним з основних технічними каналами витоку інформації протягом обробки конфіденційної та таємної інформації є електричні канали.

Реалізація загрози витоку акустичної інформації через електричні канали полягає в спроможності за наявності функції голосового введення або виведення акустичними засобами мікрофонів, які мають електричне живлення, а також за рахунок спілкування між співробітниками компанії, які є носіями конфіденційної та таємної інформації на об`єкті інформаційної діяльності, який захищається. Несанкціонований виток акустичної інформації може відбуватись через електричні канали, що в свою чергу створює велику загрозу для її знімання. Тому проблема захисту конфіденційної інформації є актуальною сьогодення.

Об'єкт дослідження: процеси захисту передачі та прийому інформації по електричним каналам.

Предмет дослідження є технології захисту, які забезпечують безпеку передачі інформації, прийому та обробки інформації в інформаційних системах через електричні канали.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації через електричні канали.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій захисту інформації через електричні канали;
- аналіз та дослідження існуючих методів захисту інформації через електричні канали;
- створення рекомендацій щодо застосування технологій захисту інформації через електричні канали.

РОЗДІЛ 1 АНАЛІЗ РЕАЛІЗОВАНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ ЧЕРЕЗ ЕЛЕКТРИЧНІ КАНАЛИ

1.1. Захист витоку інформації по телефонним каналам зв`язку

При розгляданні можливості перехоплення інформації з використанням ліній зв'язку, необхідно враховувати те, що перехоплення може здійснюватися не тільки з телефонних ліній і не тільки мовленнєвою інформацією. Можливі загрози витоку телефонним каналом представлено на рисунку 1.1.

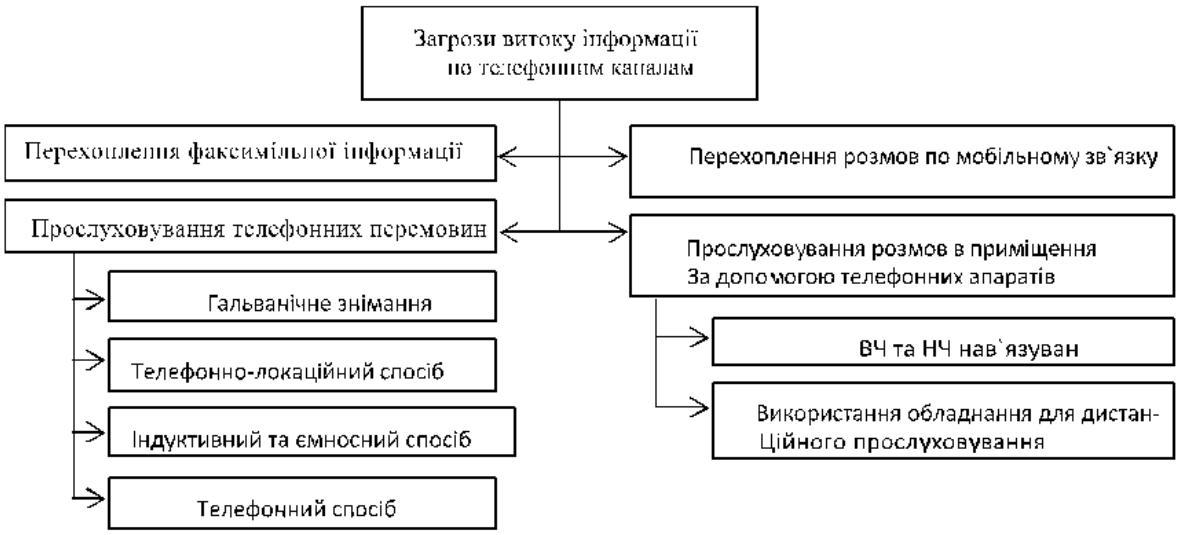

Рисунок 1.1. Можливі загрози витоку інформації через електричні канали

З аналізу загроз витоку інформації, наведених у схемі, видно, що засоби перехоплення реалізують різні фізичні принципи і у своєму складі використовують сучасні технічні рішення.

Формально ступінь небезпеки загроз відображає ймовірності їхньої реалізації за деякий умовний час. Сукупну небезпеку характеризує спектр загроз, що являє собою їх перерахування в порядку зменшення ступеня небезпеки [4].

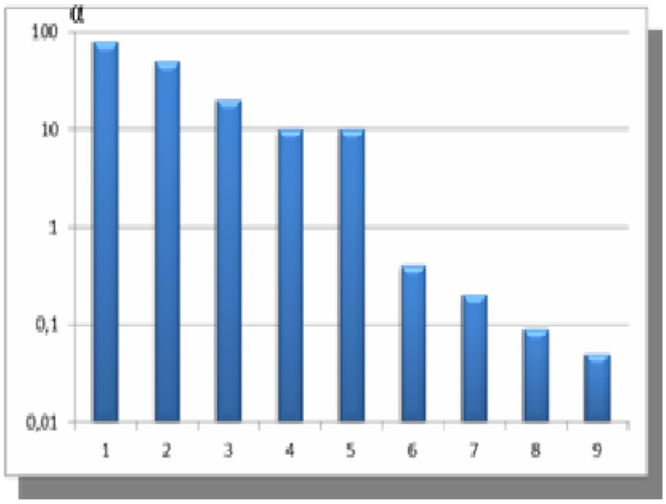

Рис. 1.2. Графік використання методів знімання інформації з телефонної лінії

Позначення: 1 - контактне підключення; 2 - застосування телефонного засобу негласного отримання інформації; 3 - індукційне підключення до лінії; 4 - професійне підключення до лінії; 5 - ємнісне підключення до лінії; 6 - перехоплення мобільного телефону в стандарті *AMPS*; 7 - перехоплення мобільного телефону в стандарті *NMT*; 8 - перехоплення мобільного телефону в стандарті *GSM*; 9 - перехоплення супутникового телефонного зв'язку (у ближній зоні); α - коефіцієнт.

З аналізу наведеного спектру загроз можна зробити висновок, що найбільшу небезпеку загрози витоку інформації телефонною лінією становить просте контактне підключення пристроїв негласного отримання інформації. Що стосується перехоплення стільникових переговорів у стандарті *GSM*, то цей вид загрози є менш можливий. Найменшу ймовірність загрози має перехоплення супутникового зв'язку в зоні околу.

Методи протидії загрозам витоку інформації телефонним каналом зв'язку можна умовно розділити на дві групи: організаційні та технічні. Організаційні методи охоплюють комплекс заходів, спрямованих на регламентацію і контроль за використанням телефонних апаратів. Застосування технічних потребують від фахівців досить глибинних знань у технічній сфері та обов'язкової наявності спеціальної апаратури, яка реалізує той чи інший методи технічного захисту.

Сучасний ринок технічних засобів захисту надає досить широкий набір рішень щодо захисту телефонної лінії від прослуховування. Їх можна розділити на два класи. До першого класу належать засоби, які безпосередньо захищають інформацію, що передається каналом зв'язку, а до другого - технічні рішення, що застосовуються для аналізу станів телефонної лінії та локалізації пристроїв негласного отримання інформації, при умові, що вони виявлені та нейтралізовані.

З першого класу можна виокремити такі рішення, як: *Sec – Stealth* - засіб, що дає змогу аналізувати стан телефонної лінії та захищати телефонні переговори; *ПРОКРУСТ* – 2000 - призначений для захисту телефонних переговорів методом постановки активної перешкоди від прослуховування на ділянці від приладу до *АТС*; *РЕФЕРЕНТ BASIC* - передавання інформації здійснюється у цифровому вигляді з застосуванням спеціальних алгоритмів стиснення та захисту і призначений для проведення оперативних заходів з виявлення та локалізації технічних засобів негласного отримання інформації; *OSCOR* – 5000 - призначений для контролю різних каналів витоку інформації і здатний здійснювати пошук і локалізацію широкого спектра засобів несанкціонованого знімання інформації.

При здійснені практичних робіт було проведено класифікацію основних загроз витоку інформації із ОІД, що захищається, телефонною лінією, ранжування способів витоку інформації з телефонного апарата на основі економіко-статистичних даних, в результаті було зроблено висновок, що серед множини способів найчастіше застосовується простий гальванічний метод

прослуховування телефонних розмов. А також було представлено засоби та методи захисту телефонного апарата від існуючих загроз.

1.2. Удосконалена система оцінки захищеності ОІД від технічних каналів витоку інформації

В даному розділі розглянуто підхід для пониження часових і фінансових витрат підприємства та організації, що проводить спеціальне дослідження на ОІД для оцінювання захищеності приміщення від електричного каналів витоку інформації.

Для оцінки захищеності ОІД від витоку по електричному каналу необхідно створити модель загроз і на основі неї вибирається найбільш небезпечний спосіб захисту. В продовження цьому спеціальне дослідження виділеного приміщення за обраним способом аналізується на виході з нього, отримане співвідношення *Сигнал* / *Шум* в визначених контрольних точках та певну іншу інформацію. Ці дані заносяться в спеціальне програмне забезпечення, яка не тільки здійснює розрахунок захищеності приміщення, а й дає практичні рекомендації щодо усунення виявлених недоліків.

1.2.1. Створення моделі загроз та вибір електричного каналу витоку інформації

Згідно результатів створення моделі загроз, експертна група заповнює спеціальну таблицю. В даній таблиці вказано технічний канал загрози витоку інформації і відповідно визначається параметр, який характеризує цей канал і приписує йому значення ризику. В основі моделі загроз лежить базова модель загроз безпеці персональних даних, протягом часу обробки їх в інформаційній системі. Як основні канали витоку розглядається електричний, побічне електромагнітне випромінювання, акустичний та оптичний. В таблиці 1.1. представлено види загроз.

Таблиця 1.1. Загальна модель загроз

ЗАГРОЗА	*АКТУАЛЬНІСТЬ ЗАГРОХЗИ*	*КОЕФІЦІЄНТ РЕАЛІЗАЦІЇ ЗАГРОЗИ*
Загрози витоку по акустичному та віброакустичному каналу		
Перехоплення за допомогою засобів, які реєструють акустичні хвилі	*Неактуальна / актуальна*	[0;1]
Перехоплення за допомогою засобів, які реєструють віброакустичні хвилі	*Неактуальна / актуальна*	[0;1]
Перехоплення за допомогою засобів, які реєструють електромагнітне випромінювання та електричні сигнали	*Неактуальна / актуальна*	[0;1]
Перехоплення за допомогою спеціальних електронних засобів зняття мовної інформації	*Неактуальна / актуальна*	[0;1]
Перехоплення за допомогою спеціальних електронних засобів зняття мовної інформації, які підключені до каналів зв`язку	*Неактуальна / актуальна*	[0;1]
Загрози витоку по оптичному каналу		
Перехоплення за допомогою перегляду оптичними засобами з застосуванням обчислювальної техніки	*Неактуальна / актуальна*	[0;1]
Перегляд ОІД за допомогою спеціальних електронних засобів зняття, які вставлені в службові приміщення	*Неактуальна / актуальна*	[0;1]
Перегляд ОІД за допомогою спеціальних електронних засобів зняття , які таємно використовують особи, які відвідують ОІД	*Неактуальна / актуальна*	[0;1]
Загрози витоку за рахунок побічного електромагнітного випромінювання		
За рахунок побічного електромагнітного випромінювання електронно-обчислювальної техніки	*Неактуальна / актуальна*	[0;1]
За рахунок наведення до мереж живлення	*Неактуальна / актуальна*	[0;1]
За рахунок радіовипромінювання, які модулюються інформативним сигналом	*Неактуальна / актуальна*	[0;1]
За допомогою засобів зняття наведених інформативних сигналів від мереж електроживлення	*Неактуальна / актуальна*	[0;1]

Будь-яка загроза може мати статус неактуальна, або актуальна. Критерієм актуальності загрози є спроможність реалізації такої загрози в конкретному

акустичному засобі, а також її небезпека для конфіденційних та таємних даних. В якості параметру успішної реалізації загроз визначається коефіцієнт реалізації загрози, який визначається експертним шляхом і який характеризує ймовірність реалізації конкретної загрози безпеці конфіденційним та таємним даним в поточний момент часу. Коефіцієнт реалізації кожної загрози експерт ставить у відповідність деяке числове значення в числовому відрізку від 0 до 1. Параметр отримує значення 0, в тому випадку, коли експерт вважає реалізацію цієї загрози неможливою, а значення 1 параметр отримує, якщо експерт вважає, що реалізація цієї загрози є достовірною. У випадку, коли загроза не актуальна, то її не розглядають, і для неї відсутній коефіцієнт реалізації загрози.

Актуальність чи неактуальність загрози, які визначаються коефіцієнтом загрози, вводиться експертом у діалоговому режимі за допомогою розробленого програмного засобу, написаного на мові програмування $C++$. На рисунку 1.3 представлено фото діалогового вікна "Заповнення коефіцієнта загрози".

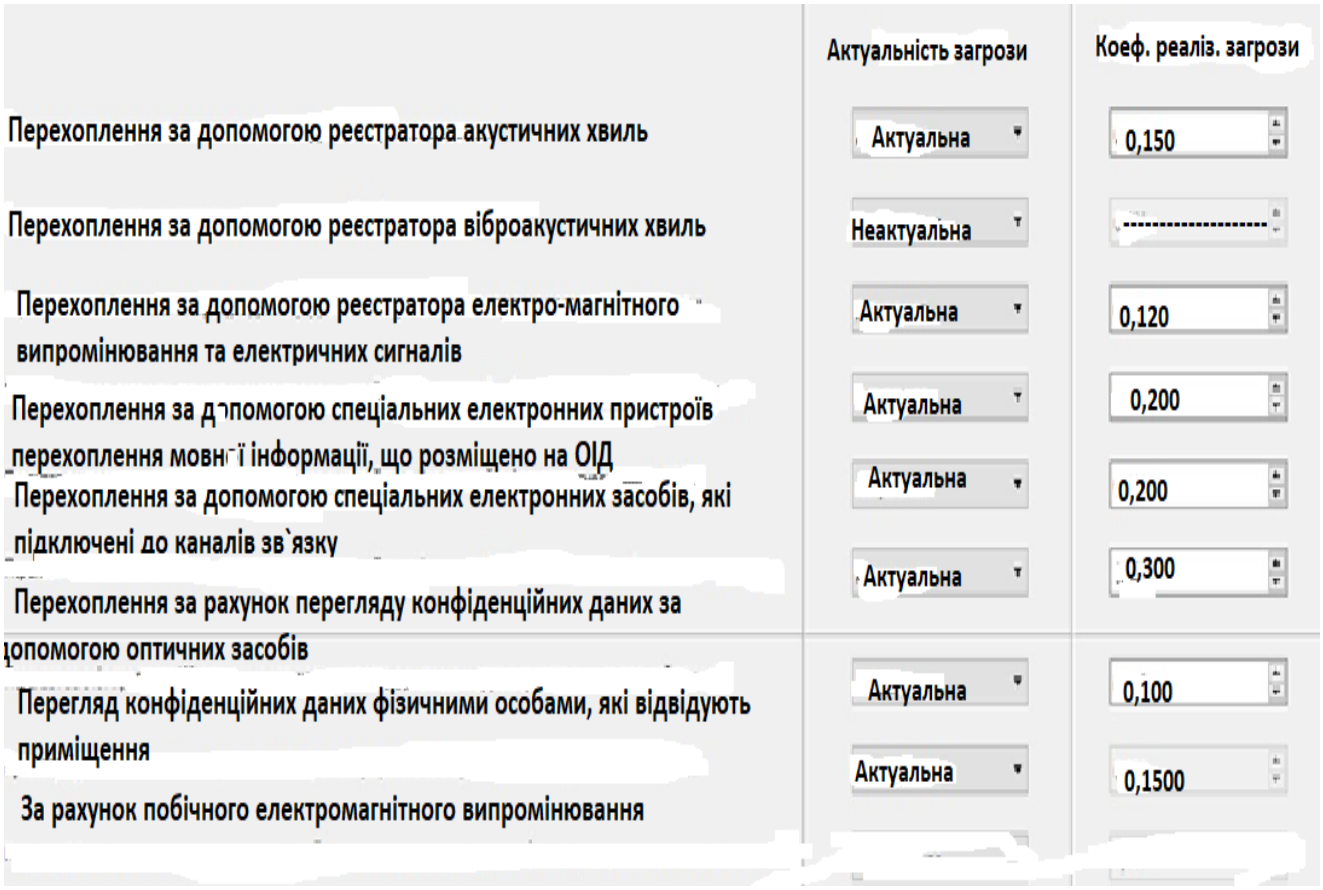

Рисунок 1.3. Діалогове вікно «Заповнення коефіцієнта загрози».

Для підвищення ступеня об'єктивності спеціального дослідження пропонується для визначення коефіцієнта загроз залучати більше двох експертів, кожен з яких незалежно один від заповнює коефіцієнт загроз, за рахунок свого досвіду. Після заповнення в діалоговому вікні, кожен експерт за допомогою математичного методу зважених експертних оцінок Сааті, що дає змогу визначити найкращу альтернативу з можливих, складає узагальнену модель загроз. Використання методу Сааті починається з побудови ієрархічної структури задачі, що розглядається. Вона, в загальному випадку, повинна складатися з трьох рівнів - мета, критерії та альтернативи. На вибір альтернативи безпосередньо впливає відносна вага кожного критерію, що визначається на етапі створення моделі [1].

Наступним кроком дослідження є побудова ієрархічної структури сформульованої задачі. При цьому за мету ставиться виявлення найнебезпечнішого каналу витоку інформації при аналізі кожного експерта, щодо загрози, які представлені на рисунку 1.3. Згідно даних експерта визначаються критерії, а саме значення коефіцієнта реалізації загроз, яке експерт задає, є вагою Сааті. Альтернативами будуть технічні канали витоку інформації, тобто – акустичний та віброакустичний, оптичний та побічне електромагнітне випромінювання. В результаті, всі критерії поділено на три групи відповідності технічним каналам витоку інформації, а сама ієрархія сформульованої задачі має представлення, яке зображено на рисунку 1.4. Важливо відмітити, що реалізовано програмно нормування коефіцієнтів реалізації загроз, тобто, сума всіх ваг критеріїв дорівнює 1, що є необхідною умовою Сааті. Найнебезпечнішим ТКВІ розглядається канал, який отримав максимальне значення ваги, обчислення якої здійснюється шляхом додавання відносних ваг груп загроз певного ТКВІ. У програмному забезпеченні передбачена можливість використання кількох експертів - у цьому разі відбувається підрахунок "голосів" за найнебезпечніший ТКВІ. Отже, програмно здійснюється не тільки розрахунок коефіцієнтів реалізації загроз, а й виявлення найнебезпечнішого ТКВІ.

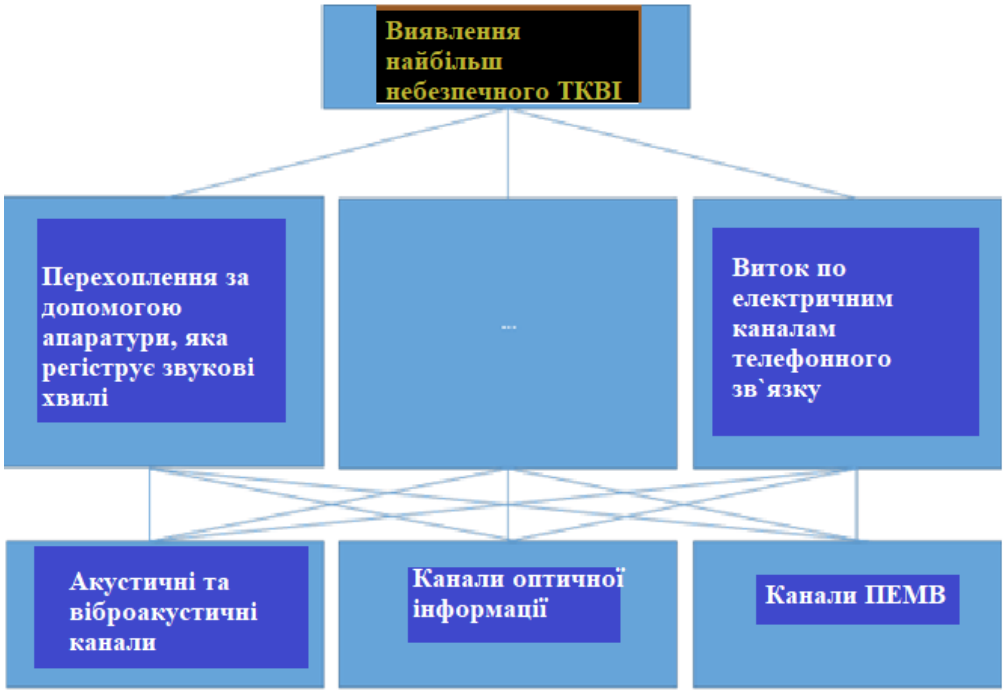

Рисунок 1.4. Ієрархія визначення найнебезпечнішого ТКВІ.

1.2.2. Оцінка захищеності об`єктів інформаційної діяльності

При побудові алгоритмів оцінювання захищеності приміщення від акустичного та вібраційних акустичних каналів витоку інформації за рахунок електричного каналу, було проаналізовано методики розрахунку значень показника захищеності інформації, викладені в роботах С. В. Дворянкіна, В. К. Железняка і Г. А. Бузова [2-5] , які базуються на основі методу Н. Б. Покровського, для визначення показника розбірливості мовленнєвої інформації, а також методика, наведена в навчальному посібнику [6] оцінки захищеності конфіденційної інформації від витоку технічними каналами для визначення захищеності приміщення від витоку мовленнєвої інформації за акустичним та вібраційним каналом.

Удосконалення процесу оцінювання захищеності приміщення від ТКВІ здійснюється за допомогою розробленого програмного засобу, написаного на мові програмування $C++$.

На рисунку 1.5 представлено фото головного меню програми. Даний програмний продукт допомагає фахівцю з технічного захисту інформації в побудові моделі загроз і у визначенні захищеності виділеного приміщення від ТКВІ.

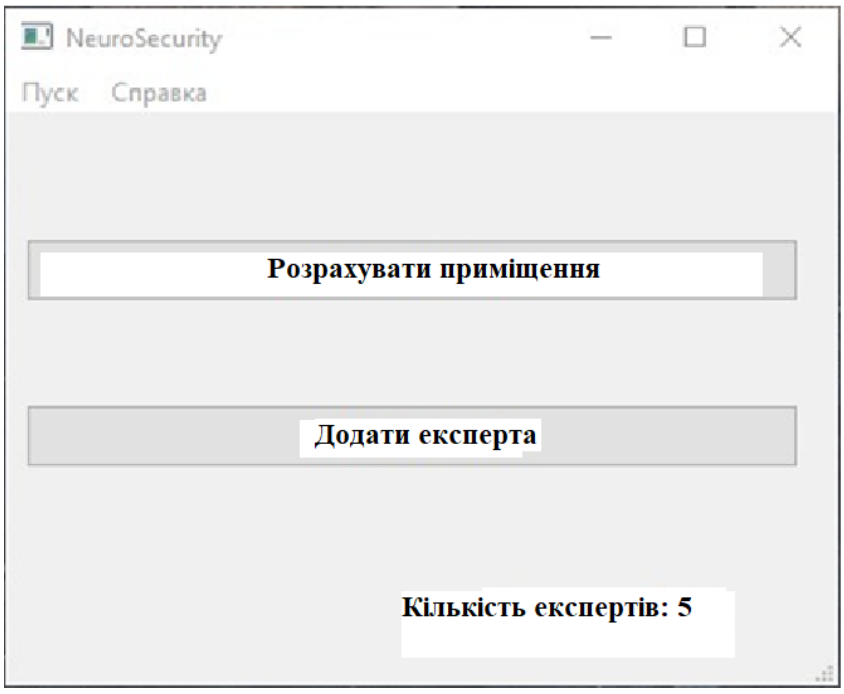

Рисунок 1.5. Фото головного меню

Після того, як експерти вносять свої данні, програма робить розрахунок приміщення для виявлення найнебезпечнішого каналу витоку інформації. Результат представлено на рисунку 1.6.

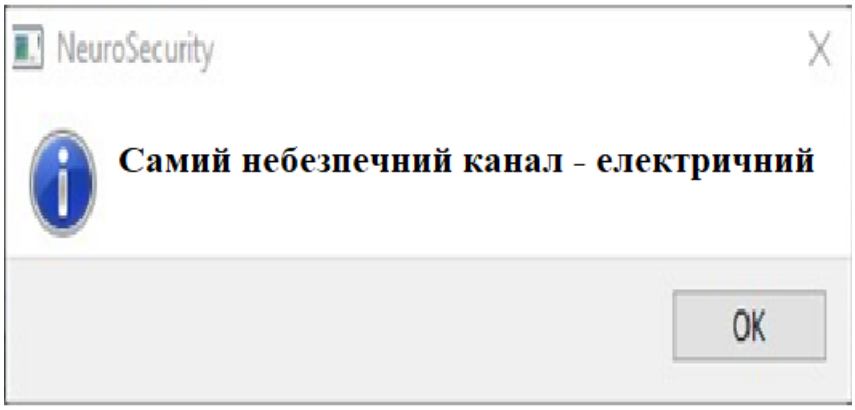

Рисунок 1.6. Результат визначення найнебезпечнішого каналу витоку інформації.

На основі аналізу отриманих результатів здатна видавати практичні поради щодо поліпшення показників захищеності ОІД.

Алгоритм роботи фахівця, який натисне кнопку "Розрахувати приміщення" має наступні кроки:

Крок 1. Маючи результат відповіді, експерт проводить відповідне спеціальне дослідження. Дослідження проводиться за допомогою спеціалізованого обладнання, наприклад, для електричного каналу витоку інформації застосовуються мережевий фільтр. Після проведення дослідження експерт отримує результати вимірювання в кожній контрольній точці - вимірювання тестового сигналу, шуму, співвідношення сигнал/шум, а також коефіцієнти гасіння та спектральний рівень шуму;

Крок 2. За результатами проведених спеціальних дослідження, які отримані на кроці 1, експерт вносить інформацію в «Розрахувати приміщення». До бази знань занесено основні об'єкти та будматеріали, які найчастіше піддаються дослідженню, - починаючи від різних дверей та вікон і закінчуються цегляною кладкою певної товщини.

Крок 3. Здійснюючи аналіз сукупних отриманих результатів проведення спеціального дослідження, введених на кроці 2, програмне забезпечення розраховує захищеність виділеного приміщення від конкретного технічного каналу витоку інформації.

Крок 4. Після проведення обчислень на кроці 3 програмне забезпечення виводить експерту результати у вікні. У лівій частині вікна експерт може або вибрати повний звіт за всіма контрольними точками, або вивчити кожну контрольну точку окремо.

1.3. Електричний канал витоку інформації

Електричний канал перехоплення інформації, що передається дротовими лініями зв'язку, дає можливість здійснювати контактне підключення апаратури перехоплення до дротових ліній зв'язку. Найпростіший спосіб - це безпосереднє паралельне підключення до лінії зв'язку. Але таке підключення легко виявляється, так як в цьому випадку відбувається зміна характеристик лінії

зв'язку за рахунок падіння напруги. Тому засоби перехоплення підключаються до лінії зв'язку або через узгоджувальний пристрій, що не суттєво знижує падіння напруги, або через спеціальний пристрій компенсації падіння напруги. Контактний спосіб використовується в основному для зняття інформації з коаксіальних і низькочастотних дротів зв'язку. Для дротів, в осьовому перерізі яких підвищений тиск повітря відмінний від нуля, застосовують пристрої, які запобігають зниженню цього тиску, що призводить запобіганню спрацювати певної сигналізації.

Електричний канал найчастіше використовується для перехоплення телефонних розмов. Пристрої, що підключаються до телефонних ліній зв'язку (рисунок 1.7) і поєднані з пристроями передачі інформації по радіоканалу, в багатьох випадках називають телефонними закладками.

Рисунок 1.7. Схема підключення до телефонної лінії зв`язку.

Спосіб, який має широке використання для контролю дротових ліній зв'язку і який не вимагає контактного підключення є індукційний. Індукційний канал створює навколо кабелю зв'язку електромагнітне поле (рисунок 1.8) під час проходження по ньому інформативних електричних сигналів, які перехоплюються спеціальними індукційними датчиками. Індукційні датчики використовуються як правило для знімання інформації із симетричних високочастотних кабелів.

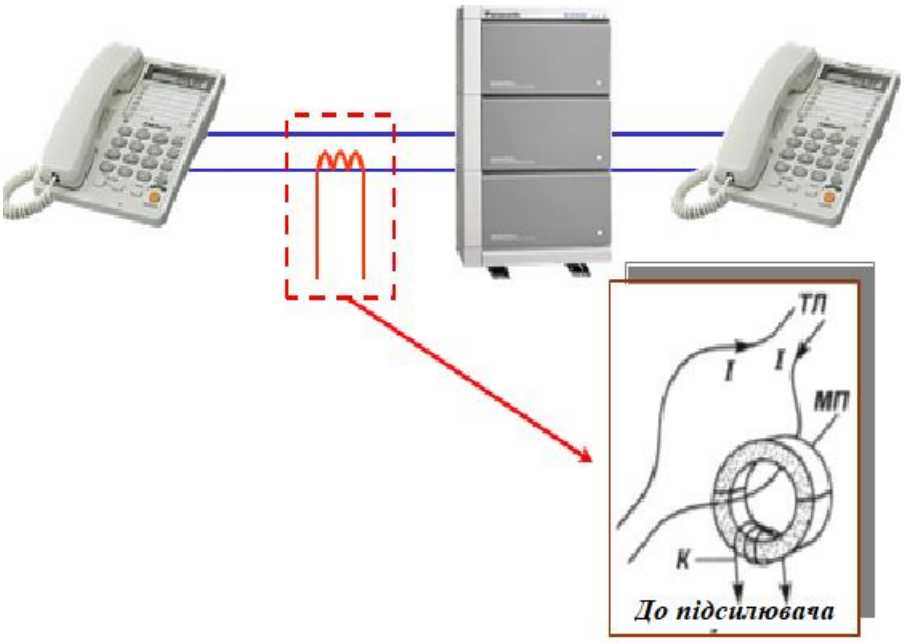

Рисунок 1.8. Індуктивний канал для контролю дротових ліній зв`язку.

Сучасні індукційні датчики спроможні реєструвати інформацію з кабелів, які не тільки ізольовані від струмів, а й подвійною бронею зі сталевої стрічки і сталевого дроту, що щільно обмотує дріт.

Для безконтактного знімання інформації з незахищених телефонних ліній зв'язку можуть використовуватися спеціальні високочутливі низькочастотні підсилювачі, які обладнані магнітними антенами. Деякі засоби безконтактного знімання інформації можуть поєднуватися з радіопередавачами для передачі її на контрольний пункт перехоплення.

Висновок до розділу 1.

1. Реалізація загрози витоку інформації через електричні канали можлива за наявності підключення спеціальних засобів до лінії зв`язку, а також безконтактно при наявності індуктивних каналів у приміщенні, що захищається.
2. Збільшення кількості контрольних точок неминуче веде до різкого зростання часових витрат на проведення спеціального дослідження.

3. Важливим є наявність спеціальних датчиків, які реєструють наявність впливу побічного електромагнітного випромінювання, за рахунок якого через індуктивні канали відбувається несанкціоноване знімання інформації через електричні канали.
4. Для безконтактного зняття інформації з незахищених телефонних ліній зв'язку можуть використовуватися спеціальні низькочастотні підсилювачі, які забезпечені магнітними антенами.
5. Деякі засоби безконтактного зняття інформації, що передається каналами зв'язку, можуть бути компенсовані радіопередавачами для ретрансляції в центр обробки інформації..
6. Завжди існує потенційна загроза виникнення електричного каналу витоку інформації. І ця проблема має вирішуватися як за рахунок удосконалення застосовуваного обладнання, так і застосування засобів активного захисту.

РОЗДІЛ 2. ОБЛАДНАННЯ, ЗАБЕЗПЕЧУЮЧЕ ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВОНАГО ДОСТУПУ ЧЕРЕЗ ЕЛЕКТРИЧНІ КАНАЛИ

2.1. Принцип роботи мережевого фільтру на 220 В

Мережевий фільтр в багатьох випадках застосовується для приєднання до електричної мережі комп`ютера, периферійних та інших пристроїв, які живляться від мережі в 220 В. За допомогою пристрою, який має функцію фільтра, забезпечується неспроможність проникнення завад, метою яких є порушення функціонування обладнання, що в свою чергу може призвести до несанкціонованого доступу до конфіденційної інформації, її підміни, або блокуванню доступу до конфіденційної та таємної інформації. На рисунку 1.1 представлено зовнішній вид найпростішого мережевого фільтру.

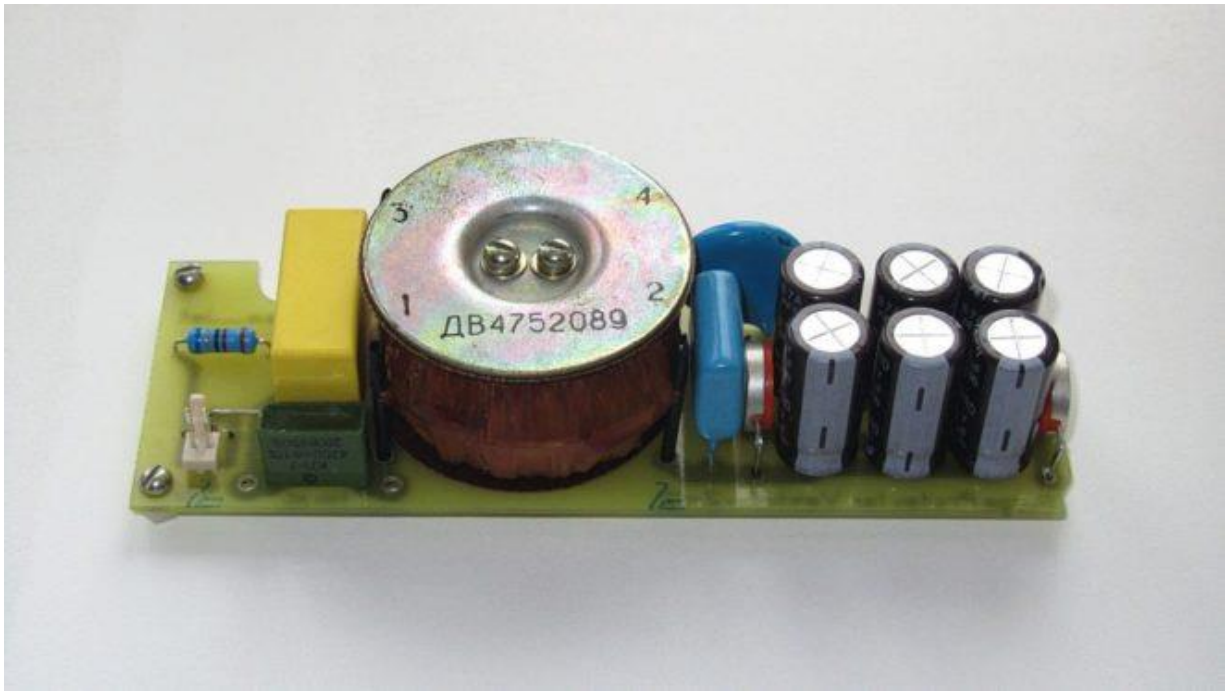

Рисунок 2.1. Зовнішній вигляд найпростішого мережевого фільтру.

Мережева напруга в 220 В є змінною та ця зміна відбувається за законом синуса, за винятком того, що форма синусоїди уявляє собою не в гладку криву, а криву, навколо якої постійно присутні завади, які мають електромагнітні властивості. В самому найкращому вигляді синусоїда описує хвильові лінії, але

на практиці значення напруги постійно здійснюють сплески, перекоси фаз, та інші джерела її флуктуацій. На рисунку 1.2 представлено структурну схему мережевого фільтру з урахуванням існуючих завад.

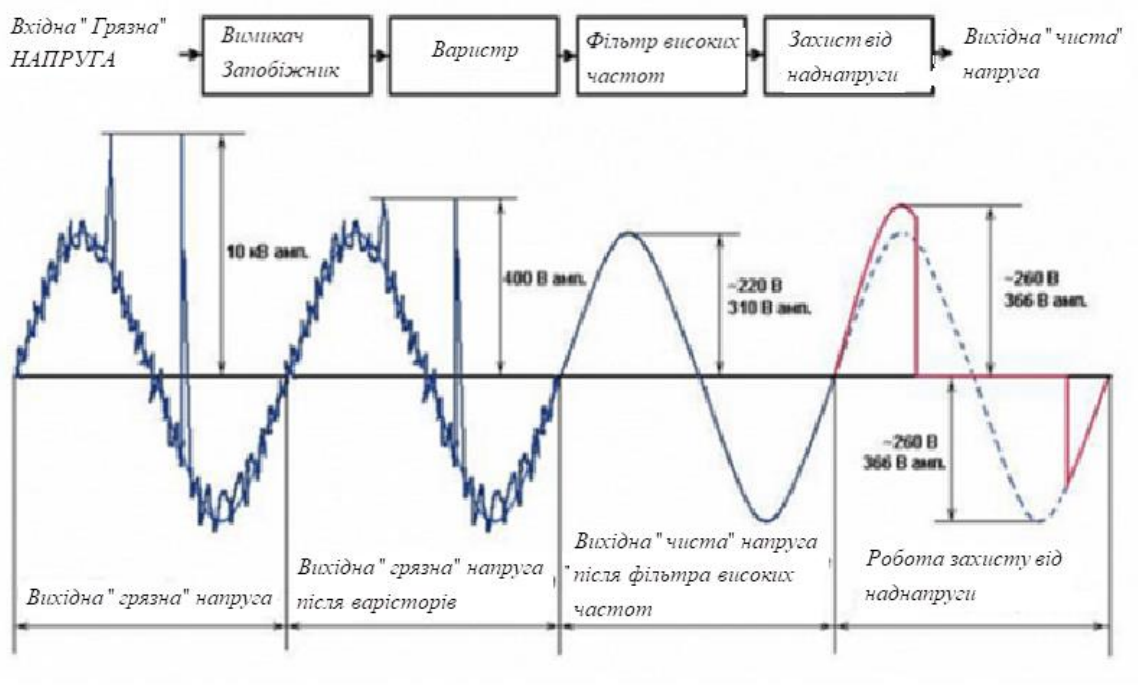

Рисунок 2.2. Структурна схема мережевого фільтру з урахуванням завд, які впливають на значення вхідної напруги.

Мережеві завади шкодять роботі чутливих електричних приладів, що в свою чергу створює необхідність здійснювати фільтрацію струму від зайвих завад. Для досягнення цієї мети застосовується мережевий фільтр, який приєднується між електричною мережею та пристроїм, який живиться від мережі 220 В. Прилад, який здійснює фільтрацію має спеціальну схему, в яку входять конденсатори та дроселі. Головне призначення фільтру – не пропускати завади високої частоти та паразитуючі імпульси. Проти завад високої частоти реалізується індуктивність, а з паразитуючими імпульсами реалізується ємність.

2.2. Структура мережевого фільтру

Засоби, які застосовуються для вилучення завад, можна приєднувати до самої схеми, або можуть бути стаціонарними. Ті, які приєднуються уявляють собою складовою деякого електричного приладу, та и встановлюються безпосередньо в його корпус або в блок живлення. Сам фільтр складається з конденсаторів, індуктивності, термічного запобіжника та варистора (рисунок 2.3). Варистор застосовується для захисту засобу від стрибків напруги.

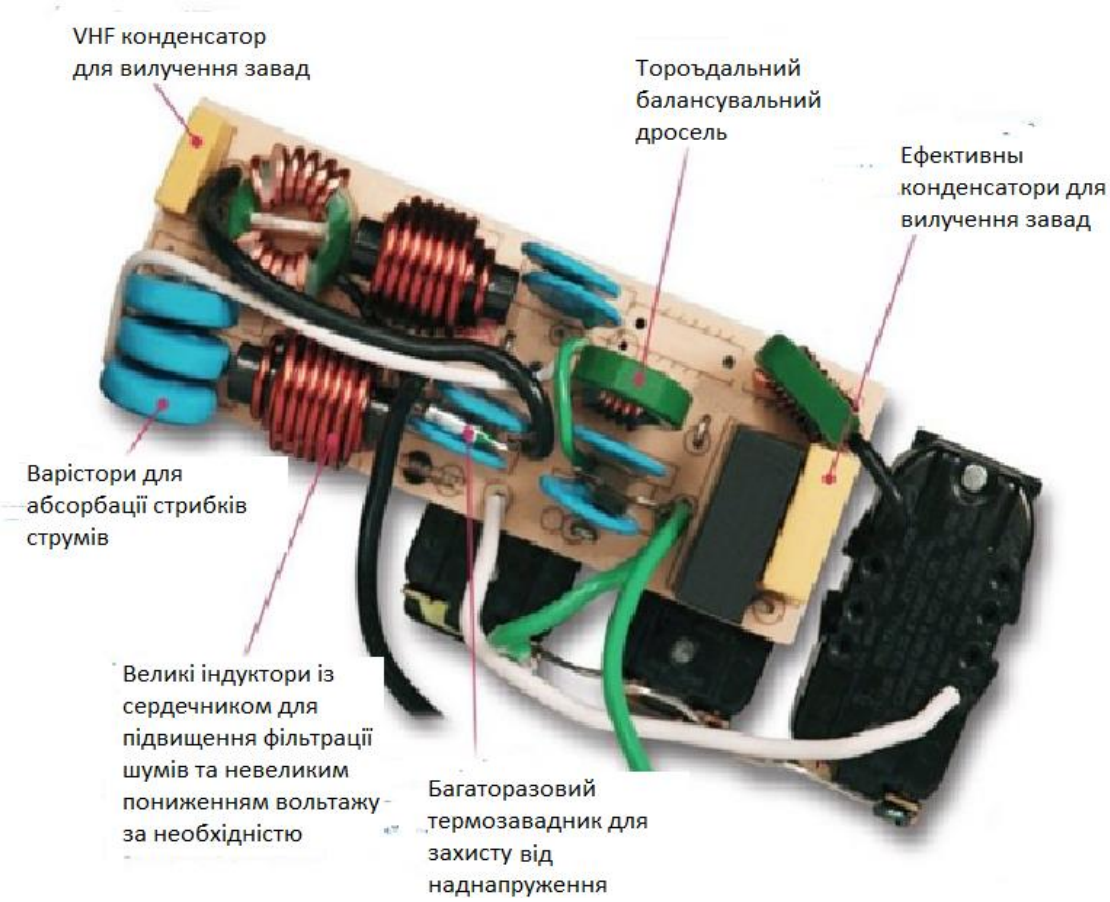

Рисунок 2.3. Елементна структура мережевого фільтру.

Стаціонарні пристрої виконані у вигляді окремого приладу з декількома розетками. Це дає змогу одночасно під'єднати до електромережі кілька одиниць електротехніки, задіявши всього одну розетку. Очищення ВЧ-перешкод забезпечується за допомогою LC-фільтру. Стрибкам напруги запобігають вогнетривкі запобіжники, що не згорають.

Корпус мережевого фільтру містить елементи (рисунок 2.4), які здійснюють фільтрацію,

Рисунок 2.4. Стаціонарний мережевий фільтр.

Для підключення фільтру до мережі застосовується мережевий дріт (рисунок 2.5). Таке конструктивне рішення застосовується в якісних фільтрах.

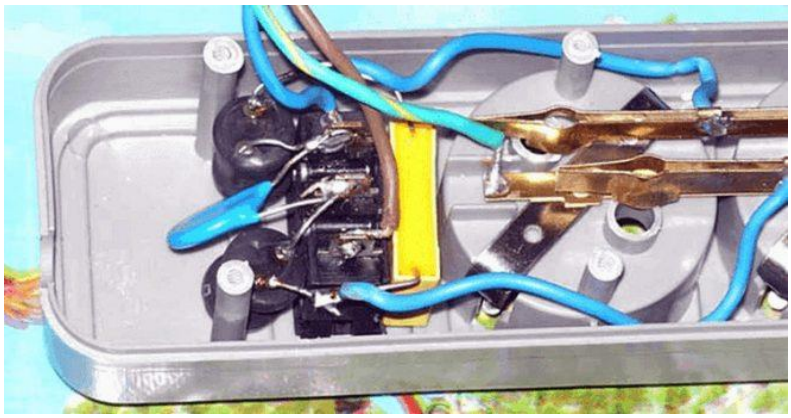

Рисунок 2.5. Мережевий дріт у фільтрі.

Сучасну побутову техніку можна застосовувати для несанкціонованого підключення до електромережі. Для запобіганню цьому, тобто для безпечного

підключення сучасної побутової техніки як правило на ОІД застосовують мережеві фільтри. Вони призначені не тільки для придушення перешкод, а й для згладжування стрибків напруги.

2.3. Етапи виготовлення мережевих фільтрів

Щоб зібрати найпростіший і найкращий мережевий фільтр, в першу чергу потрібна переноска на кілька розеток із мережевим шнуром. Виріб виготовляється з доступних деталей за схемою, яку представлено на рисунку 2.6:

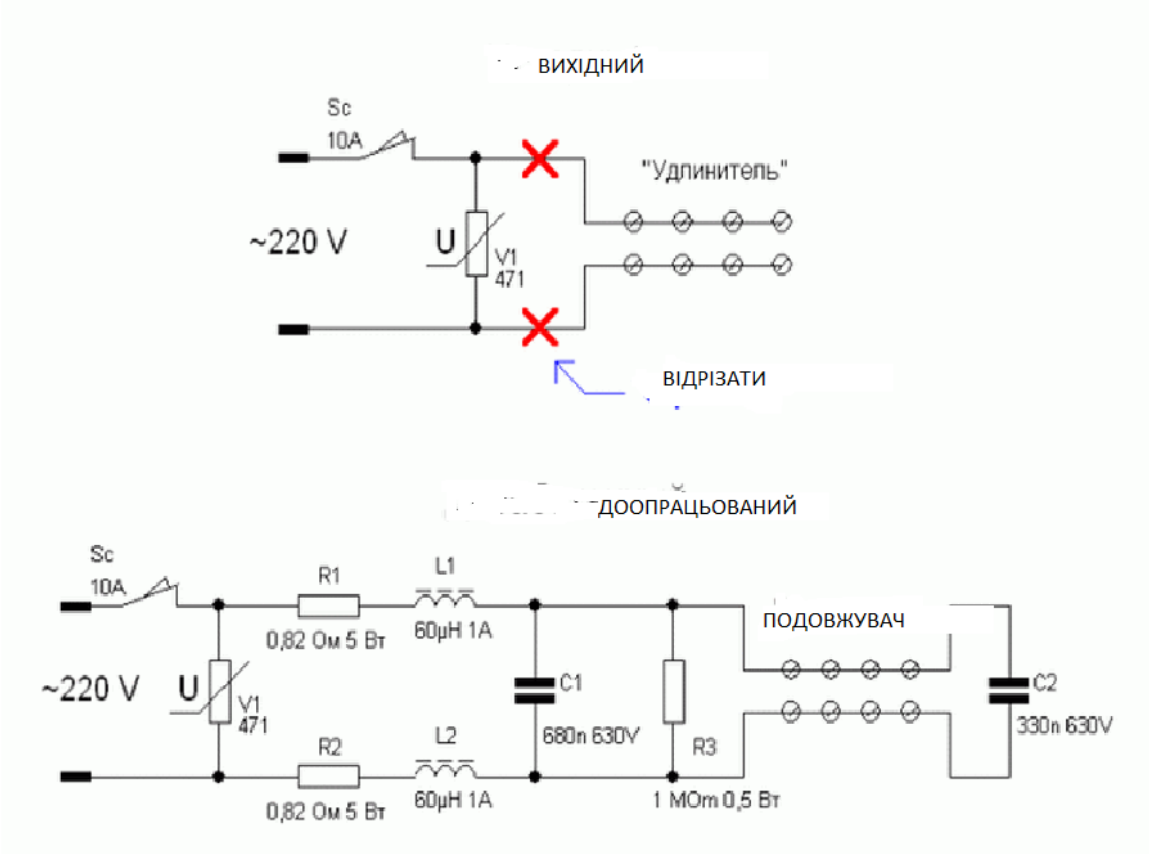

Рисунок 2.6. Схема найпростішого мережевого фільтру.

Більш надійний є фільтр з дроселем та двома обмотками. Такий фільтр з двома обмотками дроселя застосовується для апаратури з високою чутливістю. До такої належить аудіотехніка, колонки якої досить чутливо реагують на перешкоди електромережі. У результаті динаміки відтворюють спотворений звук зі стороннім фоновим шумом. Мережевий фільтр з дроселем на дві обмотки дає

змогу вирішити цю проблему. На рисунку 2.7 представлено схему такого фільтру. Монтаж зручніше виконати в окремому корпусі на друкованій платі.

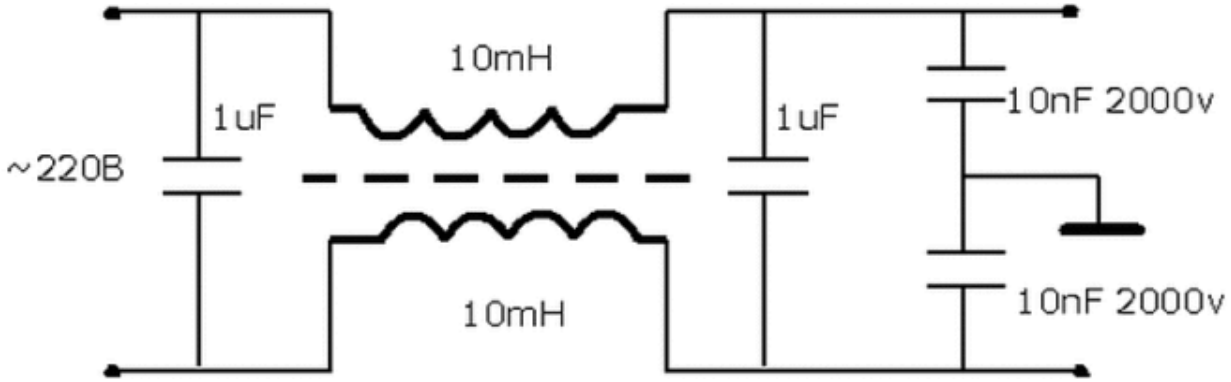

Рисунок 2.7. Схема мережевого фільтру з дроселем.

Монтаж даного фільтру можна виготовити наступним чином:

1. Намотку дроселя виготовлено з феритового кільця марки НМ з магнітною проникливістю 400-3000.
2. Ізоляцію сердечника, яка є тканиною, покривають лаком. В якості обмотки використовують провід ПЕВ, діаметр якого прямо пропорційний потужності навантаження. Як правило це провід діаметром $0{,}25-0{,}35\ мм$ (рисунок 2.8).

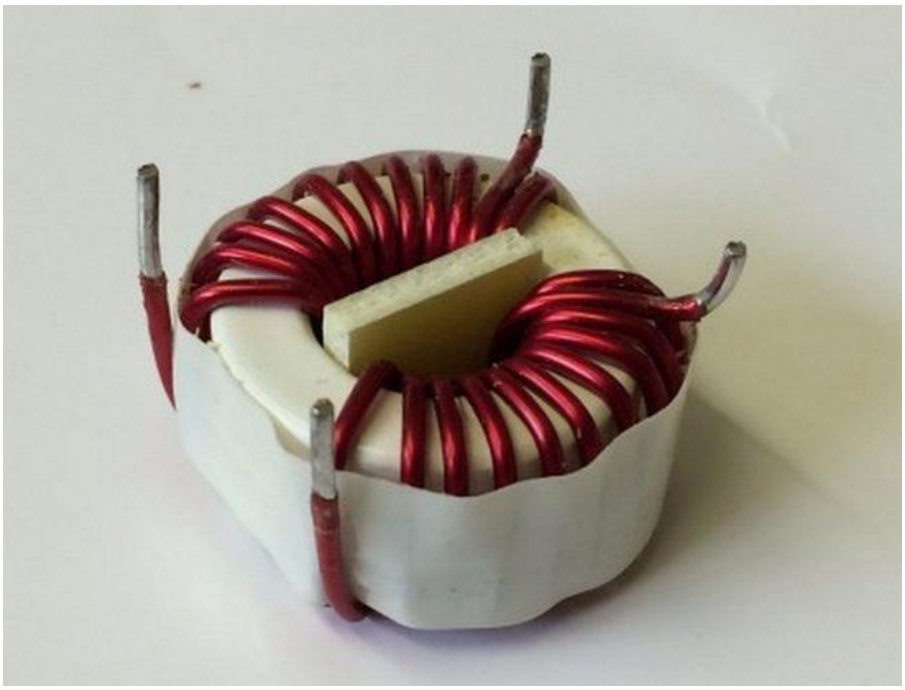

Рисунок 2.8. Сердечник фільтру.

3. Процес обмотки здійснюється одночасно двома дротами в протилежних напрямках. Кожна котушка складається з дванадцяти крутиків.

4. При конструюванні застосовується ємність з робочою напругою 400 В. Вид такої ємності представлено на рисунку 1.9.

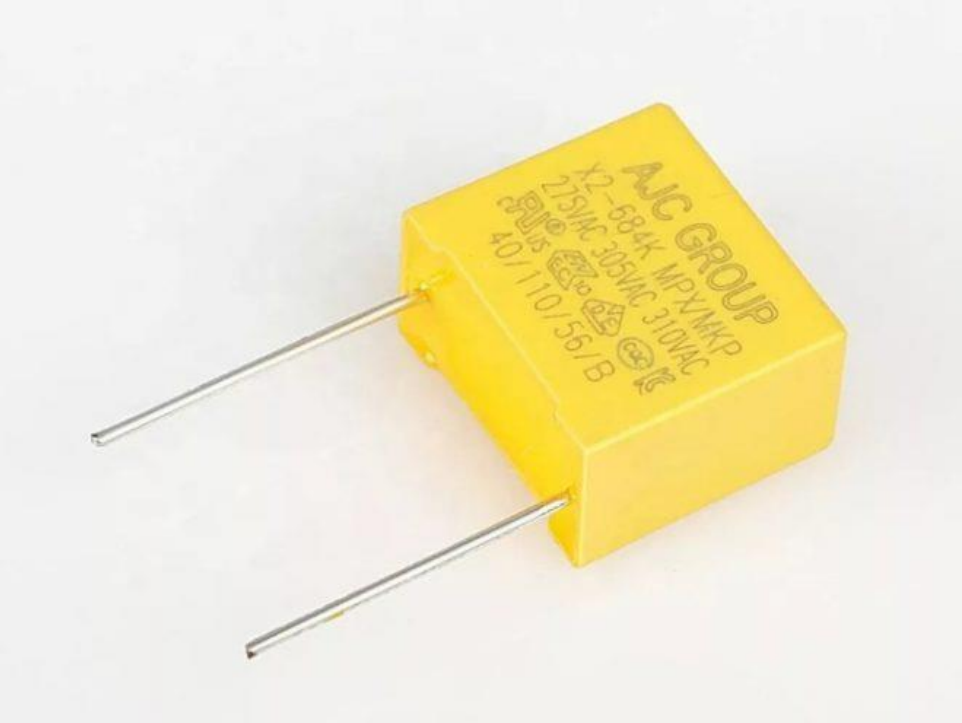

Рисунок 1.9. Ємність з робочою напругою 400 В.

Обмотки дроселя з`єднанні послідовно для того, щоб відбувалось взаємне поглинання магнітних полів. При проходженні струму ВЧ, відбувається зростання опору дроселя. За допомогою конденсаторів здійснюється поглинання шкідливих імпульсів. Сама плата знаходиться в металевому корпусі (рисунок 1.10).

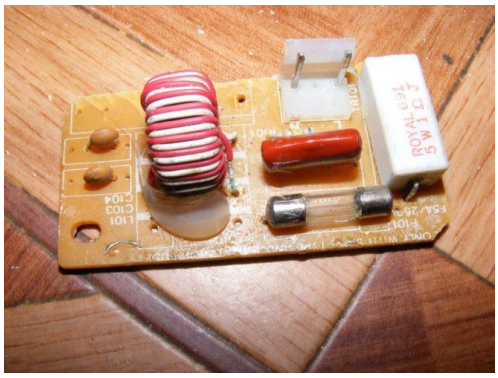

Рисунок 1.10. Плата фільтру з дроселем.

Для запобігання зв`язку між фазою та користувачем, можна зібрати не одну схему. Самий простий варіант полягає в під'єднанні двох трансформаторів від старих джерел безперебійного живлення за схемою, яку представлено на (рисунку 1.11).

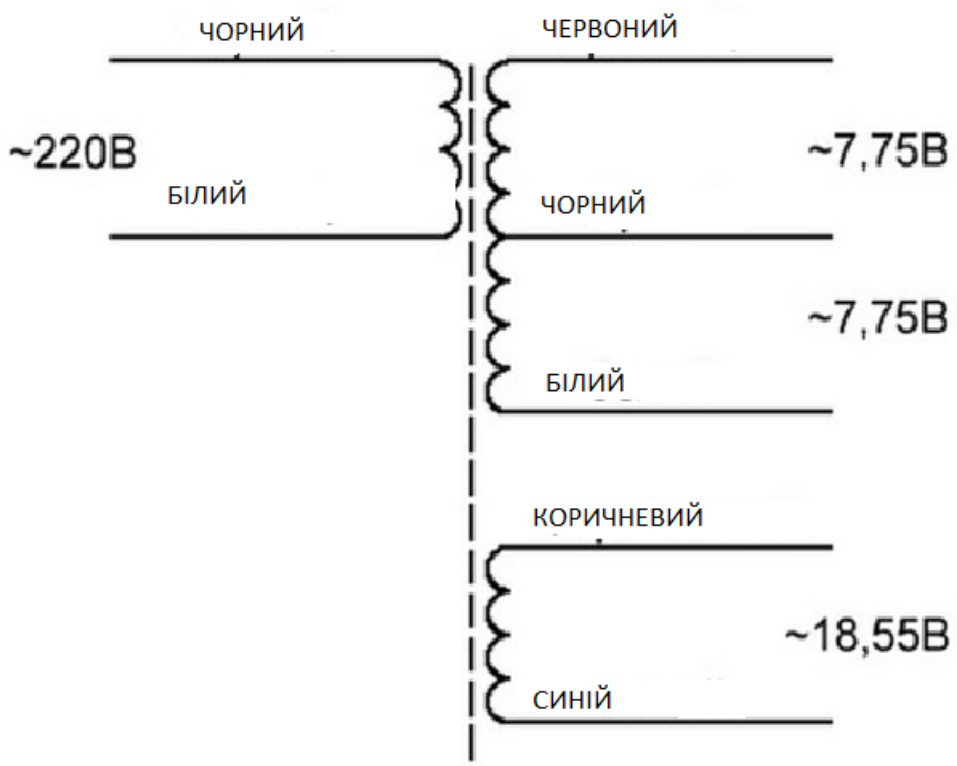

Рисунок 1.11. Схема з двома трансформаторами.

Варто відмітити, схему, яку представлено на рисунку 1.11 продовжують дороблять і остаточний результат схеми представлено на рисунку 1.12.

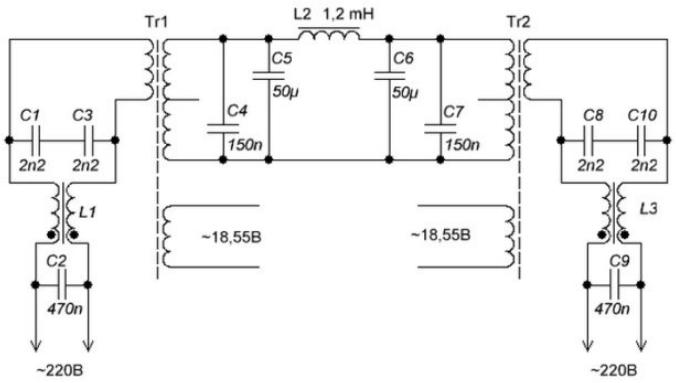

Рисунок 1.12. Остаточна схема фільтру з двома трансформаторами.

Амплітудно-частотну характеристику фільтру, схема якого представлено на рисунку 1.12, представлено на рисунку 1.13.

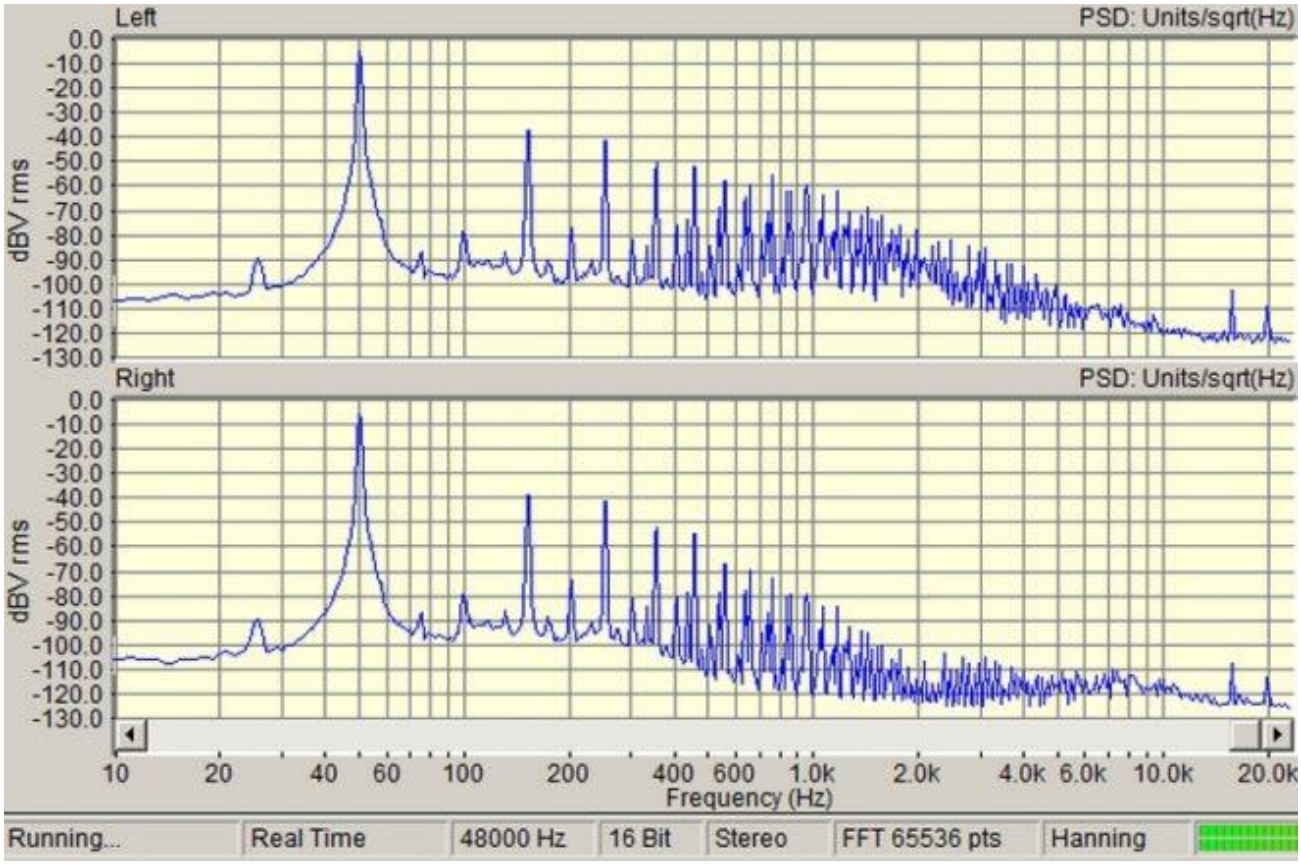

Рисунок 1.13. Амплітудно-частотна характеристика фільтру.

З рисунку 1.13 видно, що процес затухання шкідливих імпульсів здійснюється з достатньо високою швидкістю і даний фільтр варто використовувати для відбиття зовнішніх завад.

Сучасна техніка, в яких встановлено імпульсні блоки живлення, має високий показник чутливості до різних фізичних явищ, які спостерігаються в електричних мережах. Таким небезпечним явищем, як потрапляння блискавки в електромережу 0,4 кВ, можна вивести з ладу довільне обладнання. Ще однією небезпекою є підключення до мережі пристроїв, робота яких здійснюється за допомогою потужних електричних двигунів, електромагнітів, трансформаторів. На рисунку 1.13 представлено схему, яка спроможна отримувати більш високий ступінь придушення мережевих завад. Дана схема дозволяє приєднувати до фільтра монітор, підсилювач, радіочастотні засоби, обчислювальну техніку, які розраховані на роботу від мережі 220 В/50 Гц.

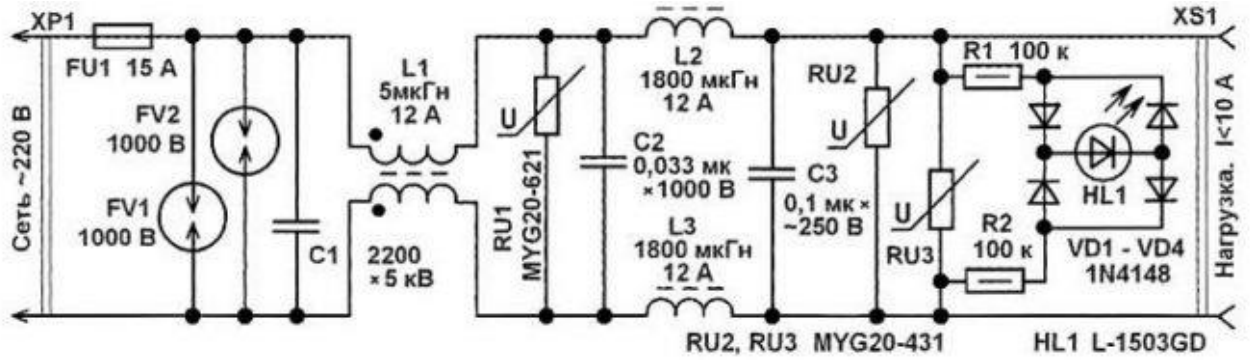

Рисунок 1.14. Схема фільтру для підключення периферійного обладнання.

Вид фільтру після монтажу приведено на рисунку 1.15. Силові лінії зроблено з мідного дроту з ПВХ-ізоляцією з осьовим перерізом 1 мм². Резистори можна використовувати звичайні МЛТ. Конденсатор С1 має бути розрахований на постійну напругу 3 кВ і мати ємність в околі 0,01 мкФ, ємність С2 дорівнює ємності С1 і розраховано на напругу 250 В змінного струму. Дросель L1 має дві обмотки. Даний дросель отримується на феритовій серцевині 600 НН і має діаметр 8 мм, а значення довжини в околі 70 мм. Кожна з двох обмоток складається з 12 завиток лист розміром 10х0,27 мм. Дроселя L2 и L3 виготовлені на броньових сердечниках Б36 з НЧ фериту. Кожен з них має по 30 витків дроту, аналогічного L1. Намотування ведеться виток до витка. Як розрядники можна

використовувати варистор на напругу 910 В. В іншому складання схеми не викликає складнощів.

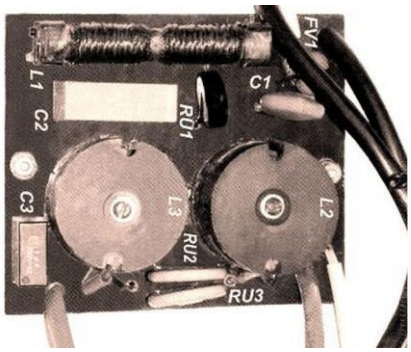

Рисунок 1.15. Вид фільтру після монтажу.

На рисунках 1.16 -1.21 представлено розроблену схему фільтра, який усуває ВЧ-перешкоди, і який не дає можливості проходити через мережі живлення, що в свою чергу не допускає витоку інформації через електричні канали. Необхідним є наявність резисторів, завдяки яким під час вимкнення обладнання ємність розряджалася. Це призведе до того, що ймовірність ураження електричним струмом у разі випадкового торкання вилки фільтра після його вимкнення буде дорівнювати нулю.

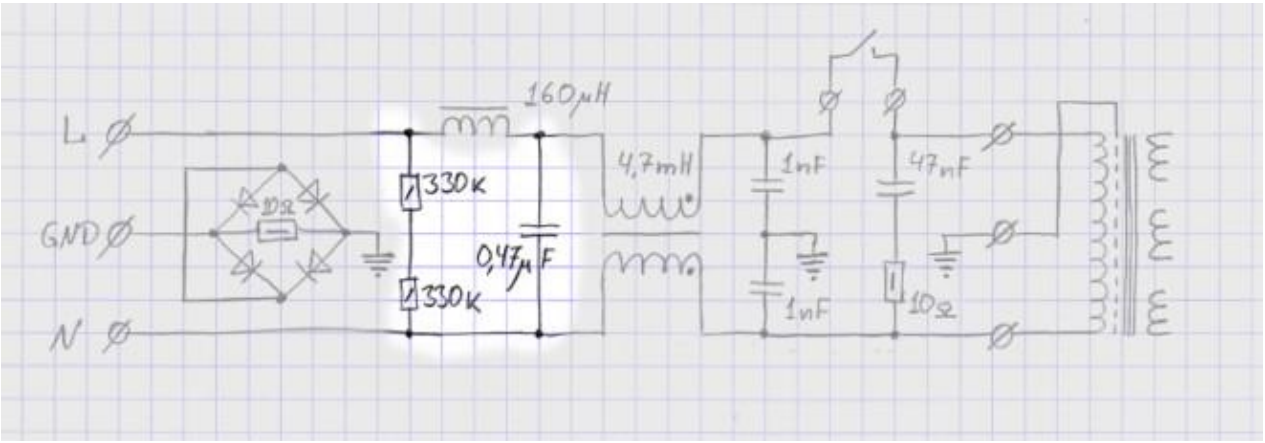

Рисунок 1.16. Фрагмент схеми «*резистор – ємність*».

Індуктивність уявляє собою Г-подібний фільтр, який містить конденсатор. Дросель повинен використовуватися із запасом за струмом, а конденсатор мати напругу не менше 310 В.

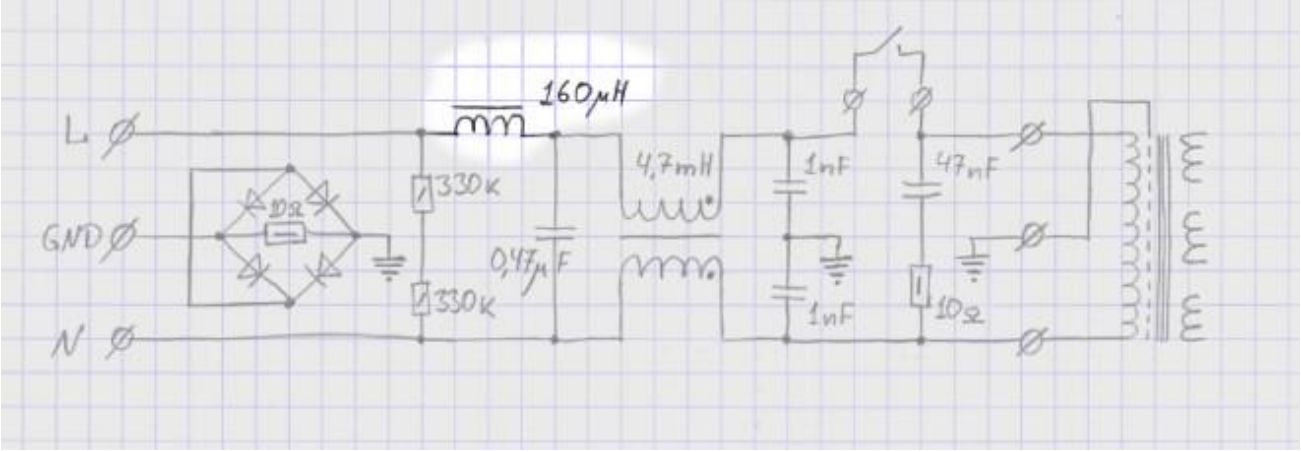

Рисунок 1.17. Фрагмент схеми «*дросель*»

Обмотки трансформатора однакові і мають зустрічне включення. Сердечник трансформатора залишається непідмагніченим основним навантаженням. У результаті створюється велика індуктивність на шляху проходження синфазної завади, перешкоджаючи її потраплянню в обладнання, яке здійснює передачу, прийом та обробку конфіденційної інформації на ОІД.

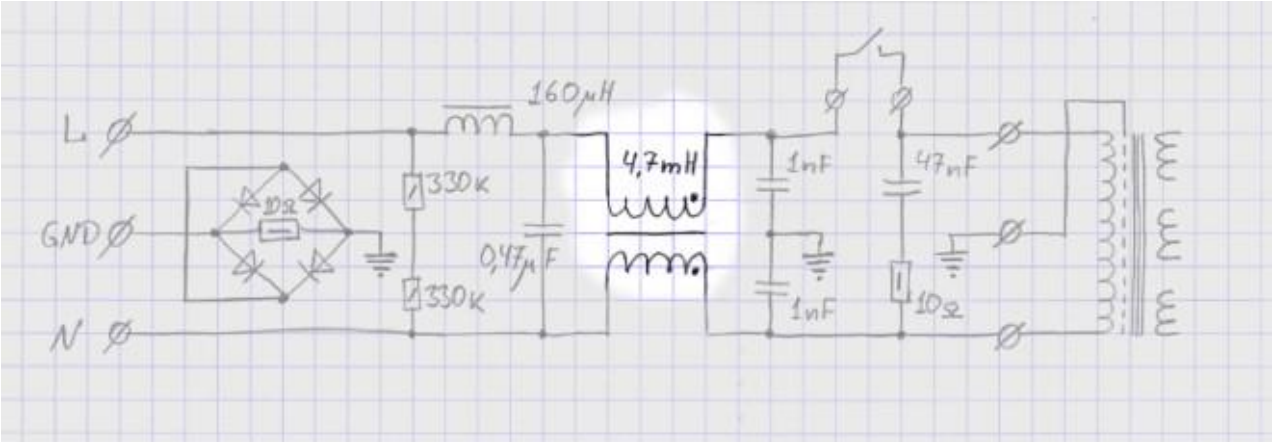

Рисунок 1.18. Фрагмент схеми «*трансформатор*»

Ємності після трансформатора коротять на масу синфазну перешкоду і створюють разом із трансформатором Г-подібний фільтр. За відсутності конденсаторів завада все одно проникне в радіоапаратуру.

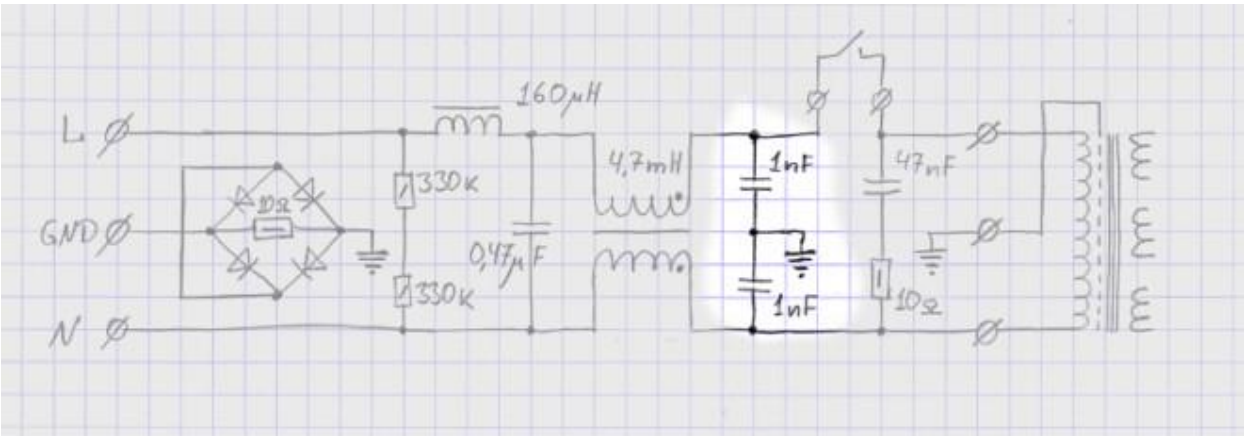

Рисунок 1.19. Фрагмент схеми «*коденсатор*»

RC-ланцюжок разом із первинною обмоткою трансформатора в обладнанні формує коливальний контур, щоб погасити те, що буде на первичному виході після відключення напруги.

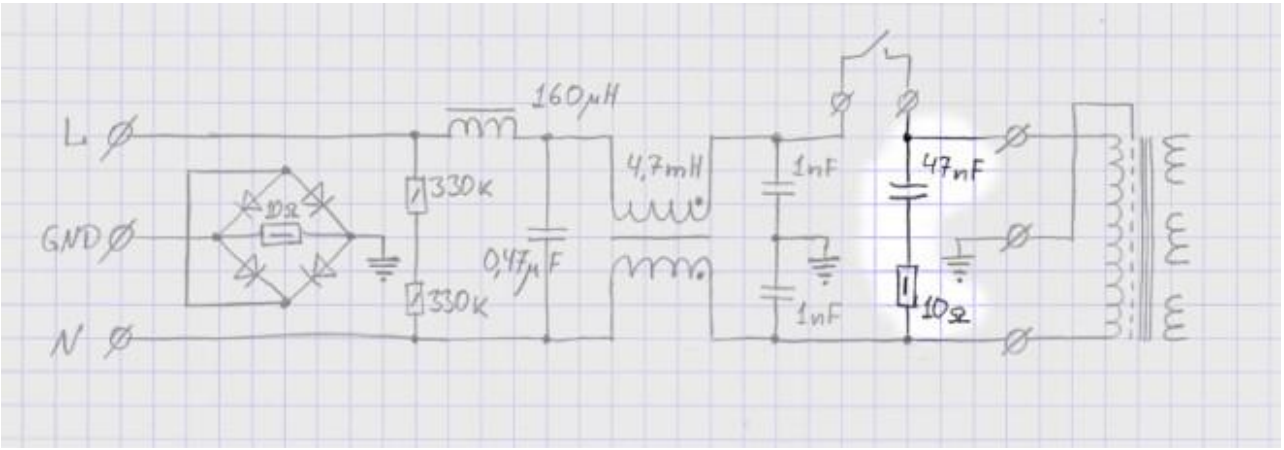

Рисунок 1.20. Фрагмент схеми «*антизвін*»

Таке ввімкнення виконано між корпусом фільтра та захисним заземленням. Схема дає змогу унеможливити появу на корпусі приладу напруги, небезпечної для життя людини. На невеликих напругах за допомогою діодів ланцюг розривається. Опір створює шлях для малих струмів. За відсутності резистора

навіть малі витоки призводили б до надлишкового розмаху напруги на корпусі щодо землі.

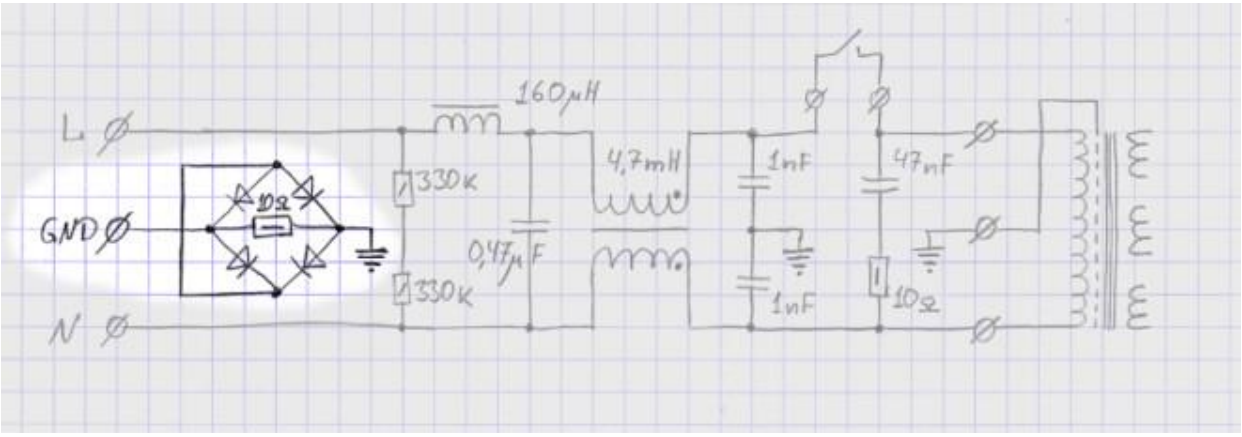

Рисунок 1.21. Фрагмент схеми « *розрив* »

Використовуючи схему відв'язування корпусу приладу від захисного заземлення, вдається зменшити можливі перешкоди, які можуть напряму підмішуватися в сигнал апаратури.

Висновки до розділу 2

1. Для забезпечення захисту інформації на ОІД від витоку по електричним каналам ефективно застосовувати мережеві фільтри з конденсаторами, трансформаторами та дроселями.
2. При спілкування по телефонним лініям дані фільтри відбивають завади, які виникають при несанкціонованому підключенні до телефонних ліній зв`язку.
3. Головними причинами появи завади з частотою мережі живлення або її спектрів є недостатнє згладжування пульсацій у вторинному джерелі живлення, паразитні зв'язки елементів із первинними колами вторинних

джерел живлення, відсутність точок заземлення, наявність загальних дротів живлення, за якими можливий гальванічний зв'язок. З усіх причин тільки перша не є наслідком паразитних процесів. Величина наведення залежить не тільки від виду паразитного зв'язку, а й від схеми підключення двофазних вторинних джерел живлення до трифазної промислової мережі.

4. Крім провідників, які здійснюють заземлення, і функція яких є безпосереднє з'єднання технічних засобів передачі інформації з контуром заземлення, гальванічний зв'язок із землею може мати різні провідники, що виходять за межі зони контролю. До них належать нульовий провід мережі електроживлення, екрани (металеві оболонки) з'єднувальних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій тощо. Усі ці провідники спільно із заземлювальним пристроєм утворюють розгалужену систему заземлення, у якій можуть наводитися інформативні сигнали.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ ЧЕРЕЗ ЕЛЕКТРИЧНІ КАНАЛИ

3.1. Аналіз інтерфейсу передавання даних стандарту Digital Visual Interface як джерела побічного електромагнітного випромінювання

На теперішній час існує чотири основні стандарти інтерфейсів передачі відеоданих, а саме *Video Graphics Array*, *Low – Voltage Differential*, *Digital Visual Interface*, *High – Difinition Multimedia Interface*. Першим стандартом інтерфейсу передачі відео потоку від монітора до персонального комп`ютера був *Video Graphics Array*, після було створено стандарт *Low – Voltage Differential*. Для його заміни у 1999 році було створено цифровий візуальний інтерфейс *Digital Visual Interface*. Стандартом *High – Difinition Multimedia Interface* використовується формат передачі даних, запозичений зі стандарту *Digital Visual Interface*. У відео тракті стандарту *Digital Visual Interface* використовується послідовність і зміст даних, що передаються, такі самі, як і в *Video Graphics Array*, успадковані із систем телевізійної розгортки. Послідовність переданих пікселів відповідає розгортці зліва, праворуч та зверху вниз. Перед кожним кадром і рядком передаються вертикальні та горизонтальні синхронні сигнали. Стандарти *Video Graphics Array* та *Digital Visual Interface* використовують передачу даних про кожен піксель за трьома каналами кольоровості стандартних кольорів *RGB*. У кожному каналі кольоровості послідовно передається одна з 256 градацій інтенсивності. На відміну від стандарту *Video Graphics Array* з аналоговими сигналами, *Digital Visual Interface* застосовує булеві сигнали та алгоритм кодування *Transition Minimized Differential Signaling*.

Transition Minimized Differential Signaling уявляє собою алгоритм кодування, мета якого мінімізація перепадів рівнів, у якому вісім біт кожного каналу кодуються в десять біт за допомогою процесу, який складається з двох етапів.

На першому етапі початковий біт залишається незмінним. Після виконується кодування послідовності з восьми біт з операціями вибору застосування "*виключаючого АБО*" → оператор *XOR*, або "*виключаючого НІ*" →

оператор *XNOR* до поточного біту входу та передуючого біту виходу. Причому під час виконання операції *XOR* останньому біту присвоюється значення "1", а під час операції *XNOR* присвоюється значення "0". Вибір операції здійснюється з метою мінімізації числа переходів. Молодший біт зберігається незмінним, що дає змогу приймачу відновити вихідну послідовність, за рахунок простого перетворення. Під час декодування молодший біт також не змінюється.

На другому етапі, у разі потреби, виконується обертання, інакше кажучи, інвертування послідовності. Десятий біт вказує на наявність звернення. Звернення біт виконується в разі значної неузгодженості потоку даних, тобто перевищення одного значення біт над іншим. Отже, потік балансується. Декодування здійснюється за рахунок звернення послідовності з дев`яти бітів, при умові, що десятий біт встановлено.

Протягом формування електричних сигналів інтерфейсу стандарту *Digital Visual Interface* може бути застосовано один із двох режимів передавання даних.

Перший режим використовує сигнал, який не має властивості симетрії і який формується тільки на одній із двох диференціальних ліній , а саме на "+", або на "–".

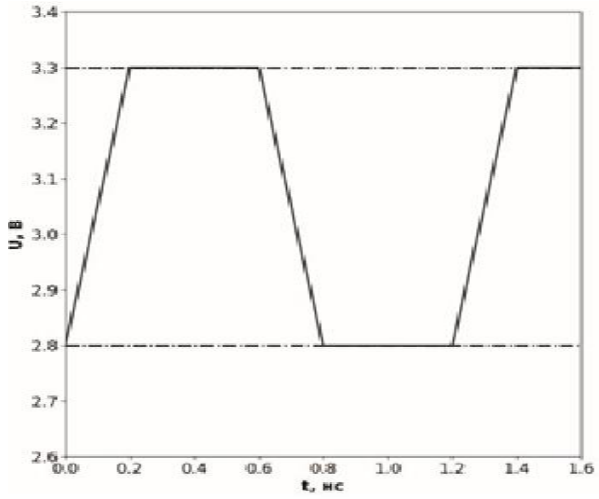

Рисунок 3.1. Форма несиметричного електричного сигналу

На рисунку 3.1 представлено форму такого несиметричного сигналу, де високому рівню несиметричного сигналу відповідає живильна напруга $U_{\max}$, номінальне значення якої становить $3.3B \pm 5\%$. Низький рівень несиметричного сигналу визначається як $U_{\max} - U$, де U уявляє собою напругу розмаху сигналу, що перебуває в діапазоні від $0{,}4B$ до $0{,}6B$.

У другому режимі застосовується диференціальний сигнал. При цьому поточне значення сигналу перебуває в діапазоні від $+U = 0{,}6B$ до $-U = -0{,}6B$. На рисунку 3.2 представлено форму такого диференціального сигналу, який було використано.

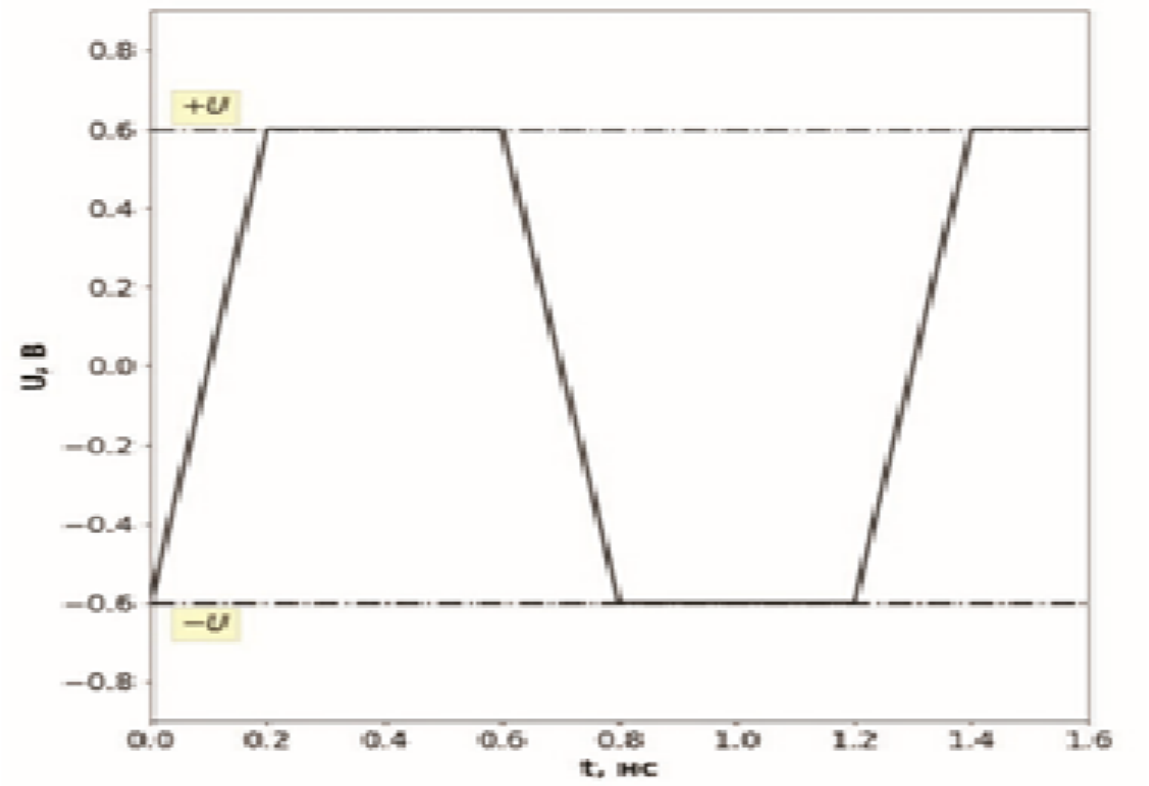

Рисунок 3.2. Форма диференціального сигналу

Алгоритм кодування *Transition Minimized Differential Signaling* реалізується в трьох каналах даних, які несуть вісім біт інформації на три канали кольорів *RGB*. Отже створюється інформація про колір для кожного пікселя в бітному потоці, об`єм якого містить 24 біта. Це дає змогу отримати 256 рівнів яскравості на кожен колір. Передавач *Transition Minimized Differential Signaling* передає

послідовні сигнали чотирма різними провідниками дроту: один має призначення для передачі тактового сигналу, а три інші для *RGB*.

Інтерфейс *Digital Visual Interface* може підтримувати як один канал, так і два канали *Transition Minimized Differential Signaling*. За двоканального *Transition Minimized Differential Signaling* збільшується інформація до шістнадцяти біт на кожен колір, або передається інформація про більшу, ніж у *FULLHD* форматі, кількість пікселів системи відображення інформації. Використання двоканального *Transition Minimized Differential Signaling* застосовується на частоті відеосигналу понад 165 *МГц*.

Алгоритм кодування *Transition Minimized Differential Signaling* забезпечує зниження рівнів побічного електромагнітного випромінювання у поєднанні з високою пропускною спроможністю інтерфейсу *Digital Visual Interface* завдяки розширенню смуги зайнятих частот, що досягається передачею інтенсивності випромінювання кодовою комбінацією з десяти біт. Водночас час передавання інформації про один піксель зберігається порівнянним із часом передавання імпульсу яскравості одного пікселя в стандарті *Video Graphics Array*. Це призводить до десятикратного розширення смуги частот побічного електромагнітного випромінювання і відповідного зниження його спектральної щільності. Крім того, *Transition Minimized Differential Signaling* використовує диференціальну передачу даних зі зменшеним числом переходів сигналів зі стану "нуль" у стан "один" або навпаки, що є добре відомим методом зниження поза смугового випромінювання передавачів за високих швидкостей передавання інформації радіоканалом . Оскільки під час реєстрації побічного електромагнітного випромінювання роздільне приймання випромінювання від різних каналів кольоровості неможливе, порушник може отримати доступ тільки до сумарної інтенсивності випромінювання *RGB*, утвореного суперпозицією електромагнітних полів від трьох каналів кольоровості , що випромінюються одночасно.

Пропонується для розроблення програмно-реалізованого способу пасивного захисту інформації від витоку через побічне електромагнітне випромінювання відео системи стандарту *Video Graphics Array* використовувати зв'язок реєстрованої сумарної інтенсивності побічного електромагнітного випромінювання, яку реєструють, із поточним варіантом відтінку кольору, який відображається на екрані монітору.

3.2. Експериментальний аналіз зв'язку зорового контрасту зображення та зміни інтенсивності побічного електромагнітного випромінювання

Для аналізу зв'язку зорового контрасту зображення і зміни інтенсивності побічного електромагнітного випромінювання відео системи стандарту *Digital Visual Interface* було використано експериментальну установку, схема якої зображено на рисунку 3.3.

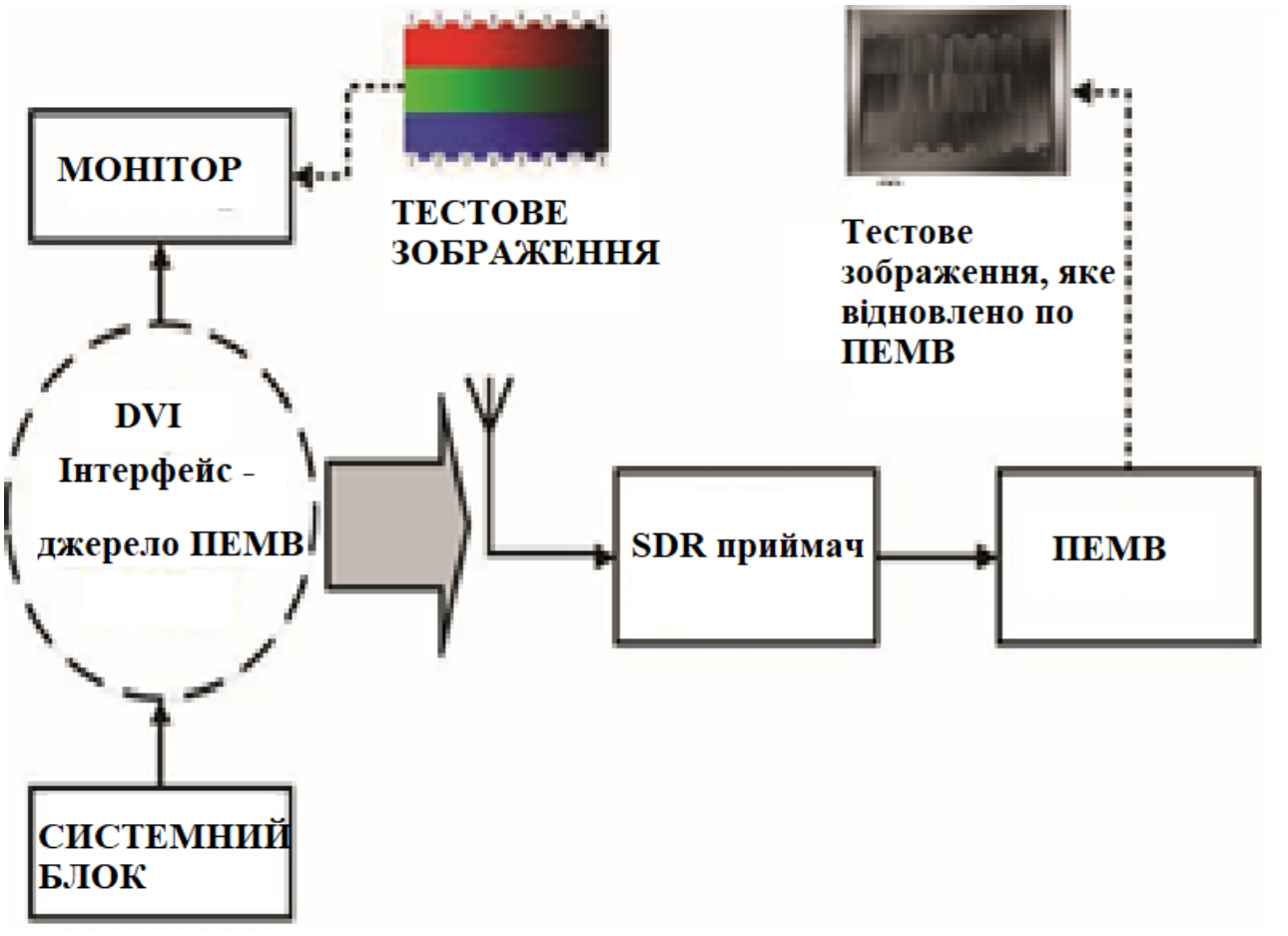

Рисунок 3.3. Структурна схема експериментальної установки

Для здійснення процесу формування графічної інформації було використано текстове зображення. Відео потік інформативних даних з тестовими зображеннями відправляється від монітору до системного блоку за допомогою відео інтерфейсу, що використовує стандарт *Video Graphics Array*, який формує ПЕМВ. Дане випромінювання приймається за допомогою антени і подається на приймач, який на рисунку зображено як *SDR*-пристрій, в якому відбувається аналого-цифрове перетворення прийнятих сигналів. Після цього здійснюється процес реєстрації синфазної та квадратурної складових вхідного вектора за допомогою спеціального програмного забезпечення, розробленого на базі *GNUradi ma Python*.

Зареєстрована вхідна реалізація містить сигнал побічного електромагнітного випромінювання, фонові шуми та завади, а також власні шуми приймача. Оскільки побічне електромагнітне випромінювання містить складові, які повторюються з певним періодом, у вигляді рядкових та кадрових синхронних груп, то для їх виявлення створюється автономна кореляційна функція (*АКФ*) вхідної реалізації. Інтервал між двома максимумами *АКФ* відповідає кількості штрихів, що припадають на один рядок зображення. Після цього виконується рядкова розгортка кадру, що відновлюється. Для поліпшення якості відновлюваного зображення записана реалізація сигналу побічного електромагнітного випромінювання розбивається на сукупність кадрів, з якої формується один кадр шляхом усереднення значень кожного окремого відліку.

Під час дослідження зв'язку кодування, використовуваного в алгоритмі *Transition Minimized Differential Signaling*, та інтенсивності побічного електромагнітного випромінювання, відбувався процес відновлення тестового зображення, яке зображено на рисунку 3.4.

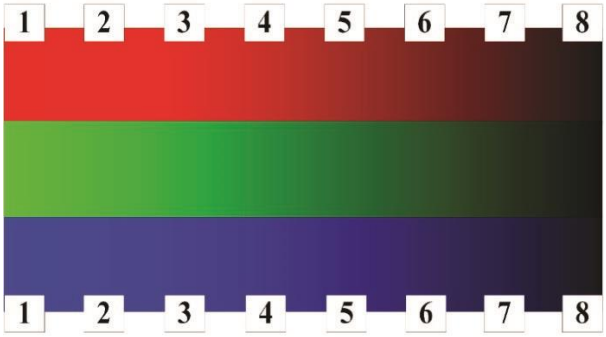

Рисунок 3.4. Тестове зображення з монітору

Графічна інформація містить три шкали градацій яскравості основних кольорів *RGB* від світлого відтінку до темного. Для аналізу рівнів зорового контрасту тестове зображення супроводжується лінійкою, в якій кожній ділянці відповідає вісім градацій яскравості та відповідно вісім різних *Transition Minimized Differential Signaling* кодів у кожному з каналів кольоровості відео тракту. Після цього було відновлено тестове зображення та реалізовано між кадрове накопичення метою якого є підвищення якості зображення.

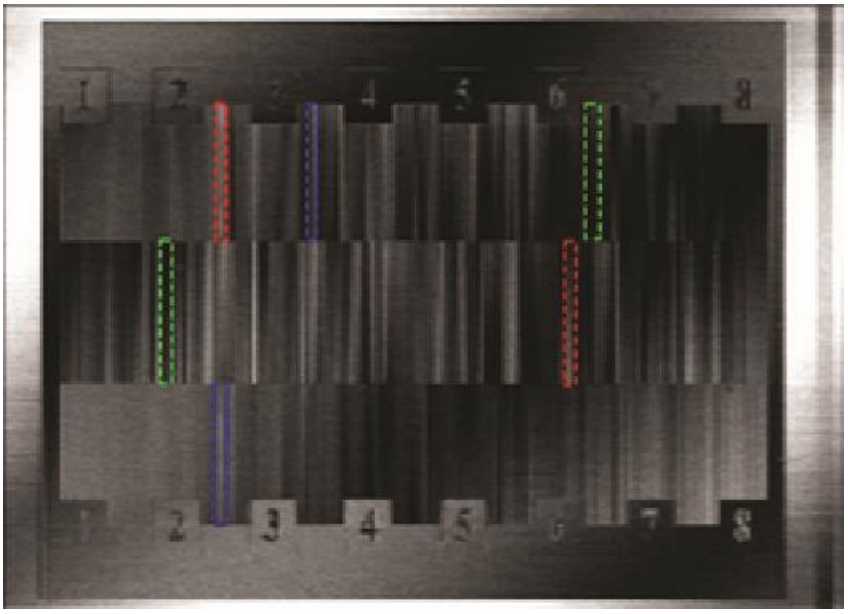

Рисунок 3.5. Відновлене тестове зображення

З рисунку 3.5 представлено відновлене зображення, яке демонструє широке розвинення яскравості побічного електромагнітного випромінювання в умовах однакових кодувань при різних каналах яскравості. При цьому завжди існує можливість підібрати області яскравих і світлих ділянок палітри, що мають

практично достатньо слабкі рівні побічного електромагнітного випромінювання. З рисунку 3.5 синім пунктиром виділено області однакової інтенсивності побічного електромагнітного випромінювання, що відповідають фрагментам тестового зображення з відтінками кольору, заданими *RGB* комбінаціями $0-0-52$ та $86-0-0$. Червоним і зеленим пунктиром виділено області з відтінками кольору: $0-201-0-0$ та $50-0-0$, а також $213-0-0-0$ та $0-40-0$. Усі обрані пари кодових комбінацій мають різні щільності різних кольорів та сусідні рівні побічного електромагнітного випромінювання. Порівняння представлених на рисунках 3.4 та 3.5 зображень демонструють можливість вибору таких відтінків кольору, які будуть прийнятними для сприйняття інформації оператором і знизять імовірність перехоплення побічного електромагнітного випромінювання зловмисником.

Спосіб підвищення захищеності інформації від витоку через електричні канали та ПЕМВ відео системи стандарту *Digital Visual Interface* реалізується виконанням наступних операцій:

- реєструються шкали синхронних фазних та квадратурних складових вхідного потоку в приймачі та створюється автономна кореляційна функція адитивної складової побічного електромагнітного випромінювання та шумів;

- визначається кількість шкал між двома сусідніми максимумами, що припадають на один рядок зареєстрованого зображення;

- здійснюється формування рядкової розгортки прийнятої реалізації, за якої для подальшого відображення її в градаціях сірого кольору кожному відліку сигналу ставиться у відповідність число від 0 до 255;

- здійснюється аналіз побудованого порядкового розгортання та наявність періодичних піків автономної кореляційної функції для визначення числа шкал, які припадають на один кадр зображення;

- визначається початковий відлік і будується один повний кадр зображення;

- здійснюється виконання між кадрового накопичення для підвищення відношення *сигнал/шум*;

- здійснюється зіставлення відтінків тестового зображення і рівня побічного електромагнітного випромінювання, яке зареєстровано;

- визначається така пара відтінків кольору, яка, з одного боку, формує рівні побічного електромагнітного випромінювання, яке зареєстровано, а з іншого боку, забезпечує прийнятний для оператора контраст двоколірного зображення, яке виводиться на монітор;

- така пара відтінків використовується для налаштування колірної палітри виведення конфіденційної інформації у вигляді двоколірних текстів або зображень на екран монітора.

Оскільки зниження контрасту, що реєструється побічним електромагнітним випромінюванням, рівновелике зниженню відношення *сигнал/шум* під час роботи системи розпізнавання інформації яка відображається на екран монітору, то це призводить або до зниження ймовірності витоку інформації через ПЕМВ відео системи стандарту , або до повної неможливості використання *Digital Visual Interface* побічного електромагнітного випромінювання потенційним зловмисником.

Для демонстрації працездатності запропонованого підходу було сформовано тестовий приклад виведення двоколірної інформації, що представлено на рисунку 3.6, у вигляді набору текстових символів у чотирьох варіантах колірних відтінків для тексту і фону. Варіанти колірних відтінків визначалися максимальним контрастом, а саме чорно/білий текст та трьома варіантами відтінків, що мають мінімальні відмінності в рівнях побічного електромагнітного випромінювання, зазначеними пунктиром на рисунку 3.6.

Рисунок 3.6. Тестове виведення двокольорової інформації на екран

Відновлені зображення тестового прикладу виведення двоколірної інформації, зареєстровані за каналом побічного електромагнітного випромінювання, представлено на рисунку 3.7.

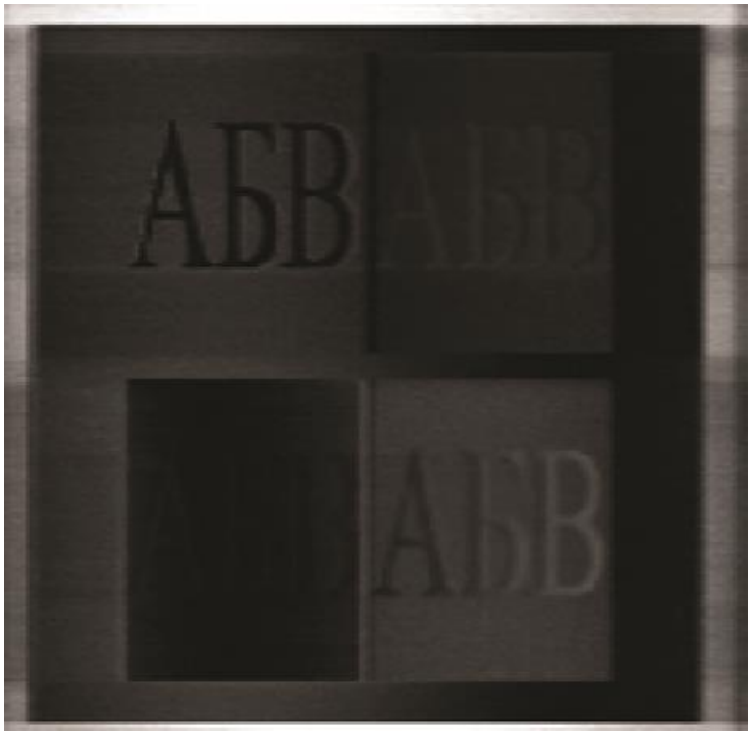

Рисунок 3.7. Відновлення з каналу побічного електромагнітного випромінювання

Висновки до розділу 3

На основі проведених експериментів можна зробити висновок, що не всі поєднання близьких за яскравістю фрагментів відновленого зображення забезпечують однакове зниження контрасту побічного електромагнітного випромінювання, однак у всіх визначених парах комбінацій відтінків величина контрасту побічного електромагнітного випромінювання знижується, що відповідає зниженню інформативності побічного електромагнітного випромінювання. Отже, на основі порівняння значень інтенсивності побічного електромагнітного випромінювання для різних відтінків кольору, що задаються *RGB* комбінаціями, показано можливість використання таких пар *RGB* комбінацій, що будуть прийнятними для сприйняття інформації оператором і знизять ризик перехоплення побічного електромагнітного випромінювання зловмисником, або дадуть змогу зменшити необхідну потужність випромінювання системи активного здійснення погашення побічного електромагнітного випромінювання відео системи стандарту *Digital Visual Interface.* .

ВИСНОВКИ

1. Електромагнітні випромінювання передавачів засобів зв'язку, модульовані інформаційним сигналом, можуть перехоплюватися природним чином із використанням стандартних технічних засобів. Цей електромагнітний канал перехоплення інформації отримав широке застосування для прослуховування телефонних розмов, що ведуться по радіотелефонах, стільникових телефонах або по радіорелейних та супутникових лініях зв'язку. Для запобігання цьому варто перетворювати інформацію в відеосигнал, де зберегти конфіденційність стає більш надійним.

2.Електричний канал перехоплення інформації, що передається кабельними лініями зв'язку, передбачає контактне підключення до цих ліній. Цей канал найчастіше використовують для перехоплення телефонних розмов, при цьому

інформацію, яку перехоплюють можна записати на диктофон або передати по радіоканалу. Подібні пристрої, що підключаються до телефонних ліній зв'язку і містять радіопередавачі для ретрансляції перехопленої інформації. В таких випадках варто застосовувати спеціальні фільтри, які не дають можливість виявляти інформативний сисгнал при несанкціонованому втручанні.

3.Варто зазначити, що безпосереднє електричне під'єднання апаратури перехоплення є компрометуючою ознакою, тому частіше використовується індукційний канал перехоплення, який не потребує контактного під'єднання до каналів зв'язку. Сучасні індукційні датчики, за повідомленнями відкритої преси, здатні знімати інформацію з кабелів, захищених не тільки ізоляцією, а й подвійною бронею зі сталевої стрічки і сталевого дроту, які щільно обвивають кабель.

\

ВИСНОВОК

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. T. Saati. Ob izmerenii neosyazaemogo. Podhod k otnositel'nym izmereniyam na osnove glavnogo sobstvennogo vektora matricy parnyh sravnenij // ZHurnal «Cloud of Science». 2015. T.2. №1. pp. 5-39;

2. S.V. Dvoryankin, Y.K. Makarov, A.A. Horev. Obosnovanie kriteriev ehffektivnosti zashchity rechevoj informacii ot utechki po tekhnicheskim kanalam // Zhurnal «Zashchita informacii. Insajd». 2007. №2. pp. 18-25;

3. A.P. Zajcev, R.V. Meshcheryakov, A.A. Shelupanov. «Tekhnicheskie sredstva i metody zashchity informacii», Moskva: «Goryachaya liniya-Telekom», 7 edition, 2012. 442 p.;

4. A.P. Durakovskij, I.V. Kunicin. Ocenka zashchishchyonnosti rechevoj informacii. Chast' 1. Vyyavlenie akusticheskih i vibracionnyh kanalov utechki rechevoj informacii. M.: NIYAU MIFI, 2015. 52 p.;

5. V.K. Zheleznyak, D.S. Ryabenko, S.V. Lavrov, A.P. Provozin. Metodologicheskoe issledovanie zashchishchyonnosti informacii ob'ektov informatizacii // Zhurnal «Vestnik Polockogo gosudarstvennogo universiteta. Seriya S: Fundamental'nye nauki». 2014. №12. pp. 21-29.

6. О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. Виявлення та блокування засобів негласного отримання інформації на об`єктах інформаційної діяльності. Навчальний посібник. 2020.: Київ «ДУТ». С. 126.

7. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

8. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

9. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

10. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

11. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

12. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

13. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

14. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

15. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.