Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Зайончковський Олег Дмитрович*

академічної групи *125-16-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Зайончковський Олег Дмитрович*** **академічної групи** ***126-16-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз каналів витоку інформації при експлуатації персональних комп'ютерів, а також існуючих підходів до ЗІ від витоків по каналу побічних електромагнітних випромінювань.	25.02.2020 – 31.03.2020
Розділ 2	Розробка підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад та оцінка його ефективності.	01.04.2020 – 12.05.2020
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2020 – 09.06.2020

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Зайончковський О.Д.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 13 рис., 3 таблиці, 4 додатки, 24 джерела.

Об’єкт розробки – канал побічних електромагнітних випромінювань і наведень.

Предмет розробки – підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора.

Мета кваліфікаційної роботи – підвищення ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання відносно інформативного сигналу.

Наукова новизна результатів полягає у застосуванні пристрою захисту інформації, який створює за допомогою СВЗ, імітаційні та маскуючі завади, що забезпечують приховування інформативних сигналів випромінювання, створюваних пристроєм відеовідображення (монітором).

У першому розділі проаналізовано канали витоку інформації при експлуатації персональних комп’ютерів, а також існуючі підходи до ЗІ від витоків по каналу побічних електромагнітних випромінювань і наведень.

У спеціальній частині роботи запропоновано підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.

ПОБІЧНЕ ЕЛЕКТРОМАГНІТНЕ ВИПРОМІНЮВАННЯ, ІМІТАЦІЙНІ ТА МАСКУЮЧІ ЗАВАДИ, ЗАХИСТ ІНФОРМАЦІЇ, АМПЛІТУДНІ СПЕКТРИ, ТЕХНІЧНИЙ ЗАСІБ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка 69 с., 13 рис., 3 таблицы, 4 приложения, 24 источника.

Объект разработки – канал побочных электромагнитных излучений и наводок.

Предмет разработки – подход к защите информации от утечки по каналу побочных электромагнитных излучений и наводок монитора.

Цель квалификационной работы – повышение эффективности использования энергии помехи за счет ее адаптивности по ширине спектра, уровню и времени излучения относительно информативного сигнала.

Научная новизна заключается в применении устройства защиты информации, создающего с помощью СИП, имитационные и маскирующие помехи, обеспечивающие сокрытие информативных сигналов излучения, создаваемых устройством видеоотображения (монитором).

В первой главе проанализированы каналы утечки информации при эксплуатации персональных компьютеров, а также существующие подходы к ЗИ от утечек по каналу побочных электромагнитных излучений и наводок.

В специальной части работы предложен подход к защите информации от утечки по каналу побочных электромагнитных излучений и наводок монитора с использованием имитационных и маскирующих помех и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на эксплуатацию системы безопасности и срок окупаемости инвестиций применения предложенного подхода.

ПОБОЧНОЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ, ИМИТАЦИОННЫЕ И МАСКИРУЮЩИЕ ПОМЕХИ, ЗАЩИТА ИНФОРМАЦИИ, АМПЛИТУДНЫЕ СПЕКТРЫ, ТЕХНИЧЕСКОЕ СРЕДСТВО, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 69, fig. 13, tab. 3, 4 additions, 24 sources.

The object of development is a channel of spurious electromagnetic radiation and interference.

The subject of development is an approach to protecting information from leakage through the channel of spurious electromagnetic radiation and interference from the monitor.

The purpose of the qualification work is to increase the efficiency of using the interference energy due to its adaptability to the spectral width, level and time of radiation relative to the informative signal.

Scientific novelty lies in the use of an information protection device that creates, using SIP, imitating and masking interference, which ensures the concealment of informative radiation signals generated by a video display device (monitor).

The first chapter analyzes the channels of information leakage during the operation of personal computers, as well as the existing approaches to ZI from leaks through the channel of secondary electromagnetic radiation and interference.

In a special part of the work, an approach to protecting information from leakage through the channel of spurious electromagnetic radiation and interference from the monitor using imitation and masking interference is proposed and its effectiveness is evaluated. Based on the results of the research, conclusions are drawn regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of operating the security system and the payback period of the application of the proposed approach.

SIDE ELECTROMAGNETIC RADIATION, SIMULATION AND MASKING INTERFERENCE, INFORMATION PROTECTION, AMPLITUDE SPECTRA, TECHNICAL MEANS, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСК – Автоматизована система керування;

ВС – Відеосистема;

ВЧ – Висока частота;

ГПЙП – Гранична повна ймовірність похибки;

ГШС – Генератор шумових сигналів;

ЗІ – Захист інформації;

ЗОТ – Засіб обчислювальної техніки;

ЕМС – Електромагнітна сумісність;

ЕОМ – Електронна обчислювальна машина;

КВА – Контрольно-вимірювальної апаратури;

ПЕМВ – Побічне електромагнітне випромінювання;

ПЕМВН – Побічне електромагнітне випромінювання і наведення;

ПЕОМ – Персональна електронна обчислювальна машина;

ПК – Персональний комп’ютер;

СВЗ – Система випромінювання завад;

СОІ – Система обробки інформації;

ТЗ – Технічний засіб;

ТЗР – Технічний засіб розвідки;

EDID –Extended display identification data – Розширені ідентифікаційні дані дисплея;

EEPROM – Electrically Erasable Programmable Read-Only Memory – Постійний запам'ятовувальний пристрій, що електрично стирається та перепрограмовується.

ЗМІСТ

с.

ВСТУП

В процесі функціонування технічних засобів (ТЗ) обробки, зберігання та передачі інформації в конструктивних елементах і кабельних з'єднаннях цих пристроїв циркулюють електричні струми інформативних сигналів. Це призводить до формування і випромінювання в навколишній простір електромагнітних полів, рівні яких можуть бути достатніми для їх прийому на відстані від технічного засобу і вилучення з них інформації за допомогою спеціальної апаратури. Можливість прихованого від власника технічного засобу знімання інформації, що обробляється на пристрої, складність виявлення електромагнітного каналу витоку інформації зумовили високий інтерес до методів і засобів аналізу побічного електромагнітного випромінювання, технічних засобів обробки, зберігання та передачі інформації.

Під витоком інформації по каналах побічного електромагнітного випромінювань і наведень (ПЕМВН) мається на увазі можливість доступу до інформації, що обробляється на технічних засобах, здійснюваного шляхом перехоплення і відповідної обробки побічних електромагнітних випромінювань технічних засобів передачі, обробки та зберігання інформації. Канал витоку інформації включає в себе технічний засіб, середу поширення електромагнітних хвиль, систему перехоплення і обробки побічних випромінювань.

Канали витоку інформації можуть виникати внаслідок випромінювання інформативних сигналів при-роботі технічного засобу і наведення цих сигналів в лініях зв'язку, ланцюгах живлення і заземлення, інших комунікаціях. ПЕМВ технічних засобів може поширюватися на великі відстані і реєструватися сучасними вимірювальними засобами. Частоти інформаційних складових побічних випромінювань залежать від типу технічного засобу і видів сигналів, що обробляються на ньому, і можуть перекривати діапазон частот від сотень Гц до декількох десятків ГГц.

Для захисту технічних засобів від витоку інформації застосовуються організаційні і технічні заходи. Організаційні заходи спрямовані на те, щоб, не

змінюючи рівня ПЕМВ досліджуваного пристрою або рівня електромагнітних шумів шляхом зміни розташування ТЗ домогтися зменшення зони можливого перехоплення інформації. До технічних заходів захисту інформації відносяться заходи і засоби, що впливають або на рівень ПЕМВ, або на рівень електромагнітних шумів. Наприклад, електромагнітне екранування є ефективним способом захисту інформації.

При проведенні інженерно-технічних досліджень для забезпечення стаціонарності випромінювання технічного засобу і, як наслідок, більш впевненого виявлення інформаційних складових в ПЕМВ ТЗ, на практиці використовують такий режим роботи пристрою, при якому в ньому циклічно виконується набір однакових операцій. Цей режим роботи ТЗ називається тестовим режимом. Наприклад, для окремих блоків персонального комп'ютера (ПК) використовуються наступні тест-режими: для монітора використовується режим відображення «точка через точку»; для жорстких магнітних дисків використовується чергування записи і читання «одиниць»; для клавіатури нажата клавіша.

Таким чином, вдосконалення підходів до захисту інформації від витоку по каналу ПЕМВН наразі є актуальною задачею.

Метою роботи є підвищення ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання відносно інформативного сигналу.

Постановка задачі:

• проаналізувати канали витоку інформації при експлуатації персональних комп’ютерів;

• провести аналіз існуючих підходів до захисту інформації від витоку по каналу побічних електромагнітних випромінювань;

• запропонувати підхід до захисту інформації від витоку по каналу ПЕМВН монітора з використанням імітаційних та маскуючих завад;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Канали витоку інформації при експлуатації ПК

1.1.1 Види і природа каналів витоку інформації при експлуатації ПК

При розгляді технічних каналів витоку інформації слід окремо зупиниться на такому актуальному питанні, як канали витоку інформації, що утворюються при експлуатації персональних електронно-обчислювальних машин (ПЕОМ), або персональних комп'ютерів (ПК) [1-9].

З точки зору захисту інформації ці технічні пристрої є прикладом для вивчення практично всіх каналів витоку інформації – починаючи від радіоканалу і закінчуючи матеріально-речовим. Враховуючи роль, яку відіграють ПЕОМ у сучасному суспільстві взагалі, а також тенденцію до повсюдного використання ПЕОМ для обробки інформації з обмеженим доступом зокрема, це питання є актуальним.

Як відомо, сучасні ПЕОМ можуть працювати як незалежно один від одного, так і взаємодіючи з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, але й глобальними [1, 3-7].

З урахуванням цього фактора, повний перелік тих ділянок, в яких можуть знаходитися дані, які підлягають захисту, може мати наступний вигляд:

• безпосередньо в оперативній або постійної пам'яті ПЕОМ;

• на знімних магнітних, магнітооптичних, лазерних та інших носіях;

• на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери тощо);

• на екранах пристроїв відображення (дисплеї, монітори, консолі);

• у пам'яті пристроїв вводу / виводу (принтери, сканери);

• в пам'яті керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Канали витоку інформації утворюються як при роботі ЕОМ, так і в режимі очікування. Джерелами таких каналів є:

• електромагнітні поля;

• струми, які наводяться, і напруги в провідних системах (живлення, заземлення, з'єднання);

• перевипромінювання оброблюваної інформації на частотах паразитної генерації елементів і пристроїв технічних засобів (ТЗ) ЕОМ;

• перевипромінювання оброблюваної інформації на частотах контрольно-вимірювальної апаратури (КВА).

Крім цих каналів, обумовлених природою процесів, що протікають в ПЕОМ та їх технічними особливостями, в ПЕОМ, які поставляються на ринок, можуть навмисне створюватися додаткові канали витоку інформації. Для утворення таких каналів може використовуватися:

• розміщення в ПЕОМ закладок на мову або оброблювану інформацію (замаскіровка під будь-які електронні блоки);

• встановлення в ПЕОМ радіомаячків;

• навмисне застосування таких конструктивно-схемних рішень, які призводять до збільшення електромагнітних випромінювань в певній частині спектра;

• установка закладок, що забезпечують знищення ПЕОМ ззовні (схемні рішення);

• установка елементної бази, що виходить з ладу.

Крім того, класифікацію можливих каналів витоку інформації в першому наближенні можна провести на підставі принципів, відповідно до яких обробляється інформація, що отримується з можливого каналу витоку. Передбачається три типи обробки: людиною, апаратурою, програмою. Відповідно з кожним типом обробки всілякі канали витоку також розбиваються на три групи. Щодо ПЕОМ, групу каналів, в яких основним видом обробки є обробка людиною, складають наступні можливі канали витоку:

• розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);

• читання інформації з екрану сторонньою особою;

• читання інформації з залишених без нагляду паперових роздруківок.

У групі каналів, в яких основним видом обробки є обробка апаратури, можна виділити наступні можливі канали витоку:

• підключення до ПЕОМ спеціально розроблених апаратних засобів, які забезпечують доступ до інформації;

• використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів ПЕОМ.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі канали витоку:

• несанкціонований доступ програми до інформації;

• розшифровка програмою зашифрованої інформації;

• копіювання програмою інформації з носіїв;

• блокування або відключення програмних засобів захисту.

При перехопленні інформації з ПЕОМ використовується схема, представлена на рис. 1.1.

При цьому технічному контролю повинні піддаватися наступні потенційні канали витоку інформації:

• побічні електромагнітні випромінювання в діапазоні частот від 10 Гц до 100 МГц;

• наводки сигналів в ланцюгах електроживлення, заземлення і в лініях зв'язку;

• небезпечні сигнали, що утворюються за рахунок електроакустичних перетворень, які можуть відбуватися в спеціальній апаратурі контролю інформації (ці сигнали повинні контролюватися в діапазоні частот від 300 Гц до 3,4 кГц);

• канали витоку інформації, що утворюються в результаті впливу високочастотних електромагнітних полів на різні дроти, які знаходяться в

приміщенні і можуть, таким чином, стати приймальною антеною. У цьому випадку перевірка проводиться в діапазоні частот від 20 кГц до 100 МГц.

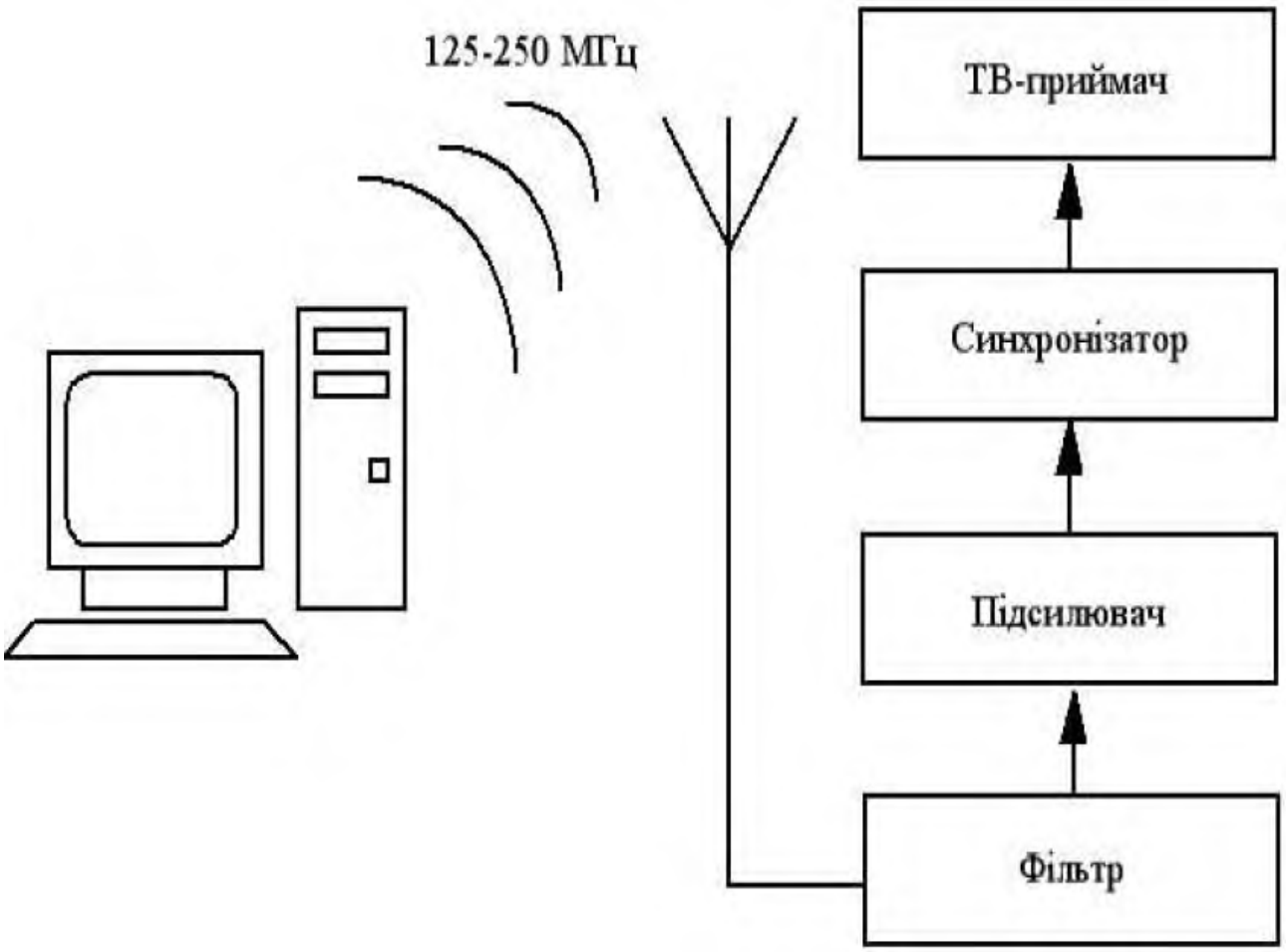

Рисунок 1.1 – Схема перехопленні інформації з ПЕОМ

Найбільш небезпечним каналом витоку є дисплей, оскільки з точки зору захисту інформації він є найслабшою ланкою в обчислювальній системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів керування обладнання, яке забезпечує генерацію зображення [1-9].

Схеми адаптера формують сигнали, що визначають інформацію, яка відображається на екрані. Для цього в усіх відеосистемах мається відеобуфер. Він представляє собою область оперативної пам'яті, яка призначена тільки для зберігання тексту або графічної інформації, виведеної на екран. Основна функція відео системи (ВС) полягає в перетворенні даних з відеобуфера в

керуючі сигнали дисплея, за допомогою яких на його екрані формується зображення. Ці сигнали й намагаються перехопити.

1.1.2 Аналіз можливості витоку інформації через побічні електромагнітні випромінювання

При проведенні аналізу можливості витоку інформації необхідно враховувати такі особливості радіотехнічного каналу витоку з засобів цифрового електронної техніки [1-3, 8]:

1. Для відновлення інформації мало знати рівень побічних електромагнітних випромінювань (ПЕМВ), потрібно знати їх структуру.

2. Оскільки інформація в цифрових засобах електронної техніки переноситься послідовностями прямокутних імпульсів, то оптимальним приймачем для перехоплення ПЕМВ є виявник (важливий сам факт наявності сигналу, а відновити сигнал просто, тому що форма його відома).

3. Не всі ПЕМВ є небезпечними точки зору реального витоку інформації. Як правило, найбільший рівень відповідає неінформативним випромінюванням (в ПЕОМ найбільший рівень мають випромінювання, породжувані системою синхронізації).

4. Наявність великої кількості паралельно працюючих електричних ланцюгів призводить до того, що інформативні та неінформативні випромінювання можуть перекриватися за діапазоном (взаємна завада).

5. Для відновлення інформації смуга пропускання розвідприймача повинна відповідати смузі частот сигналів, які перехоплюються. Імпульсний характер інформаційних сигналів призводить до різкого збільшення смуги пропускання приймача і, як наслідок, до збільшення рівня власних і наведених шумів.

6. Періодичне повторення сигналу призводить до збільшення можливої дальності перехоплення.

7. Використання паралельного коду у більшості випадків робить практично неможливим відновлення інформації при перехопленні ПЕМВ.

1.1.3 Засоби і методи забезпечення захисту інформації від витоку через побічні електромагнітні випромінювання

Класифікація засобів і методів захисту інформації (ЗІ), що обробляється засобами цифрової електронної техніки, від витоку через ПЕМВ наведена на рис. 1.2 [1-3, 8-20].

Електромагнітне екранування приміщень в широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат, постійного контролю і не завжди можливо з естетичних і ергономічних міркувань.

Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ здійснюється організаціями, що мають відповідні ліцензії. Використовуючи різні радіопоглинаючі матеріали та схемотехнічні рішення, за рахунок доопрацювання вдається істотно знизити рівень випромінювань. Вартість такого доопрацювання залежить від радіуса необхідної зони безпеки і становить від 20% до 70% від вартості ПЕОМ.

Криптографічне закриття інформації, або шифрування, є радикальним способом її захисту. Шифрування здійснюється або програмно, або апаратно за допомогою вбудованих засобів. Такий спосіб захисту виправдовується при передачі інформації на великі відстані по лініях зв'язку. Використання шифрування для захисту інформації, що міститься в службових сигналах цифрового електронного засобу, наразі неможливо.

Активне радіотехнічне маскування передбачає формування і випромінювання маскуючого сигналу в безпосередній близькості від засобу, який захищається. Розрізняють декілька методів активного радіотехнічного маскування: енергетичні методи; метод «синфазної завади»; статистичний метод.

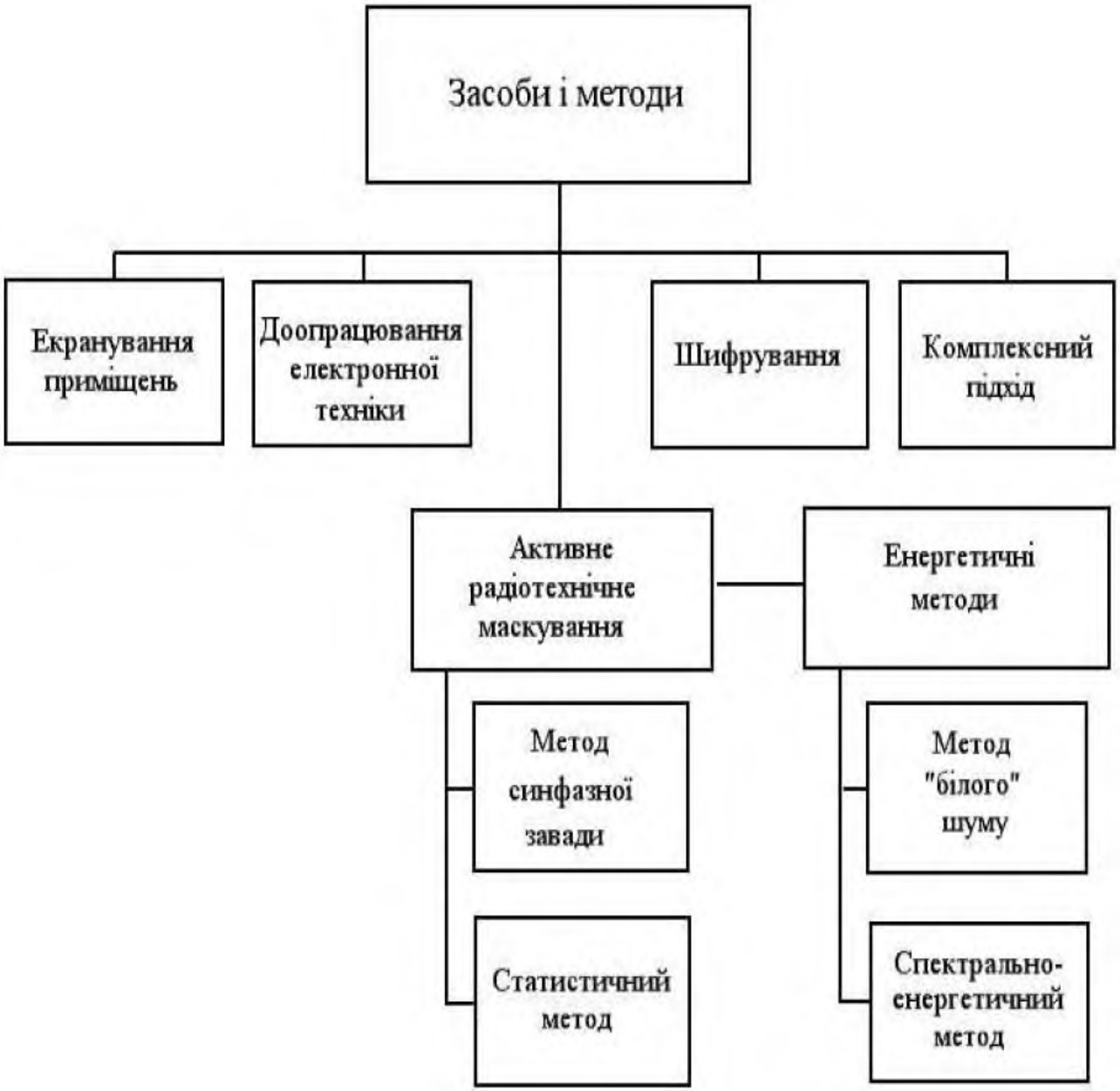

Рисунок 1.2 – Способи и методи ЗІ, оброблюваної засобами електронної техніки, від витоку по радіочастотному каналу

При енергетичному маскування методом «білого шуму» випромінюється широкосмуговий шумовий сигнал з постійним енергетичним спектром, що істотно перевищує максимальний рівень випромінювання електронної техніки. Наразі найбільш поширені пристрої ЗІ, що реалізують саме цей метод. До його недоліків слід віднести створення неприпустимих завад радіотехнічним й електронним засобам, що знаходяться поблизу від апаратури, яка захищається.

Спектрально-енергетичний метод полягає в генеруванні завади, що має енергетичний спектр, який визначається модулем спектральної щільності інформативних випромінювань техніки і енергетичним спектром атмосферної завади. Даний метод дозволяє визначити оптимальну заваду з обмеженою потужністю для досягнення необхідного співвідношення сигнал / завада на межі контрольованої зони.

Перераховані методи можуть бути використані для ЗІ як в аналоговій, так і в цифровій апаратурі. Як показник захищеності в цих методах використовується співвідношення сигнал / завада. Наступні два методи призначені для ЗІ в техніці, що працює з цифровими сигналами.

У методі «синфазної завади» в якості маскуючого сигналу використовуються імпульси випадкової амплітуди, що збігаються за формою і часу існування з корисним сигналом. У цьому випадку завада майже повністю маскує сигнал, прийом сигналу втрачає сенс, тому апостеріорні ймовірності наявності і відсутності сигналу залишаються рівними їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність похибки (ГПЙП) на кордоні мінімально допустимої зони безпеки. Однак через відсутність апаратури для безпосереднього вимірювання цієї величини пропонується перерахувати ГПЙП в необхідне співвідношення сигнал / завада.

Статистичний метод ЗІ полягає в зміні ймовірнісної структури сигналу, прийнятого розвідприймачем, шляхом випромінювання у спеціальний спосіб формованого маскуючого сигналу. В якості контрольованих характеристик сигналів використовуються матриці ймовірностей зміни станів. У разі оптимальної захищеності матриці ймовірностей зміни станів ПЕМВ буде відповідати еталонній матриці (всі елементи цієї матриці однакові). До переваг даного методу варто віднести те, що рівень формованого маскуючого сигналу не перевищує рівня інформативних ПЕМВ техніки. Однак статистичний метод має деякі особливості реалізації на практиці.

Відновлення інформації, яка міститься в ПЕМВ, найчастіше під силу тільки професіоналам, що мають у своєму розпорядженні відповідне

обладнання. Але навіть вони можуть бути безсилі у разі грамотного підходу до забезпечення ЗІ від витоку через ПЕМВ.

1.1.4 Механізм виникнення ПЕМВ засобів цифрової електронної техніки

Побічні електромагнітні випромінювання, що генеруються електромагнітними пристроями, зумовлені протіканням диференціальних та синфазних струмів [1, 11-14].

У напівпровідникових пристроях випромінюване електромагнітне поле утворюється при синхронному протіканні диференційних струмів в контурах двох типів. Один тип контуру формується провідниками друкованої плати або шинами, по яких на напівпровідникові прилади подається живлення. Площа контуру системи живлення приблизно дорівнює добутку відстані між шинами на відстань від найближчої логічної схеми до її розв'язуючого конденсатора. Інший тип контуру утворюється при передачі логічних сигналів від одного пристрою до іншого з використанням, як зворотний провідник, шини живлення. Провідники передачі даних спільно з шинами живлення формують динамічно працюючі контури, що з'єднують передавальні і приймальні пристрої.

Випромінювання, викликане синфазними струмами, обумовлено виникненням падінь напруги в пристрої, що створює синфазну напругу відносно «землі».

Як правило, в цифровому електронному обладнанні здійснюється синхронна робота логічних пристроїв. В результаті при перемиканні кожного логічного пристрою відбувається концентрація енергії у вузькі збіжні за часом імпульсні складові, при накладенні яких сумарні рівні випромінювання можуть виявитися вище, ніж може створити будь-який з окремих пристроїв.

Значний вплив на рівень ПЕМВ здійснюють способи з’єднань з від’ємною шиною джерела живлення або із «землею». Це з'єднання повинно мати дуже низький імпеданс, оскільки і друковані провідники на високих частотах (ВЧ) є скоріше дроселями, ніж коротко замкненими ланцюгами.

У багатьох випадках основними джерелами випромінювань є кабелі, по яких передається інформація в цифровому вигляді. Такі кабелі можуть розміщуватися всередині пристрою або з'єднувати їх між собою.

Застосування заземлюючих перемичок з обплетення кабелю або проводу, що характеризуються великими індуктивністю і активним опором для ВЧ завад і не забезпечують доброї якості заземлення екрана, призводить до того, що кабель починає діяти як передавальна антена.

Отже, побічні електромагнітні випромінювання – вид електромагнітних хвиль, що виникають в результаті роботи електричних приладів, зокрема протікання електричного струму по провіднику. Оскільки електромагнітні випромінювання є збуреннями електромагнітного поля, то при передачі конфіденційної інформації через локальну мережу або на монітор за допомогою кабелів, виникають електромагнітні випромінювання, які при попаданні на провідник (антену пристрою, що зчитує), вони породжують в ньому струм, схожий з оригіналом. Після дискретизації зчитаного сигналу можна відновити дані передавання через провідник, що може привести до витоку конфіденційної інформації. Найпростішим прикладом може бути рація. Потрапивши на потрібну частоту можна перехопити переговори.

Однак побічні електромагнітні випромінювання мають властивість затихати при видаленні від джерела мовлення і з певного моменту злитися з електромагнітним шумом. Небезпека даного мовлення полягає в тому, що буде існувати певні місця доступні зловмисникам для зчитування побічних електромагнітних випромінювань з достатнім співвідношенням сигнал / шум, щоб провести дискретизацію і скористатися каналом витоку інформації.

Однак сигнал може не тільки безпосередньо віщатися від різних провідників, по яким безпосередньо передається інформація, електромагнітні випромінювання можуть спокійно ретранслюватись через різні електропровідні матеріали, наприклад, система опалення або різна проводка. Коротка схема каналу ПЕМВН представлена на рис. 1.3 (ТЗР – Технічний засіб розвідки).

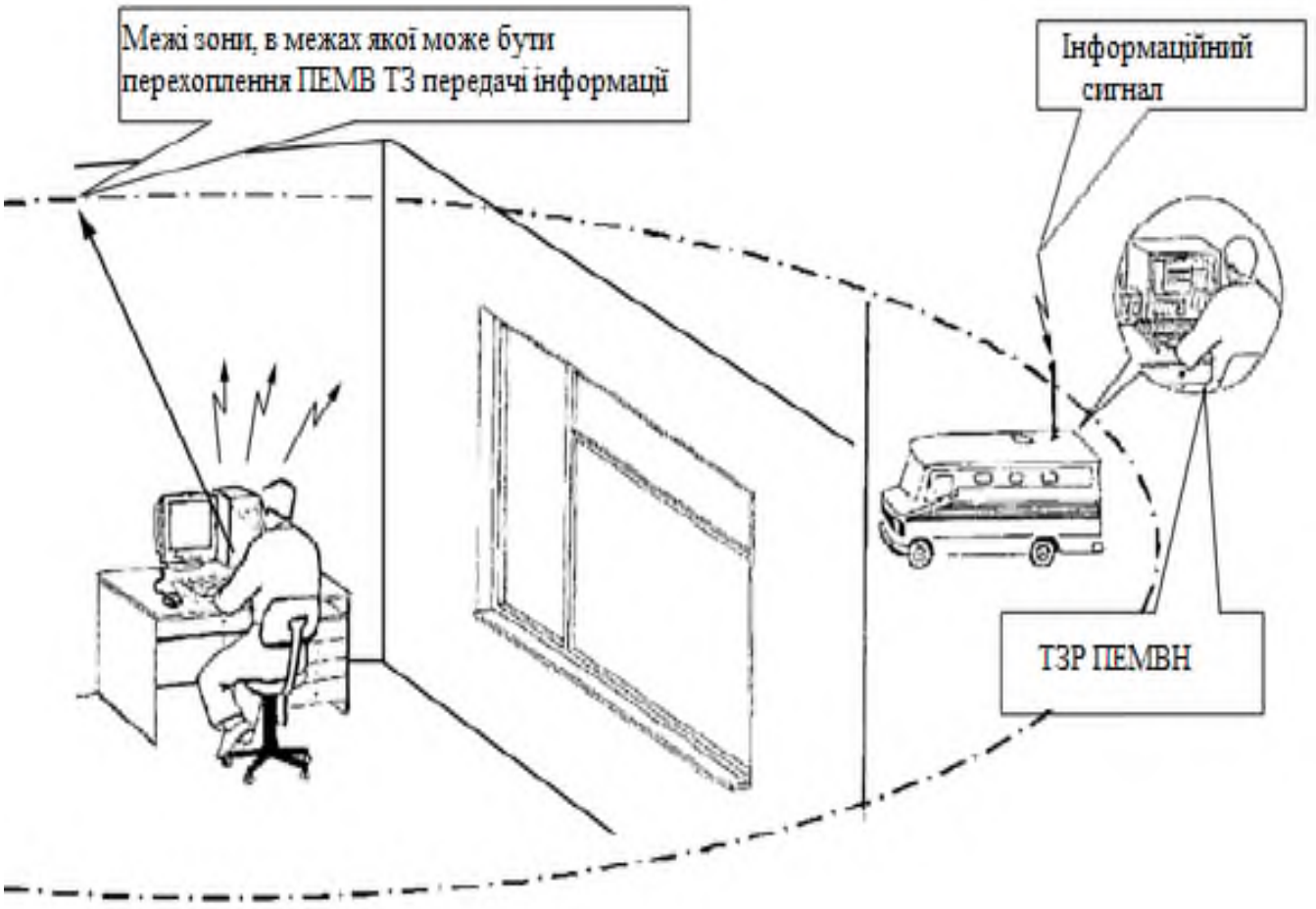

Рисунок 1.3 – Схема витоку інформації по каналу ПЕМВН

На рис. 1.3 введено такі скорочення: ТЗР – Технічний засіб розвідки.

Слід зазначити, що канал витоку інформації ПЕМВ є пасивним, тобто інформація не витече, якщо не буде передаватися через різні провідники / випромінювачі. Даний факт також вказує на те що помітити витік через даний канал інформації досить складно, навіть досвідченому фахівцеві зі спеціальним обладнанням. Також зловмисники можуть скористатися різними шкідливими програмами для штучного створення факту передачі інформації через провідники / випромінювачі для подальшого перехоплення. Подібні можливості впливу на інформацію усуваються шляхом ізолювання робочих станцій від глобальної мережі інтернет.

1.1.5 Технічна реалізація пристроїв маскування

Для здійснення активного радіотехнічного маскування ПЕМВ використовуються пристрої, що створюють шумове електромагнітне поле в діапазоні частот від декількох кГц до 1000 МГц із спектральним рівнем, що істотно перевищує рівні природних шумів та інформаційних випромінювань засобів ЕОМ. Для цих цілей використовуються малогабаритні надширокосмугові передавачі шумових маскуючих коливань ГШ-1000 і ГШ-К-1000, які є модернізацією виробу «Шатер-4» [1, 15-17].

Їх принцип дії базується на нелінійній стохастизації коливань, при якій шумові коливання реалізуються в автоколивальній системі не внаслідок флуктуацій, а за рахунок складної внутрішньої нелінійної динаміки генератора. Сформований генератором шумовий сигнал за допомогою активної антени випромінюється в простір.

Спектральна щільність випромінюваного електромагнітного поля рівномірно розподілена по частотному діапазону і забезпечує необхідне перевищення маскуючого сигналу над інформативним в задану кількість разів (як вимагають нормативні документи) на кордонах контрольованої зони об'єктів обчислювальної техніки 1-3 категорії по ефіру, а також наводить маскуючий сигнал на вихідні слабкострумові кола та на мережу живлення.

Статистичні характеристики сформованих генератором маскуючих коливань близькі до характеристик нормального білого шуму.

Генератор шуму ГШ-1000 виконаний у вигляді окремого блоку з живленням від мережі і призначений для загального маскування ПЕМВ ПЕОМ, комп'ютерних мереж і комплексів на об'єктах автоматизованих систем керування (АСК) та ЕОМ 1-3 категорій. Генератор ГШ-К-1000 виготовляється у вигляді окремої плати, що вбудовується у вільний роз'єм розширення системного блоку ПЕОМ і живиться напругою 12 В від загальної шини комп'ютера. У порівнювання з аналогічними за призначенням виробами генератори ГШ-1000 і ГШ К-1000 вигідно відрізняються підвищеним

коефіцієнтом якості маскуючого сигналу, формують електромагнітне поле з круговою поляризацією.

Існують два способи захисту від подібних атак на канал витоку інформації ПЕМВН: активний і пасивний метод.

Наочна схема, яка показує роботу даних методів показана на рис. 1.4.

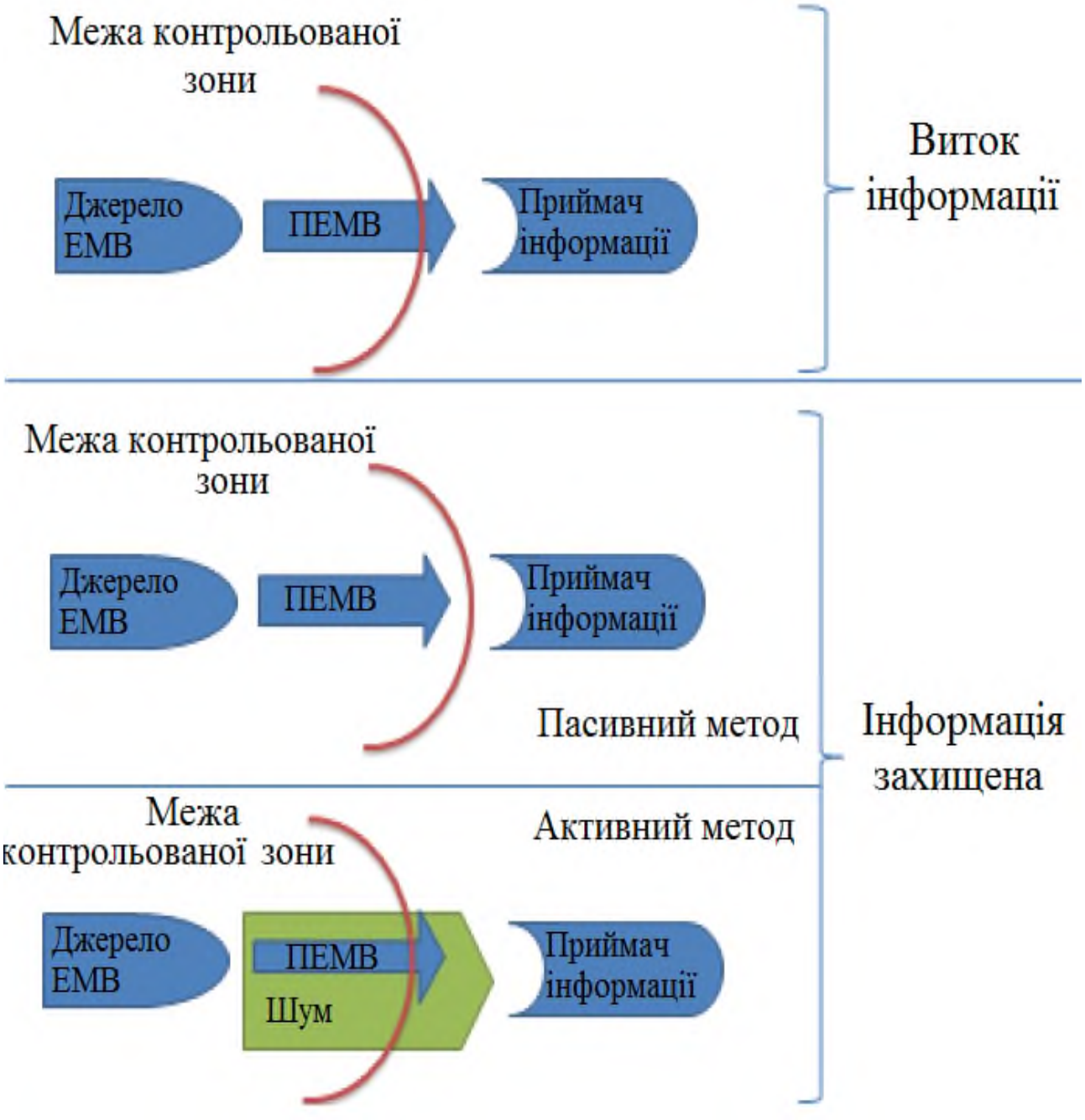

Рисунок 1.4 – Схема роботи методів захисту від витоку інформації по каналу ПЕМВН

Активний метод полягає в перекритті корисного сигналу більш потужним шумом. Даний метод захисту здійснюється апаратно, через спеціальні пристрої, так звані генератори шуму. Генератори шумів спеціально створюють потужні електромагнітні випромінювання, які не мають інформативної цінності і ускладнюють або роблять зовсім неможливим аналіз корисного сигналу щодо навколишнього шуму. Слід зазначити, що генератори шумів від побічних електромагнітних випромінювань мають свої недоліки, такі як:

- досить потужне джерело випромінювання не є корисним для здоров'я;
- наявність маскуючого сигналу говорить про наявність конфіденційної інформації;
- не можна гарантувати абсолютну захищеність інформації.

Пасивний метод полягає у зменшенні потужності самого випромінюваного сигналу. Здійснення подібного методу полягає в ізоляції випромінюючих провідників, пристроїв, а також периметра приміщення спеціальними матеріалами, що поглинають електромагнітні поля. Основною перевагою пасивного методу є те, що він усуває недоліки активного методу. Однак при застосуванні пасивного методу екранується абсолютно все, що призводить до досить серйозних витрат.

Отже, найбільш оптимальним у співвідношенні ціна / якість є комбінований підхід, з використанням активного і пасивного методу.

1.1.6 Оцінка рівня побічних електромагнітних випромінювань

Оцінка рівня ПЕМВ засобів цифрової електронної техніки може проводитися з точки зору відповідності цих рівнів наступним нормам і вимогам:

- санітарно-гігієнічні норми (ГОСТ 12.1.006-84);
- норми електромагнітної сумісності (ЕМС);
- норми і вимоги по ЗІ про витік через ПЕМВ.

Залежно від того, відповідність яким нормам потрібно встановити, використовуються ті чи інші прилади, методи та методики проведення вимірювань.

Слід зауважити, що норми на рівні ЕМВ з точки зору ЕМС істотно (на кілька порядків) суворіше санітарно-гігієнічних норм. Очевидно, що норми, методики і прилади, які використовуються в системі забезпечення безпеки життєдіяльності, не можуть бути використані при вирішенні завдань ЗІ.

Рівні ПЕМВ цифрової електронної техніки з точки зору ЕМС регламентовані цілим рядом міжнародних та вітчизняних стандартів (публікації CISPR – спеціального міжнародного комітету щодо радіозавад, ГОСТ 29216-91) встановлює такі норми напруженості поля радіозавад від обладнання інформаційної техніки (табл. 1.1).

Таблиця 1.1 – Норми напруженості поля радіозавад

Смуга частот, МГц	Квазіпікові норми, дБ (мВ/м)
30÷230	30 (31,6)
230÷1000	37 (70,8)

Рівні напруженості поля випромінюваних завад нормуються на відстані 10 або 30 м від джерела перешкод в залежності від того, де буде експлуатуватися обладнання (у житлових приміщеннях або в умовах промислових підприємств).

Наведені рівні випромінювання, що допускаються, достатні для перехоплення ЕМВ на значній відстані. Крім того, в діапазоні частот 0,15-30 МГц нормуються тільки визначені рівні напруги завад на мережевих клемах обладнання і не нормується напруженість поля радіозавад. Дані норми при серійному випуску виконуються з деякою ймовірністю.

Таким чином, відповідність ПЕМВ засобів цифрової електронної техніки нормам на ЕМС не може бути гарантією збереження конфіденційності інформації, що обробляється за допомогою цих засобів. Однак високий ступінь стандартизації методик і апаратури вимірювання рівня ЕМВ при вирішенні

завдань оцінки ЕМС робить можливим (з урахуванням деяких особливостей) використання їх при вирішенні завдань ЗІ. Основні характеристики вимірювальної апаратури, що використовується:

• діапазон робочих частот – 9 МГц ÷ 1000 МГц;

• можливість зміни смуги пропускання;

• наявність детекторів квазіпікового, пікового, середнього і середньоквадратичного значень;

• можливість слухового контролю сигналу, що має амплітудну і частотну модуляцію;

• наявність виходу проміжної частоти і виходу на осцилограф;

• наявність комплекту стандартних калібрувальних антен.

Прилади, які використовуються на практиці для визначення ЕМС, перераховані в табл. 1.2.

Таблиця 1.2 – Прилади, які використовуються для визначення ЕМС

Прилад	Діапазон робочих частот, МГц	Виробник
SMV-8	26÷1000	Messelecktronik, Німеччина
SMV-11	0,009÷30	-//-
SMV-41	0,009÷1000	-//-
„Элмас”	30÷1300	ПО „Вектор”, С.-Петербург
ESH-2	0,009÷30	RHODE&SHWARZ, Німеччина
ESV	20÷1000	-//-
ESH-3	0,009÷30	-//-
ESVP	20÷1300	-//-

Сучасні вимірювальні приймачі (ЭЛМАС, ESH-3, ESVP, SMV-41) автоматизовані і обладнані інтерфейсами за стандартом IEEE-488, що дає можливість управляти режимами роботи приймача за допомогою зовнішньої ЕОМ, а передавати виміряні значення на зовнішню ЕОМ для їх обробки.

Крім перерахованих в табл. 1.2 приладів, для вимірювання побічних ЕМВ засобів цифрового електронної техніки можуть бути використані аналізатори спектру в комплекті з вимірювальними антенами (табл. 1.3).

Таблиця 1.3 – Аналізатори спектру

Прилад	Діапазон робочих частот, МГц	Діапазон вимірювання	Виробник
СЧ-82	$3 \cdot 10^{-4} \div 1500$	1мВ÷3В	СНД
СКЧ-84	$3 \cdot 10^{-5} \div 110$	70нВ÷2,2В	-//-
СЧ-85	$1 \cdot 10^{-4} \div 39{,}6 \cdot 10^{3}$	1мВ-3В $10^{-16} \div 10^{-2}$ Вт	-//-
РСКЧ-86	25÷1500	40нВ÷2,8В $3 \cdot 10^{-17} \div 1$ Вт	-//-
РСКЧ-87	1000÷4000	$10^{-12} \div 0{,}1$ Вт	-//-
РСКЧ-90	1000÷17440	$10^{-12} \div 0{,}1$ Вт	-//-
HP8568B	$1 \cdot 10^{-4} \div 1500$	$10^{-16} \div 1$ Вт	Hewlett-Packard, США
HP71100A	$1 \cdot 10^{-4} \div 2900$	$10^{-16} \div 1$ Вт	-//-
HP8566B	$1 \cdot 10^{-4} \div 22000$	$10^{-16} \div 1$ Вт	-//-
2756P	$1 \cdot 10^{-2} \div 3{,}25 \cdot 10^{3}$	$10^{-16} \div 1$ Вт	Tektronix, США
2380-2383	$1 \cdot 10^{-4} \div 4200$	$10^{-18} \div 1$ Вт	Marconi Instruments, Англія
FSA	$1 \cdot 10^{-4} \div 2000$	$10^{-17} \div 1$ Вт	RHODE&SHWARZ, ФРН
FSB	$1 \cdot 10^{-4} \div 5000$	$10^{-17} \div 1$ Вт	-//-

Сучасні аналізатори спектра з вбудованими мікропроцесорами дозволяють аналізувати різні параметри сигналів. Є можливість об'єднання аналізатора спектра за допомогою інтерфейсу з іншими вимірювальними приладами і зовнішньою ЕОМ в автоматизовані вимірювальні системи.

В процесі обробки можуть виконуватися такі функції: пошук екстремальних значень сигналу; відбір сигналів, рівень яких перевищує заданий зсув по осі частот для оптимальної реєстрації сигналу. Вбудований мікропроцесор забезпечує обробку амплітудно-частотних спектрів, а також оптимізацію часу вимірювання і роздільної здатності для розглянутого інтервалу частот.

На відміну від задач ЕМС, де потрібно визначити максимальний рівень випромінювання в заданому діапазоні частот, при вирішенні задач ЗІ потрібно

визначити рівень випромінювання в широкому діапазоні частот, відповідному інформативному сигналу. Тому оцінка рівня випромінювань при вирішенні задач ЗІ повинна починатися з аналізу технічної документації та відбору електричних ланцюгів, за якими можна передавати інформацію з обмеженим доступом. Необхідно провести аналіз і визначити характеристики небезпечних сигналів:

• використовуваний код: послідовний, паралельний;

• періодичне повторення сигналу: є, немає;

• часові характеристики сигналу;

• спектральні характеристики сигналу.

Після цього можна приступати безпосередньо до визначення рівнів інформативних ПЕМВ.

1. Метод оціночних розрахунків. Згідно даного методу, визначаються елементи конструкції обладнання, в яких циркулюють небезпечні сигнали, складаються моделі, проводиться оцінний розрахунок рівня випромінювань. Цей метод добре реалізується за наявності програмного забезпечення для ЕОМ у вигляді експертної системи, що містить банк моделей випромінювачів.

2. Метод примусової (штучної) активізації. Згідно даного методу, активізується (програмно або апаратно) канал (одне небезпечне коло) еталонним сигналом, який дозволяє ідентифікувати випромінювання, і вимірюються рівні ПЕМВ. Для вимірювань в даному методі можуть бути використані вимірювальні приймачі та аналізатори спектра.

3. Метод еквівалентного приймача. Згідно даного методу, спочатку синтезується приймач для відновлення інформації, що міститься в ПЕМВ. Після калібрування такий приймач може бути використаний для вимірювання рівнів інформаційних випромінювань.

Кожен з методів має свої переваги і недоліками. Наразі найбільш прийнятним для практики методом оцінки рівнів інформативних ПЕМВ є метод примусової активізації.

1.2 Існуючі підходи до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень

Ефективним способом запобігання витоку інформації з ЗОТ є активна радіотехнічна маскування побічних електромагнітних випромінювань за допомогою генераторів шумових сигналів (ГШС).

З існуючих підходів до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень відомий генератор шумових сигналів [21], принципова електрична схема якого показана на рис. 1.5.

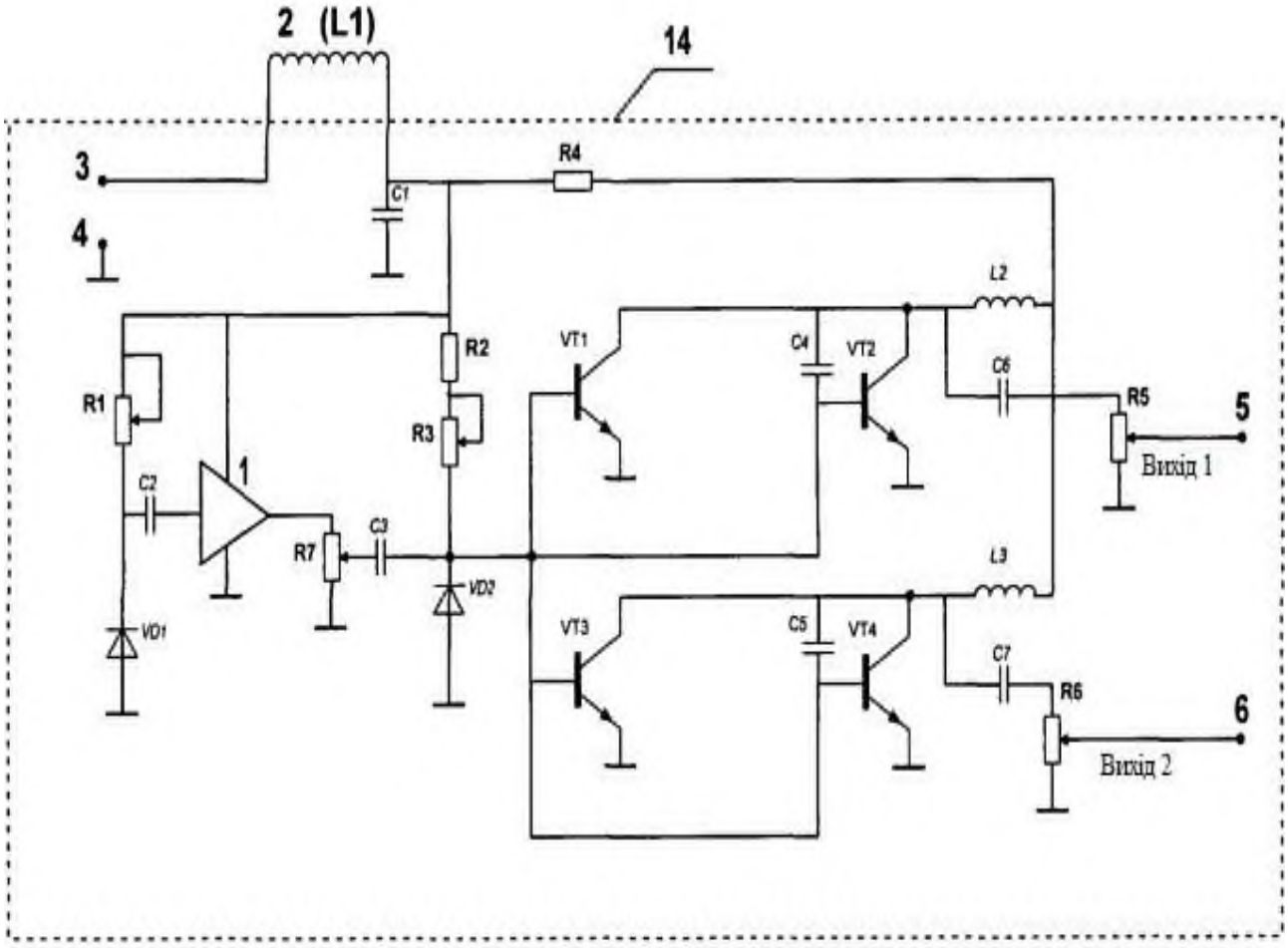

Рисунок 1.5 – Принципова електрична схема відомого генератора шумових сигналів.

Відомий ГШС [21] містить контакти для підключення джерела живлення, друковану плату 14, яка містить перший і другий автогенератори, третій і

шостий змінні резистори, четвертий, п'ятий і сьомий конденсатори. Причому кожен з автогенераторів виконаний на двох транзисторах за схемою із загальним емітером, а бази перших транзисторів першого і другого автогенераторів і бази других транзисторів першого і другого автогенераторів з'єднані. Другий постійний резистор і третій змінний резистор, включений в ланцюг обмеження струму баз транзисторів, четвертий постійний резистор включений в ланцюг обмеження струмів колекторів транзисторів, а в ланцюзі регулювання рівня генерованого шумового сигналу в якості розділового включений сьомий конденсатор з послідовно з'єднаним з ним шостим змінним резистором. Напівпровідниковий діод приєднаний до баз транзисторів і через послідовно з'єднані обмежувальні резистори до позитивної клеми джерела живлення, а анод діода – до корпусу. В ланцюг живлення генератора шумових сигналів встановлена котушка індуктивності з розподіленими параметрами, приєднана до третього контакту ГШС і обмежувального резистору R4, резисторам R1, R2, контакту живлення підсилювача і конденсатору C1 (рис. 1.5).

Генератор шумових сигналів може містити лавинно-пролітний діод, конденсатори C2 і C3, підсилювач I, змінні резистори R1 і R7, при цьому утворюють схему додаткового формування низькочастотних шумових сигналів. Генератор шумових сигналів може містити індуктивності L2 і L3, конденсатор C6, змінний резистор R5, контакти виходу 1 і виходу 2, при цьому генератор шумових сигналів може мати регульовані виходи сигналів, контакти 5 і 6 (рис. 1.5).

Генератор шумових сигналів може бути виконаний на друкованій платі в двох варіантах виконань, для установки в вільний слот шини PCI, для установки в корпус, який встановлюється на кабель DVI.

Технічним результатом, що забезпечується наведеною сукупністю ознак ГШС, є розширення спектру вихідного шумового сигналу в область низьких і високих частот від 0,5 кГц до 2700 МГц, підвищення рівномірності

спектральної щільності потужності шумового сигналу, можливість регулювання рівнів шумових сигналів.

Недоліками відомого генератора шумових сигналів [21] є:

• висока вартість і складність технічної реалізації пристрою;

• неоптимальне використання маскуючих завад у зв'язку з їх надмірними значеннями рівня і ширини спектра для захисту інформації, яка циркулює в каналах передачі даних ТЗ, що має в своєму складі відеосистему, від витоку по каналу ПЕМВН.

Також з існуючого рівня техніки відомий спосіб захисту оброблюваної інформації засобами обчислювальної техніки шляхом зашумлення інформативних побічних електромагнітних випромінювань і наведень, пристрій захисту інформації для реалізації способу [22], що полягає у формуванні широкосмугового шумового сигналу і змішуванні його з додатковим сигналом, при подальшому використанні отриманого в результаті змішування сигналу в якості маскуючого широкосмугового шумового сигналу, в якості додаткового сигналу використовують тактовий сигнал системи обробки інформації (СОІ), формування маскуючого широкосмугового шумового сигналу здійснюють використанням двох шумових сигналів з розподілом частотного спектра і подальшим підсумовуванням сигналів по електромагнітному полю.

Схема пристрою захисту оброблюваної інформації засобами обчислювальної техніки шляхом зашумлення інформативних побічних електромагнітних випромінювань і наведень показана на рис. 1.6 [22].

Пристрій є двоканальним генератором широкосмугового шумового сигналу і містить в своєму складі: друковану плату 14 з елементами схеми, контакти електроживлення К1 і К2, вимикач В1, джерело шумового сигналу нижніх частот 1, розділювальний конденсатор С1, широкосмуговий підсилювач 2, розділювальний конденсатор С2, змінний резистор R1, розділювальний конденсатор С3, фільтр нижніх частот 3, розділювальний конденсатор С4, широкосмуговий підсилювач 4, розділювальний конденсатор С5, широкосмуговий підсилювач 5, розділювальний конденсатор С6, резистор

навантаження R2, вихідний високочастотний роз'єм Р1, детектор сигналів 6, логічний елемент 2І-НЕ 7, випромінювач звуку з вбудованим генератором ЕР2, джерело шумового сигналу верхніх частот 9, розділювальний конденсатор С7, широкосмуговий підсилювач 10, розділювальний конденсатор С8, змінний резистор R3, розділювальний конденсатор С9, фільтр верхніх частот 11, розділювальний конденсатор С10, широкосмуговий підсилювач 12, розділювальний конденсатор С11, широкосмуговий підсилювач 13, розділювальний конденсатор С12, резистор навантаження R4, вихідний високочастотний роз'єм Р2, детектор сигналів 8, індикаторний світлодіод HL1 з резистором R5 (рис. 1.6).

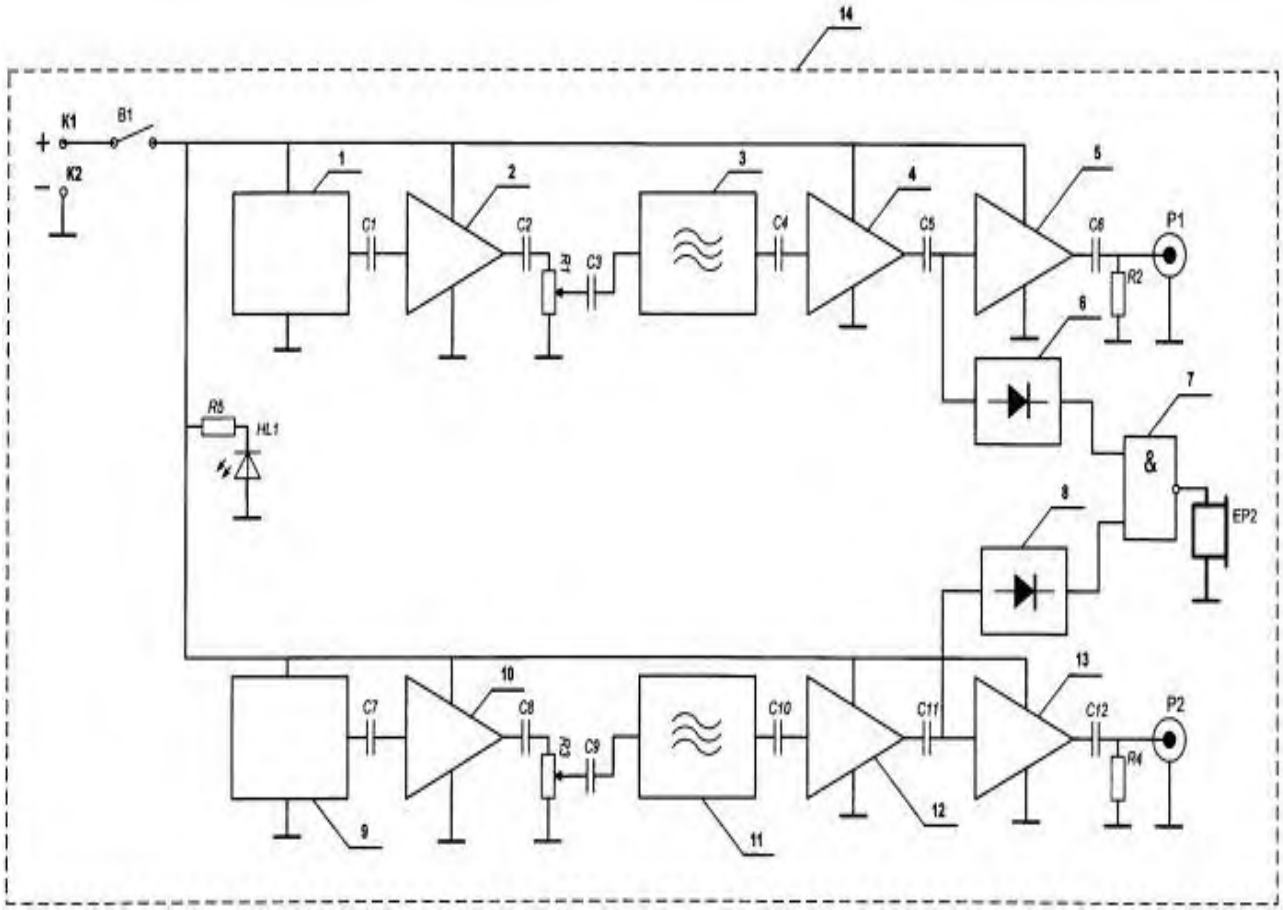

Рисунок 1.6 – Схема відомого пристрою захисту оброблюваної інформації ЗОТ шляхом зашумлення інформативних побічних ЕМВН

Недоліками відомого способу захисту оброблюваної інформації засобами обчислювальної техніки шляхом зашумлення інформативних побічних електромагнітних випромінювань і наведень [22] є:

• висока вартість і складність технічної реалізації пристрою;

• неоптимальне використання маскуючих завад в зв'язку з їх надмірними значеннями рівня і ширини спектра для захисту інформації, яка циркулює в каналах передачі даних ТЗ, що має в своєму складі відеосистему, від витоку по каналу ПЕМВН.

Найбільш близьким до розробленого підходу є відомий спосіб захисту засобів обчислювальної техніки (ЗОТ) від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [23], обраний в якості прототипу.

Спосіб полягає в формуванні маскуючого сигналу шляхом утворення власних неінформативних побічних електромагнітних випромінювань, що створюються типовими вузлами і пристроями ПК під керуванням спеціального програмного забезпечення і забезпечують приховування інформативних сигналів випромінювання.

Зазначений підхід полягає у формуванні маскуючого сигналу, а також в тому, що формують N файлів, вміст яких не потрібно захищати, потім першу частину файлів із загального списку, відповідну 0,5N, записують на перший цифровий накопичувач, а другу частину файлів із загального списку, відповідну 0,5N – на другий цифровий накопичувач. Після цього з першого цифрового накопичувача зчитують файл, обраний зі списку за випадковим законом, і записують його на другий цифровий накопичувач і одночасно з другого цифрового накопичувача зчитують файл, обраний зі списку за випадковим законом, і записують його на перший цифровий накопичувач. Запис і зчитування файлів здійснюють багаторазово протягом часу, необхідного для маскування інформативного сигналу, при цьому одні й ті ж файли багаторазово записують на одне й те ж місце в цифрових накопичувачах для виконання умови неперевищення сумарного розміру всіх файлів, що копіюються, розміру

пам'яті цифрового накопичувача, на якому записані сформовані файли, при проходженні яких по з'єднувальним лініям типових вузлів і блоків засобів обчислювальної техніки виникають власні неінформативні побічні електромагнітні випромінювання. Збіг спектра інформативного сигналу з максимальною інтенсивністю спектра неінформативних побічних електромагнітних випромінювань забезпечують шляхом корекції огинаючої спектра неінформативних побічних електромагнітних випромінювань за рахунок зміни структури бітової послідовності в формованих файлах.

Схема розміщення обладнання для реалізації відомого способу захисту засобів обчислювальної техніки (ЗОТ) від витоку інформації по каналу ПЕМВН показана на рис. 1.7.

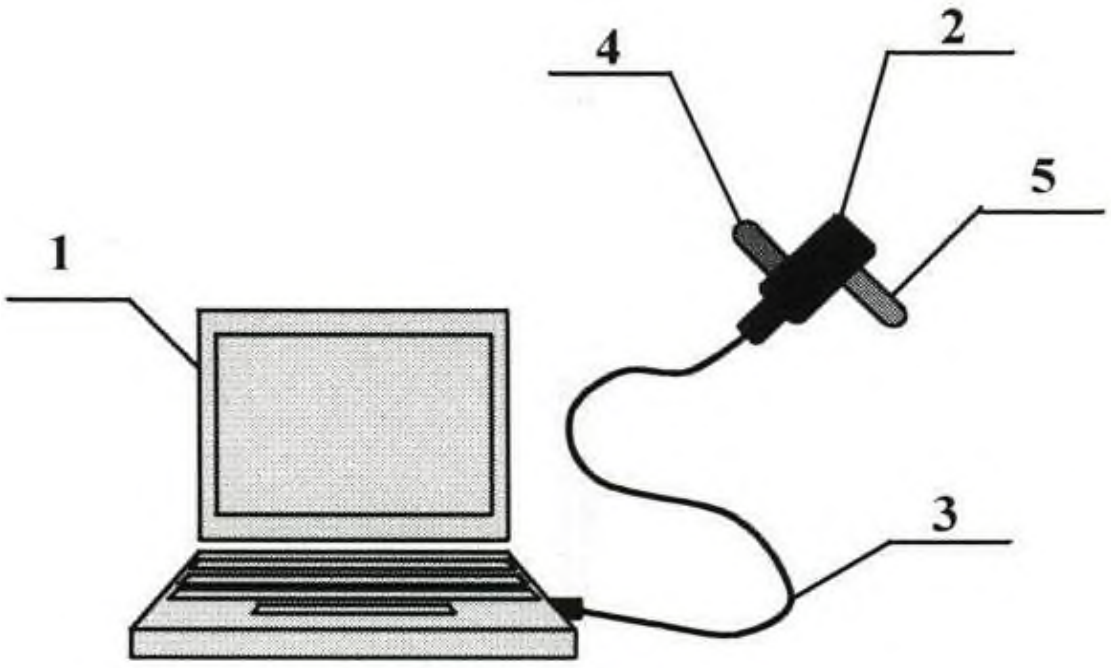

Рисунок 1.7 – Схема розміщення обладнання для реалізації способу-прототипу захисту ЗОТ від витоку інформації по каналу ПЕМВН

На рис. 1.7 показані ноутбук 1, з'єднаний з USB-концентратором 2 за допомогою неекранованого кабелю 3, спеціальний флеш-накопичувач (F1) 4 і флеш-накопичувач (F2) 5 для запам'ятовування неінформативних файлів.

Переваги відомого способу-прототипу захисту засобів обчислювальної техніки від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [23] полягають в наступному:

• реалізація способу не вимагає вирішення складних технічних проблем, пов'язаних з формуванням маскуючих сигналів в ЗОТ;

• реалізація способу не вимагає конструктивних змін вузлів і блоків ЗОТ, а спеціальне програмне забезпечення для формування маскуючих завад просте у використанні і має інтуїтивно зрозумілий інтерфейс;

• спосіб не використовує ключової інформації і тому не втрачає своєї ефективності при отриманні її зловмисником;

• реалізація способу здійснюється при незначних фінансових витратах, які визначаються в основному витратами на придбання двох флеш-накопичувачів і USB-концентратора в торговій мережі;

• в умовах функціонування ЗОТ спосіб забезпечить підвищення рівня захищеності інформації від витоку за рахунок ПЕМВН.

Недоліками способу захисту засобів обчислювальної техніки від витоку інформації по каналу ПЕМВН [23] (прототипу) є:

• участь оператора в процесі технічного захисту інформації;

• відсутність синхронізації між імітаційною завадою і інформативним сигналом;

• висока вартість і складність технічної реалізації пристрою;

• підхід може бути використаний для захисту інформації циркулюючої тільки в одному пристрої вводу / виводу інформації (каналі передачі даних) – USB.

1.3 Висновок. Постановка задачі

В розділі проаналізовано канали витоку інформації при експлуатації персональних комп’ютерів. Встановлено, що найнебезпечнішим каналом витоку є дисплей, оскільки з точки зору захисту інформації він є найслабшою

ланкою в обчислювальній системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів керування обладнання, яке забезпечує генерацію зображення.

Встановлено, що наразі існують два способи захисту від витоку на канал ПЕМВН: активний і пасивний метод. Активний метод полягає в перекритті корисного сигналу більш потужним шумом, але має певні недоліки: досить потужне джерело випромінювання не є корисним для здоров'я; наявність маскуючого сигналу говорить про наявність конфіденційної інформації; не можна гарантувати абсолютну захищеність інформації. Пасивний метод полягає у зменшенні потужності самого випромінюваного сигналу. Основною перевагою пасивного методу є те, що він усуває недоліки активного. Однак при застосуванні пасивного методу екранується абсолютно все, що призводить до досить серйозних витрат. Отже, найбільш оптимальним у співвідношенні ціна / якість є комбінований підхід, з використанням активного і пасивного методу.

В розділі проаналізовано існуючі підходи до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень. Встановлено, що недоліки відомих генератора шумових сигналів [21] та способу захисту оброблюваної інформації засобами обчислювальної техніки шляхом зашумлення інформативних побічних електромагнітних випромінювань і наведень [22], такі:

- висока вартість і складність технічної реалізації пристроїв;

- неоптимальне використання маскуючих завад в зв'язку з їх надмірними значеннями рівня і ширини спектра для захисту інформації, яка циркулює в каналах передачі даних ТЗ, що має в своєму складі відеосистему, від витоку по каналу ПЕМВН.

Встановлено, що недоліками відомого способу захисту засобів обчислювальної техніки від витоку інформації по каналу ПЕМВН [23] (прототипу) є:

- участь оператора в процесі технічного захисту інформації;

- відсутність синхронізації між імітаційною завадою і інформативним сигналом;

- висока вартість і складність технічної реалізації пристрою;

- підхід може бути використаний для захисту інформації циркулюючої тільки в одному пристрої вводу / виводу інформації (каналі передачі даних) – USB.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до захисту інформації від витоку по каналу ПЕМВН монітора з використанням імітаційних та маскуючих завад;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад

Запропонований підхід відноситься до техніки зв'язку і може використовуватися для захисту інформації, що обробляється технічним засобом, що мають в своєму складі відеосистему, яка функціонує на основі стандартів DVI, VGA, Display Port, HDMI і аналогічних, від витоку інформації по каналу ПЕМВН. Технічний результат полягає в усуненні впливу людського фактору на процес технічного захисту інформації від витоку по каналу ПЕМВН і в підвищенні ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання відносно інформативного сигналу. Для цього в підході, що полягає у формуванні ТЗ на додатковому порті вводу / виводу інформації, до якого підключено пристрій вводу / виводу інформації, структурованого неінформаційного сигналу, при цьому в якості порту вводу / виводу інформації, на якому ТЗ формує неінформаційний чотирьохканальний сигнал, використовується додатковий відеопорт ТЗ, в якості пристрою вводу / виводу інформації використовується пристрій захисту інформації.

Як відомо, до однієї з основних загроз безпеки інформації обмеженого доступу, що обробляється ТЗ, відноситься витік інформації по технічним каналам, під якою розуміється неконтрольоване поширення інформативного сигналу від його джерела через фізичне середовище до ТЗ, що здійснює перехоплення інформації.

Пристрої вводу / виводу інформації (канал передачі даних), при обробці ТЗ інформації, створюють побічне електромагнітне випромінювання (ПЕМВ), яке поширюється в ефірі і створює наводки на ланцюги заземлення та електроживлення, струмопровідні лінії і інженерно-технічні комунікації, що

виходять за межі контрольованої зони . Приймаючи і декодуючи ці сигнали, можна відновити інформацію, оброблювану ТЗ.

Як вже було сказано в розділі 1.1, найнебезпечним (з точки зору витоку інформації за рахунок ПЕМВН) режимом роботи ТЗ є вивід інформації на екран монітора.

Для захисту інформації від витоку по каналу ПЕМВН необхідно в точці можливого перехоплення інформативних сигналів зменшити відношення сигнал-шум, щоб унеможливити перехоплення, обробку та аналіз інформативних сигналів з метою отримання інформації. Це може бути досягнуто двома способами.

По-перше, зменшенням рівня інформативних сигналів в точці (місці) можливого перехоплення інформації. Здійснення пасивного методу полягає в екрануванні джерела випромінювання, вдосконаленні конструктивно-технологічного та схемотехнічного виконання, фільтрації сигналів в лініях, а також оснащення периметра приміщення спеціальними матеріалами, що поглинають електромагнітні поля.

По-друге, збільшенням рівня шуму в ефірі, ланцюгах заземлення та електроживлення, струмопровідних лініях і інженерно-технічних комунікаціях в точці (місці) можливого перехоплення інформації. Здійснення активного методу полягає в створенні за допомогою генератора шуму просторових широкосмугових електромагнітних завад в ефірі і лінійних завад в ланцюгах заземлення та електроживлення, струмопровідних лініях і інженерно-технічних комунікаціях, що виходять за межі контрольованої зони, що забезпечують перекриття інформаційних сигналів по рівню і смузі частот.

Використання маскуючих завад призводить до зменшення ймовірності правильного виявлення інформативного сигналу, зниження точності вимірювання його параметрів і збільшення ймовірності помилкової тривоги. Ефективність маскуючих завад залежить від часової і частотної структури, як завади, так і сигналу, а також від енергетичного співвідношення завади і сигналу на вході приймального пристрою.

Для захисту інформації від витоку по каналу ПЕМВН використовувати маскуючі завади надлишково, тому що:

• параметри сигналів (структура, тривалості, частоти), що протікають в каналах передачі даних ТЗ, і параметри ПЕМВН, відомі зловмиснику, оскільки канали передачі даних працюють на основі відкритих стандартів;

• маскуючі завади мають ширину спектра частот і рівні, що значно перевищують смугу і рівні, які зайняті інформативним сигналом;

• маскуючі завади можуть чинити негативний вплив, за параметрами електромагнітної сумісності, на функціонування радіозасобів.

Для захисту інформації від витоку по каналу ПЕМВН використовувати імітаційні завади, створені при використанні неінформаційних сигналу, сформованого ТЗ, достатньо, тому що:

• імітаційні завади містять неправдиву інформацію і наносять максимальний інформаційний збиток потенційному зловмиснику, оскільки імітаційні завади і інформативний сигнал синхронізовані між собою і мають однакові параметри;

• імітаційні завади і інформативні сигнали мають частотні енергетичні спектри, що взаємно перекриваються, та співмірні рівні інтенсивності і можуть бути реалізовані малопотужним передавачем завад.

• імітаційні завади надають мінімальний вплив на функціонування радіозасобів.

Технічним результатом, отриманим від впровадження запропонованого підходу є усунення впливу людського фактора на процес технічного захисту інформації від витоку по каналу ПЕМВН.

Додатковим технічним результатом є підвищення ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання щодо інформативного сигналу, зниження складності і вартості технічної реалізації пристрою і робіт з технічного захисту інформації, що обробляється ТЗ, від витоку по каналу ПЕМВН, розширення функціональних можливостей, що полягає в тому, що пристрій захисту

інформації крім імітаційних завад, що забезпечують захист інформації, яка циркулює в відеосистемі ТЗ, створює маскуючі завади з рівнем і шириною спектру достатніми для захисту інформації, яка циркулює в інших каналах передачі даних ТЗ, що відповідають за ввід / вивід інформації зокрема USB, PS/2, COM, LPT.

Технічний результат досягається за рахунок того, що у відомому підході, що полягає у формуванні ТЗ на додатковому порті вводу / виводу інформації, до якого підключено пристрій вводу / виводу інформації, структурованого неінформаційного сигналу, при проходженні якого по з'єднувальним лініям типових вузлів і блоків технічного засобу виникають власні неінформативні побічні електромагнітні випромінювання, що забезпечують приховування інформативних сигналів випромінювання від пристрою вводу / виводу інформації, підключеного до основного порту вводу / виводу інформації. Новим є те, що в якості порту вводу / виводу інформації, на якому ТЗ формує неінформаційний чотирьохканальний сигнал, використовується додатковий відеопорт ТЗ, як пристрій вводу / виводу інформації використовується пристрій захисту інформації, що є емулятором монітора , що визначається ТЗ як пристрій відеовідображення, що створює за допомогою системи випромінювання завад (СВЗ), імітаційні та маскуючі завади, які забезпечують приховування інформативних сигналів випромінювання, створюваних пристроєм відеовідображення, підключеного до основного відеопорту і інших каналів передачі даних відповідно.

Запропонований підхід до захисту інформації, що обробляється ТЗ, від витоку по каналу ПЕМВН є універсальним для всіх ТЗ, що мають в своєму складі відеосистему, і не вимагає участь оператора в процесі технічного захисту інформації.

Пристрій захисту інформації, що використовується в запропонованому підході, є індивідуальним засобом захисту для кожного окремого ТЗ, має просту конструкцію.

Відеоадаптер ТЗ використовується в якості джерела неінформаційного сигналу:

• програмне забезпечення, яке функціонує на ТЗ, періодично формує цифрове зображення, у якого колір кожного пікселя має випадкове значення;

• відеоадаптер перетворює зображення в чотирьохканальний сигнал (3 незалежні один від одного компоненти кольору і синхронізація) і виводить його на додатковий відеопорт, до якого підключено пристрій захисту інформації.

Пристрій захисту інформації, використовуючи неінформаційний чотирьохканальний сигнал, сформований відеоадаптером на додатковому відеопорті, створює імітаційні та маскуючі завади.

Ширина спектра і частоти завад, створених пристроєм захисту інформації, залежить від прошивки EDID (Extended display identification data, розширені ідентифікаційні дані дисплея), отриманої з основного пристрою відеовідображення в пристрої захисту інформації та цифрового зображення, сформованого програмою.

Рівень завад, створених пристроєм захисту інформації, залежить від конструктивно-технологічного та схемотехнічного виконання відеоадаптера і системи випромінювання завад в пристрої захисту інформації.

Імітаційні завади, забезпечують приховування інформативних сигналів, створюваних основним пристроєм відеовідображення в ефірі і наведень в ланцюгах заземлення та електроживлення, струмопровідних лініях і інженерно-технічних комунікаціях.

Імітаційні завади, створені пристроєм захисту інформації, і ПЕМВН від основного пристрою відеовідображення мають однакові параметри, тому що відеоадаптер формує на додатковому і основному портах синхронізований між собою сигнал, який має однакові параметри: структуру сигналу, тривалості імпульсів, період синхронізації, частоти сигналу, ширину спектра і амплітуду.

Маскуючі завади забезпечують перекриття інформативних сигналів, створюваних іншими каналами передачі даних ТЗ (USB, PS/2, COM, LPT) в

ефірі і наведень в ланцюгах заземлення та електроживлення, струмопровідних лініях і інженерно-технічних комунікаціях.

Для створення маскуючих завад під конкретний канал передачі даних може бути використано додатковий пристрій захисту інформації зі зміненою прошивкою EDID під конкретні частоти випромінювання.

Для реалізації запропонованого підходу запропоновано пристрій захисту інформації, схема якого зображена на рис. 2.1.

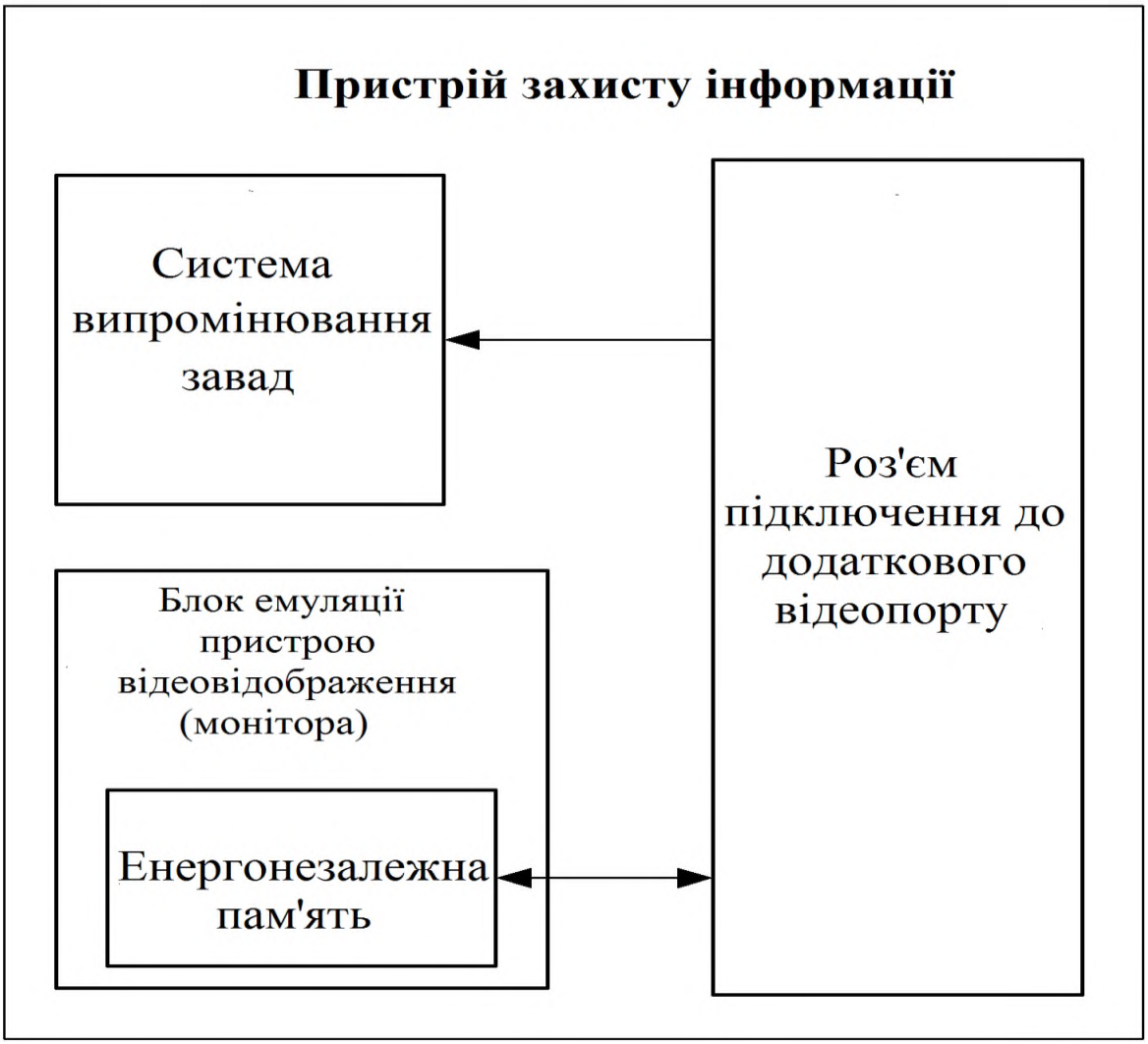

Рисунок 2.1 – Схема запропонованого пристрою захисту інформації, що обробляється ТЗ, від витоку по каналу ПЕМВН монітора

Приклад підключення ТЗ до пристрою захисту інформації проілюстрований на рис. 2.2.

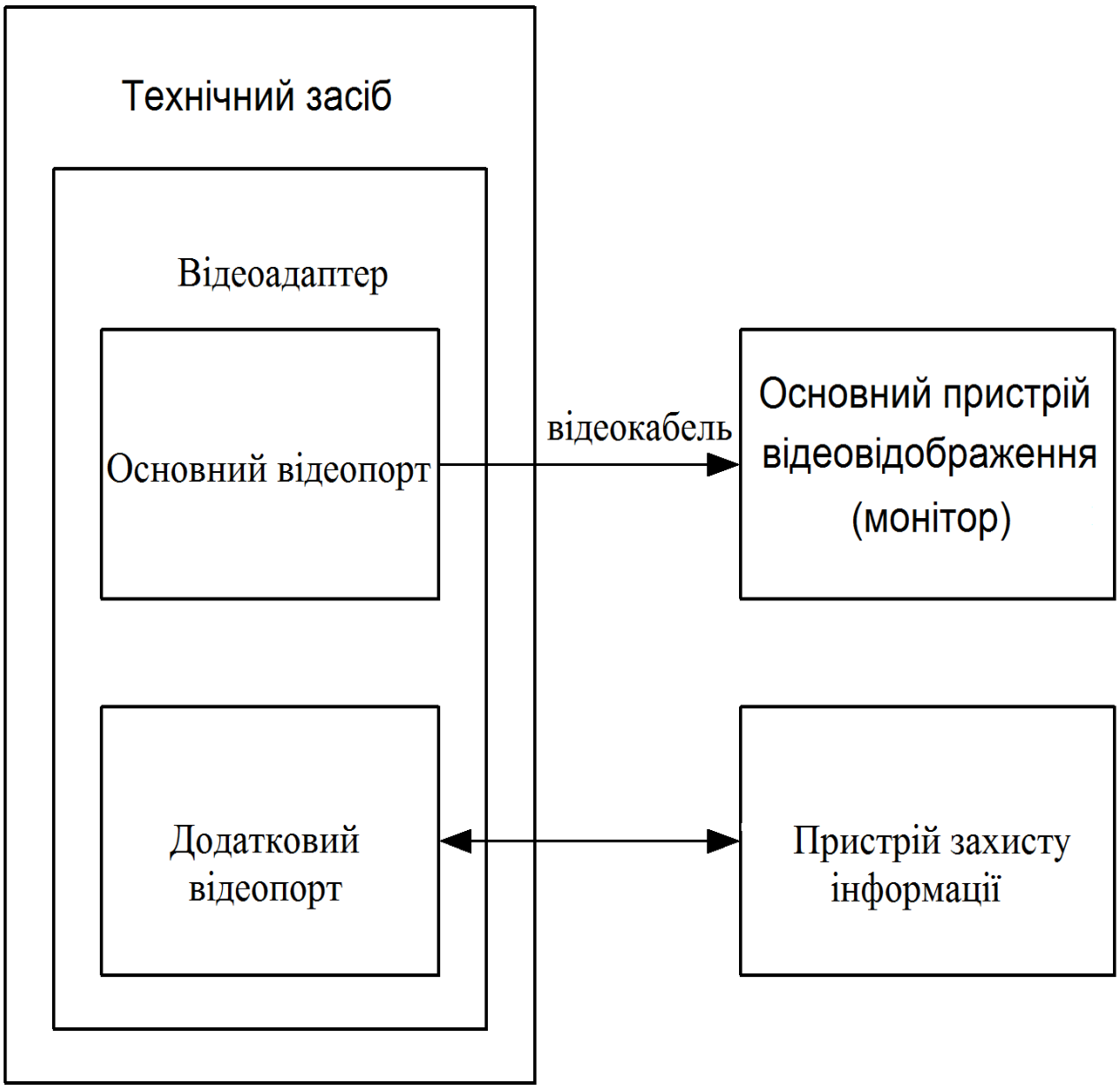

Рисунок 2.2 – Приклад підключення ТЗ до запропонованого пристрою захисту інформації від витоку по каналу ПЕМВН монітора

Запропонований пристрій захисту інформації включає в себе роз'єм підключення до додаткового відеопорту, СВЗ, блок емуляції пристрою відеовідображення, що містить незалежну пам'ять типу EEPROM (Electrically Erasable Programmable Read-Only Memory, постійний запам'ятовувальний

пристрій, що електрично стирається та перепрограмовується), в яку записується прошивка EDID. EDID включає базову інформацію про пристрій, зчитану з основного пристрою відеовідображення (рис. 2.1).

Як роз'єми використовуються, роз'єми типу «тато» стандартів DVI, VGA, HDMI, Display Port і аналогічних. Енергонезалежна пам'ять підключена двостороннім каналом зв'язку до роз'єму. Вхід СВЗ підключений до виходу роз'єму (рис. 2.1).

СВЗ призначена для створення імітуючих і маскуючих завад. В якості випромінюючого елемента використовуються, наприклад, провідні лінії узгоджені навантаженням, підключені до зворотної лінії, заземленою на корпусі ТЗ або антени. При недостатньому рівні випромінювання завад для захисту від витоку по каналу ПЕМВН в кожен канал СВЗ вводиться підсилювач сигналу. Для зручності експлуатації СВЗ може об'єднуватися в один кабель з відеокабелем по якому передається інформація, що захищається, в основний пристрій відеовідображення (монітор) (рис. 2.1, рис. 2.2).

Слід зазначити, що EEPROM – постійний запам'ятовувальний пристрій, що програмується та очищується за допомогою електрики, один з видів енергонезалежної пам'яті. Пам'ять такого типу може очищуватися та заповнюватися інформацією декілька десятків тисяч разів. Використовується в твердотільних накопичувачах. Одним з різновидів EEPROM є флеш-пам'ять.

Принцип роботи EEPROM оснований на зміні та реєстрації електричного сигналу в ізольованій області (кишені) напівпровідникової структури.

Зміна заряду («запис» та «стирання») виконується поданням між затвором і витоком великого потенціалу, щоб напруженість електричного поля в тонкому діелектрику між каналом транзистора і кишенею виявилася достатньою для виникнення тунельного ефекту. Для посилення ефекту тунелювання електронів у кишеню при записі застосовується невелике прискорення електронів шляхом пропускання струму через канал польового транзистора. Читання виконується польовим транзистором, для якого кишеня виконує роль затвора. Потенціал

плавного затвору змінює порогові характеристики транзистора, що й реєструється ланцюгами читання.

Основна особливість класичної осередку EEPROM – наявність другого транзистора, який допомагає керувати режимами запису і стирання. Деякі реалізації виконувалися у вигляді одного трьохзатворного польового транзистора (один затвор плаваючий і два звичайних). Ця конструкція забезпечується елементами, які дозволяють їй працювати у великому масиві таких же осередків. З'єднання виконується у вигляді двовимірної матриці, в якій на перетині стовпців і рядків знаходиться одна клітинка. Оскільки осередок EEPROM має третій затвор, то крім підкладки до кожної клітинки підходять три провідника (один провідник стовпців і два провідника рядків).

Запропонований пристрій захисту інформації від витоку по каналу ПЕМВН монітора з використанням імітаційних та маскуючих завад працює наступним чином.

До основного відеопорту підключається основний пристрій відео відображення (монітор), на який виводиться інформація, що підлягає захисту. ТЗ визначає його як «монітор-1». Потім до додаткового відеопорту підключається пристрій захисту інформації, який визначається ТЗ як ще один пристрій відеовідображення «монітор-2» (рис.2.2).

Пристрій захисту інформації і основний пристрій відеовідображення визначаються ТЗ як два однакових пристрої, що мають однакові параметри роздільної здатності і частоти поновлення (рис.2.2).

Програмне забезпечення, встановлене на ТЗ, періодично формує цифрове зображення, у якого колір кожного пікселя має випадкове значення. Відеоадаптер перетворює цифрове зображення в чотирьохканальний сигнал і виводить його на додатковий відеопорт (рис.2.2).

Пристрій захисту інформації, використовуючи сигнал, сформований відеоадаптером на додатковому відеопорті, створює імітаційні та маскуючі завади (рис.2.2).

2.2 Оцінка ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад

В якості підтвердження ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад було проведено моделювання в середовищі Matlab / Simulink по визначенню рівнів і частот інформативних ПЕМВН, створених основним пристроєм відеовідображення і іншими каналами передачі даних, і завад, створених пристроєм захисту інформації [24].

Структура імітаційної моделі підключення ТЗ до запропонованого пристрою захисту інформації від витоку по каналу ПЕМВН монітора представлена на рис. 2.3.

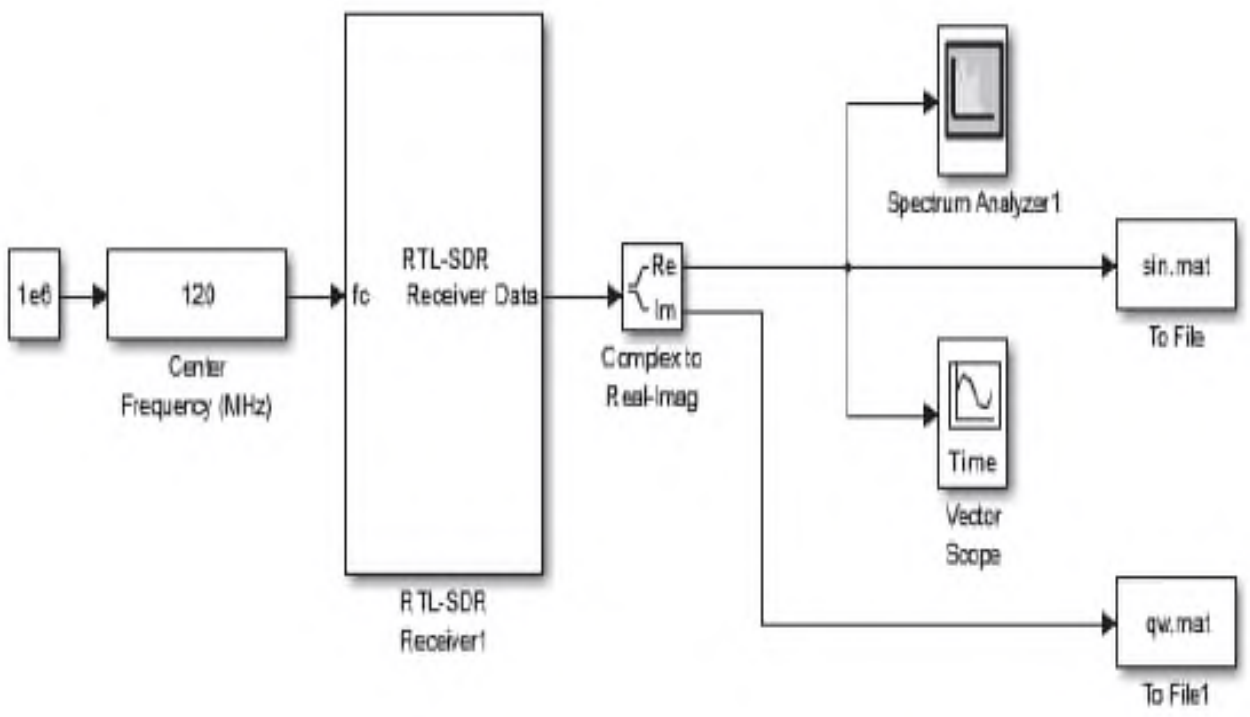

Рисунок 2.3 – Структура імітаційної моделі для оцінки ефективності запропонованого підходу до захисту інформації від витоку по каналу ПЕМВН монітора

На основі отриманих результатів було оцінено рівень відношення сигнал-завада для конкретного об'єкта, що захищається ТЗ.

На рис. 2.4, 2.5 і 2.6 наведені амплітудні спектри, отримані в результаті моделювання. На рис. 2.4, 2.5 і 2.5 позначено сірим – спектр ПЕМВН від монітора, а чорним – спектр сумарного сигналу ПЕМВН від монітора і імітаційних завад від пристрою захисту інформації.

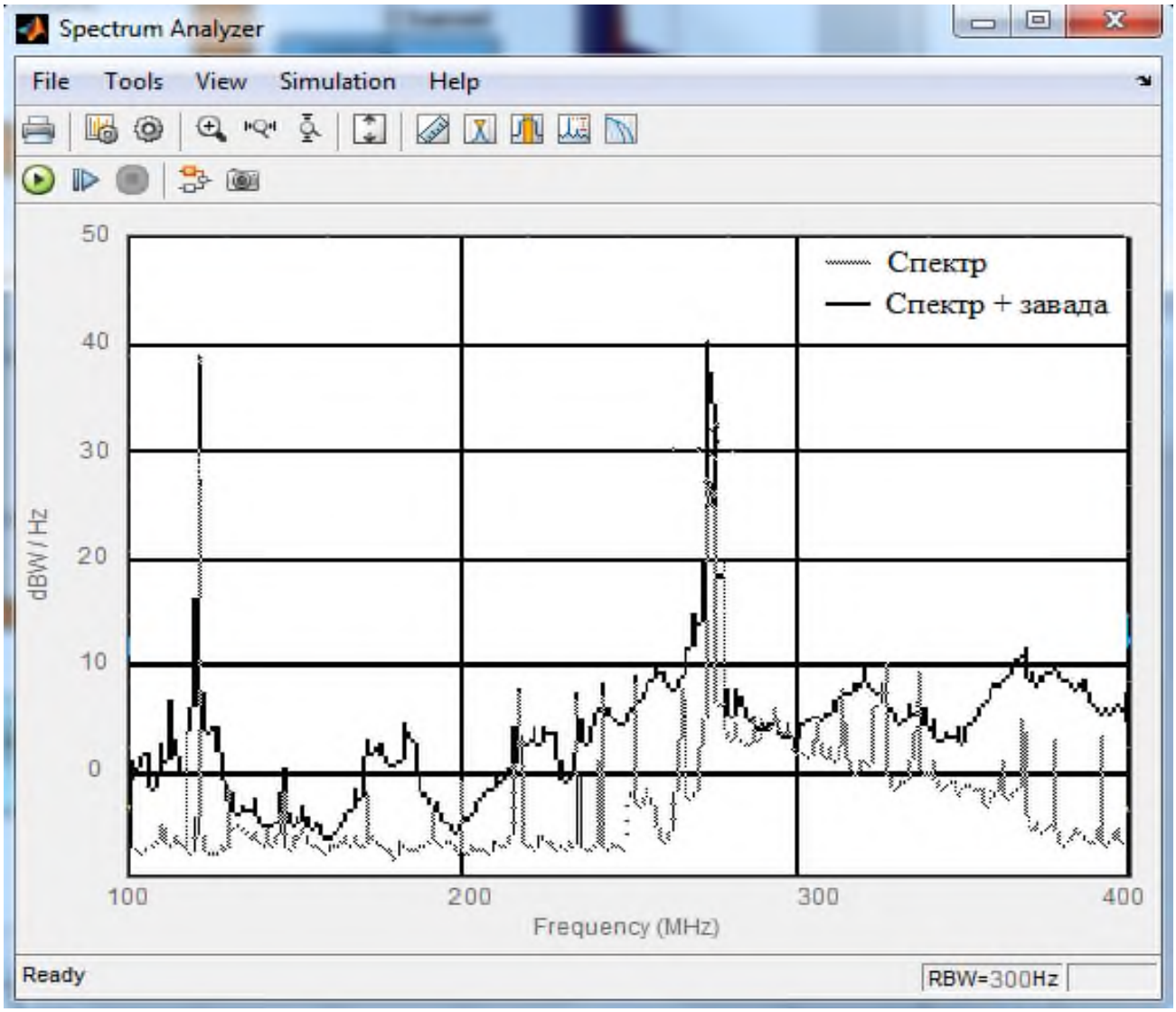

Рисунок 2.4 – Амплітудні спектри, отримані в результаті моделювання (виведення сигналу типу «меандр»)

На рис. 2.4, 2.5 і 2.6 видно, що імітаційні завади і ПЕМВН мають частотні спектри, що взаємно перекриваються. Рівень інтенсивності імітаційних завад

перевищує ПЕМВН від пристрою відеовідображення в режимі максимального випромінювання монітора з використанням тестового сигналу типу «меандр» (рис. 2.4), виведення текстової (рис. 2.5) і графічної (рис. 2.6) інформації.

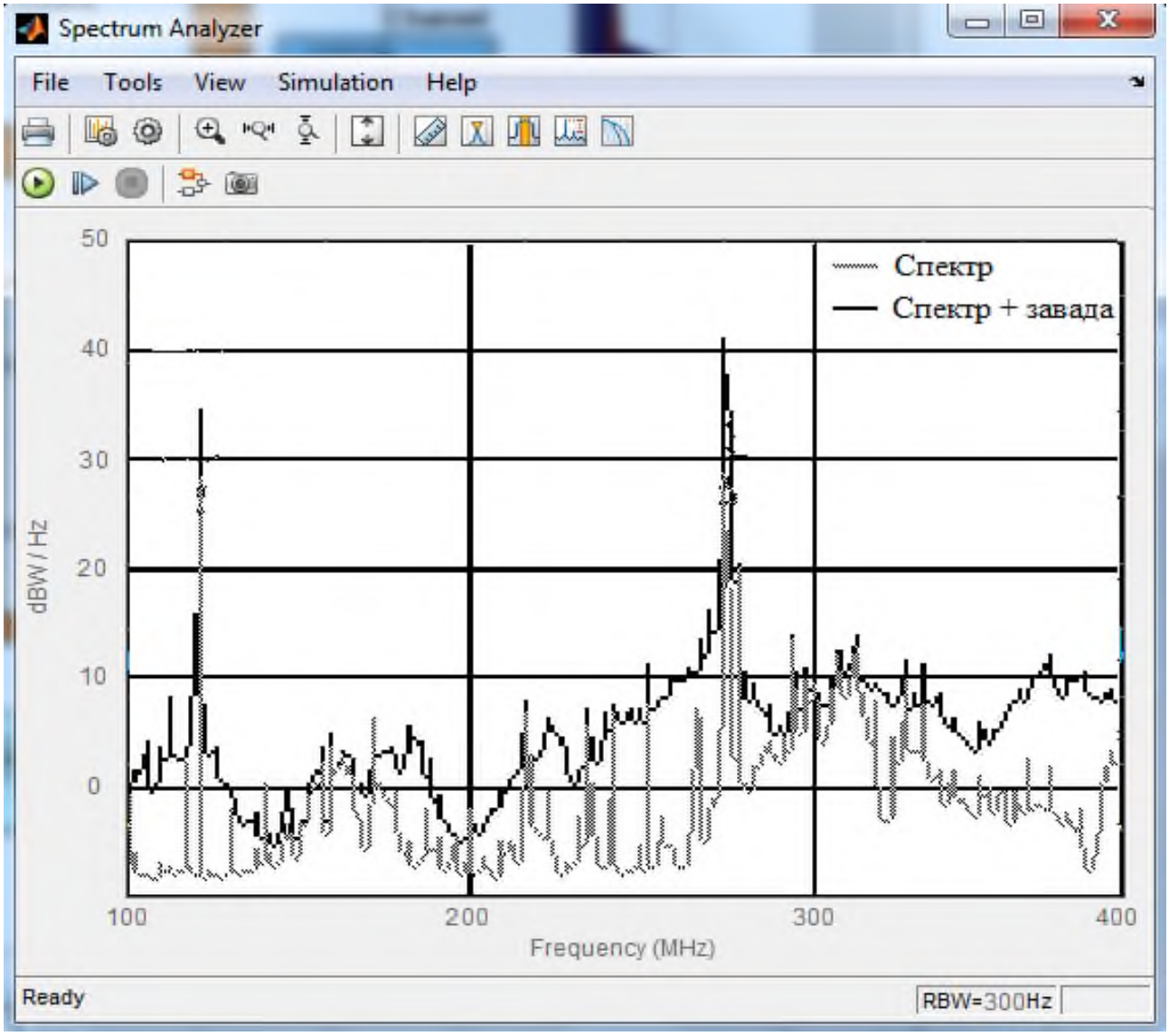

Рисунок 2.5 – Амплітудні спектри, отримані в результаті моделювання (виведення текстової інформації)

Таким чином, за рахунок використання запропонованого підходу до захисту інформації від витоку по каналу ПЕМВН монітора з використанням імітаційних та маскуючих завад виключається вплив людського фактора на процес технічного захисту інформації від витоку по каналу ПЕМВН.

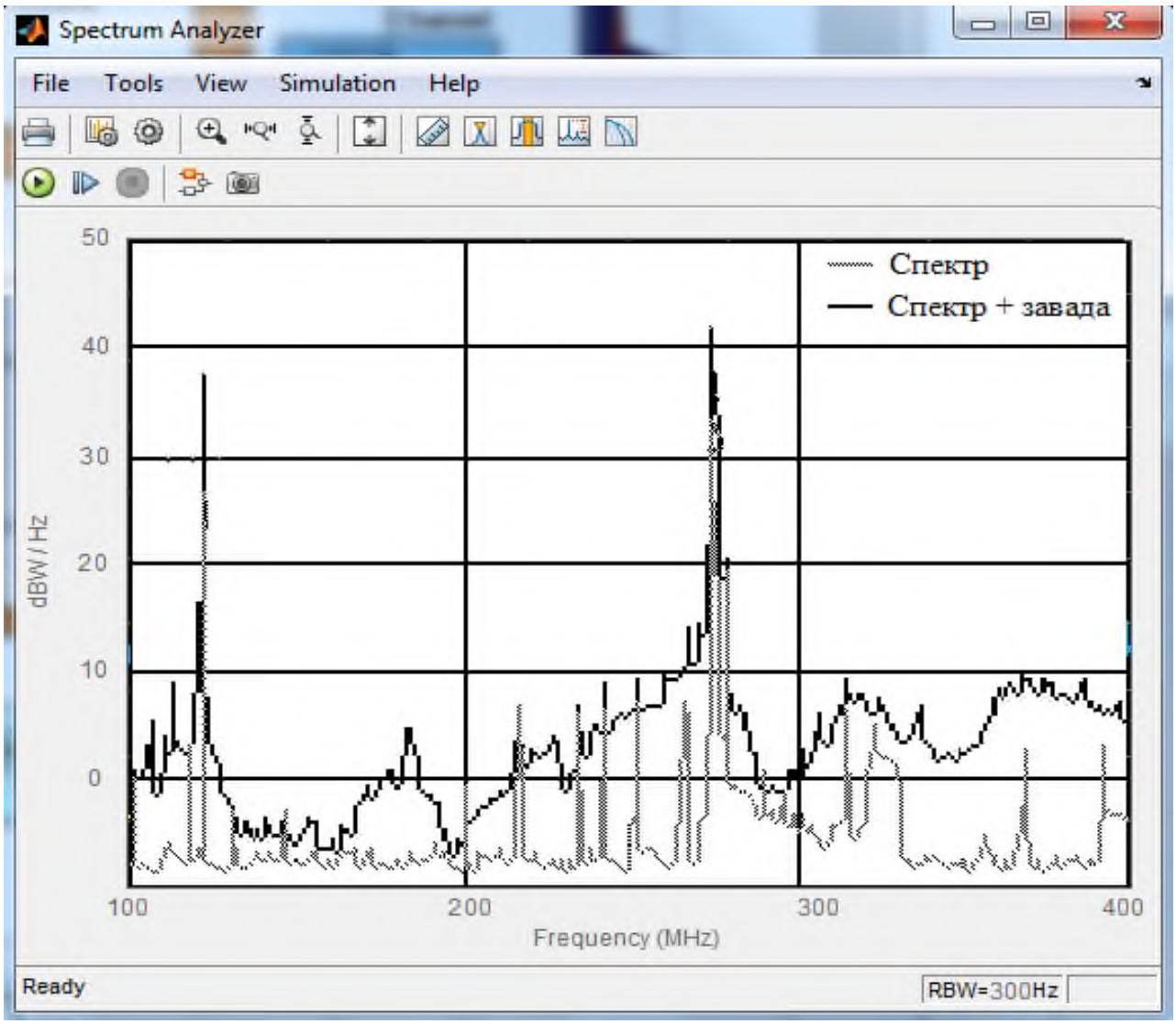

Рисунок 2.6 – Амплітудні спектри, отримані в результаті моделювання (виведення графічної інформації)

Крім того, підвищується ефективність використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання щодо інформативного сигналу. Знижується складність і вартість технічної реалізації пристрою і робіт з технічного захисту інформації, що обробляється ТЗ, від витоку по каналу ПЕМВН. Відбувається розширення функціональних можливостей, що полягає в тому, що запропонований пристрій захисту інформації крім імітаційних завад, що забезпечують захист інформації, яка циркулює в відеосистемі ТЗ, створює маскуючі завади з рівнем і шириною спектру достатніми для захисту інформації, яка циркулює в інших каналах

передачі даних ТЗ, що відповідають за вводу / вивід інформації зокрема USB, PS/2, COM, LPT.

2.3 Висновки

Запропонований підхід відноситься до техніки зв'язку і може використовуватися для захисту інформації, що обробляється ТЗ, що мають в своєму складі ВС, яка функціонує на основі стандартів DVI, VGA, Display Port, HDMI і аналогічних, від витоку інформації по каналу ПЕМВН.

Метою розробки запропонованого підходу є усунення впливу людського фактора на процес технічного захисту інформації від витоку по каналу ПЕМВН. Додатковою метою є підвищення ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання щодо інформативного сигналу, зниження складності і вартості технічної реалізації пристрою і робіт з технічного захисту інформації, що обробляється ТЗ, від витоку по каналу ПЕМВН, розширення функціональних можливостей, що полягає в тому, що пристрій захисту інформації крім імітаційних завад, що забезпечують захист інформації, яка циркулює в відеосистемі ТЗ, створює маскуючі завади з рівнем і шириною спектру достатніми для захисту інформації, яка циркулює в інших каналах передачі даних ТЗ, що відповідають за вводу / вивід інформації зокрема USB, PS/2, COM, LPT.

Мета кваліфікаційної роботи досягається за рахунок того, що у відомому підході, що полягає у формуванні ТЗ на додатковому порті вводу / виводу інформації, до якого підключено пристрій вводу / виводу інформації, структурованого неінформаційного сигналу, при проходженні якого по з'єднувальним лініям типових вузлів і блоків технічного засобу виникають власні неінформативні побічні електромагнітні випромінювання, що забезпечують приховування інформативних сигналів випромінювання від пристрою вводу / виводу інформації, підключеного до основного порту вводу / виводу інформації. Новим є те, що в якості порту вводу / виводу

інформації, на якому ТЗ формує неінформаційний чотирьохканальний сигнал, використовується додатковий відеопорт ТЗ, як пристрій вводу / виводу інформації використовується пристрій захисту інформації, що є емулятором монітора , що визначається ТЗ як пристрій відеовідображення, що створює за допомогою СВЗ, імітаційні та маскуючі завади, які забезпечують приховування інформативних сигналів випромінювання, створюваних пристроєм відеовідображення, підключеного до основного відеопорту і інших каналів передачі даних відповідно.

Оцінка ефективності запропонованого підходу до захисту інформації від витоку по каналу ПЕМВН монітора була проведена шляхом моделювання в середовищі Matlab / Simulink. На основі отриманих результатів було оцінено рівень відношення сигнал-завада для конкретного об'єкта, що захищається ТЗ.

Встановлено, що імітаційні завади і ПЕМВН мають частотні спектри, що взаємно перекриваються. Рівень інтенсивності імітаційних завад перевищує ПЕМВН від пристрою відеовідображення в режимі максимального випромінювання монітора з використанням тестового сигналу типу «меандр», виведення текстової і графічної інформації.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою економічного розділу є обґрунтування економічної доцільності захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від захисту акустичної інформації;

– показники економічної ефективності застосування імітаційних та маскуючих завад.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на розробку та впровадження систем захисту інформації складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н},$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Визначення витрат на розробку заходів із захисту інформації

3.1.1.1. Визначення трудомісткості розробки заходів із захисту інформації

Визначення трудомісткості розробки заходів із захисту інформації здійснюється, виходячи з тривалості кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = t_{тз} + t_{в} + t_{а} + t_{д}, \text{ годин,}$$

де $t_{тз}$ – тривалість складання технічного завдання, $t_{тз}$=22 години;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $t_{в}$=18 годин;

$t_{а}$ – тривалість аналізу витоку інформації по каналу побічних електромагнітних випромінювань і наведень монітора, $t_{а}$=50 годин;

$t_{мз}$ – тривалість розробки заходів із захисту інформації із використанням імітаційних та маскуючих завад, $t_{в}$=48 годин;

$t_{д}$ – тривалість підготовки технічної документації, $t_{д}$=10 годин.

Тоді:

$$t = 22+18+50+48+10=148 \text{ годин.}$$

3.1.1.2. Розрахунок витрат на розробки заходів із захисту інформації

Витрати на створення програмного продукту $К_{пз}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання задач на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} .$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування) і визначається за формулою:

$$З_{зп} = t \cdot З_{пр}, \quad \text{грн.},$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн./годину.

За формулою визначається заробітна плата виконавця з урахуванням середньогодинної заробітної плати з нарахуваннями у розмірі 135 грн./годину.

$$З_{зп}=148*210 = 31080 \text{ грн.},$$

Вартість машинного часу для опрацювання задач на ПК визначається за формулою:

$$З_{мч} = t \cdot C_{мч}, \quad \text{грн.},$$

де t – трудомісткість опрацювання задач на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість машинного часу для опрацювання задач на ПК визначається за формулою:

$$З_{мч}=148*1,81=267,88 \text{ грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}, \quad \text{грн.},$$

де P – встановлена потужність ПК (P = 0,8 кВт);

C_e – тариф на електричну енергію (C_e = 1,64 грн./кВт за годину);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік ($Ф_{зал}$ = 5150 грн.);

H_a – річна норма амортизації на ПК (H_a = 0,1 частки одиниці);

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення ($H_{апз}$ = 0,2 частки одиниці);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення ($К_{лпз}$ = 2118 грн.);

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня ($F_р$ = 1920 годин).

Вартість 1 години машинного часу ПК визначається за формулою (3.5):

$$С_{мч} = 0{,}8 \cdot 1 \cdot 1{,}64 + \frac{5150 \cdot 0{,}1}{1920} + \frac{2118 \cdot 0{,}2}{1920} = 1{,}81 \text{грн.}$$

Отже, витрати на обґрунтування методики вибору інструментальних засобів в системі захисту акустичної інформації:

$$К_{пз} = 31080 + 267{,}88 = 31347{,}88 \text{ грн.}$$

Для захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад планується придбання пам'яті типу EEPROM (Electrically Erasable Programmable Read-Only Memory), вартість якого складає 1856 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 3300 грн.

Таким чином, капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = 31347{,}88 + 1856 + 3300 = 36503{,}88 \text{ грн.},$$

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.}$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в$ = 0);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 2000 грн.).

Амортизації підлягає пам'ять типу EEPROM зі строком корисного використання 2 роки:

$$С_а = 1856 / 2 = 9028 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Для забезпечення захисту акустичної інформації в контексті забезпечення інформаційної безпеки спеціаліст необхідно додаткове виконання функцій на 0,4 ставки посадового окладу спеціаліста з інформаційної безпеки. Отже,

$$С_з = 0,4*15000*12 + 0,4*15000*12*0,08= 77760 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2019 року складає 22%.

$$С_{єв} = 77760*0,22 = 17107,2 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається наступним чином:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,85 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$=1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається:

$$С_{ел} = 0,85*1920*1,64 = 2676,48 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат -1% ($С_{тос}$ = 36503,88*0,01=365,04 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються наступним чином:

$$С_к = 2000 + 9028 + 77760 + 17107,2 +2676,48 + 365,04 = 108936,7 \text{ грн.}$$

Відповідно, річні поточні витрати на функціонування системи інформаційної безпеки складуть:

$$С = 108936,7 \text{ грн.}$$

3.2 Оцінка можливого збитку

Забезпечення інформаційної безпеки через захист акустичної інформації передбачає відвернення загроз розголошення та витоку інформації щодо ведення перегорів тощо. Для підприємств середнього та малого бізнесу вартість контракту може складати біля 250 000 грн. Якщо підприємство заключає біля 15 контрактів на рік, то можлива величина збитку (В) на рік від загроз щодо акустичної інформації, вірогідність реалізації яких складає 20% (R=20%), становитиме:

$$В = 250000*15 = 3\ 750\ 000 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи захисту акустичної інформації для підвищення рівня інформаційної безпеки

Загальний ефект від впровадження системи захисту акустичної інформації для підвищення рівня інформаційної безпеки становить:

$$E = B \cdot R - C \text{ грн.,}$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації акустичних загроз, частки одиниці (0,2);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження від впровадження системи захисту акустичної інформації для підвищення рівня інформаційної безпеки визначається наступним чином:

$$E = 37500000*0,2 – 108936,7 = 7391063 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI складає:

$$ROSI = \frac{7391063}{36503,88} = 20,03, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (13%).

Розрахункове значення коефіцієнта повернення інвестицій визначається наступним чином:

$$20{,}03 > (18 - 13)/100 = 20{,}03 > 0{,}05.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{20{,}03} = 0{,}05, \quad \text{років.}$$

3.4 Висновок

Відповідно до наведених розрахунків обґрунтовано економічну доцільність захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад.

Розраховані капітальні витрати, які складають 36503,88 грн., поточні витрати на експлуатацію системи інформаційної безпеки, що становлять 108936,7 грн. Відповідно до отриманого значення коефіцієнту ROSI на одну гривню капітальних інвестицій приходитиметься 20,03 грн. додаткового прибутку. Термін окупності інвестицій складе 0,05 років.

ВИСНОВКИ

1. В результаті аналізу каналів витоку інформації при експлуатації персональних комп’ютерів встановлено, що найнебезпечнішим каналом витоку є дисплей, оскільки з точки зору захисту інформації він є найслабшою ланкою в обчислювальній системі.

2. В результаті аналізу існуючих підходів до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень встановлено їх недоліки. Недоліки відомих генератора шумових сигналів [21] та способу захисту оброблюваної інформації засобами обчислювальної техніки шляхом зашумлення інформативних побічних електромагнітних випромінювань і наведень [22], полягають у високій вартості і складності технічної реалізації пристроїв, а також в неоптимальному використанні маскуючих завад у зв'язку з їх надмірними значеннями рівня і ширини спектра.

Встановлено, що недоліками відомого способу захисту засобів обчислювальної техніки від витоку інформації по каналу ПЕМВН [23] (прототипу) є: участь оператора в процесі технічного захисту інформації; відсутність синхронізації між імітаційною завадою і інформативним сигналом; висока вартість і складність технічної реалізації пристрою; а також те, що підхід може бути використаний для захисту інформації циркулюючої тільки в одному пристрої вводу / виводу інформації (каналі передачі даних) – USB.

3. Запропоновано підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора з використанням імітаційних та маскуючих завад, згідно якого пристрій захисту інформації крім імітаційних завад, що забезпечують захист інформації, яка циркулює в відеосистемі ТЗ, створює маскуючі завади з рівнем і шириною спектру достатніми для захисту інформації, яка циркулює в інших каналах передачі даних ТЗ, що відповідають за ввід / вивід інформації зокрема USB, PS/2, COM, LPT.

4. В результаті оцінки ефективності запропонованого підходу було оцінено рівень відношення сигнал-завада для конкретного об'єкта, що захищається ТЗ. Встановлено, що імітаційні завади і ПЕМВН мають частотні спектри, що взаємно перекриваються. Рівень інтенсивності імітаційних завад перевищує ПЕМВН від пристрою відеовідображення в режимі максимального випромінювання монітора з використанням тестового сигналу типу «меандр, виведення текстової і графічної інформації. Отримані результати дослідження запропонованого підходу (рис. 2.4-2.6) демонструють те, що використання запропонованого підходу підвищує ефективність використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання щодо інформативного сигналу.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. Ярочкин В.И. Информационная безопасность: Учебник для вузов. 2-е издание. / В.И. Ярочкин. – М.: Академический Проект, Гаудеамус, 2004. – 544 с.

3. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие. / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия - Телеком, 2005. – 416 с.

4. Хорошко В.О. Методы и средства защиты информации. / В.О. Хорошко, А.А. Чекатков. – К.: Издательство Юниор, 2003. – 504 с.

5. Домарев В.В. Безопасность информационных технологий. Системный подход. / В.В. Домарев. – К.: ТОВ «ТВД «ДС», 2004. – 992 с.

6. Грайворонський М.В. Безпека інформаційно-комунікаційних систем. / М.В. Грайворонський, О.М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.

7. Деднев М.А. Защита информации в банковском деле и электронном бизнесе. / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М.: Кудиц-образ, 2004. – 512 с.

8. Коне И.Р. Информационная безопасность предприятия. / И.Р. Коне. – СПб.: БХВ-Петербург, 2003. – 752 с.

9. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр Академия, 2009. – 416 с.

10. Гавриш В. Практические пособие по защите коммерческой тайны. / В. Гавриш. – Симферополь : «Таврида», 1994. – 112 с.

11. Архіпов О.Є. Захист інформації в телекомунікаційних мережах та системах зв’язку. Навч.-метод. посібник. / О.Є. Архіпов, В.М. Луценко, В.О. Худяков. – К.: ІВЦ «Видавництво «Політехніка», 2003. – 40 с.

12. Вертузаєв М.С. Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посібник / М.С. Вертузаєв, О.М. Юрченко; За ред. С.Г. Лаптєва. – К. : Видавництво Європейського ун-ту, 2001. – 321 с.

13. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах: навч. посіб. для студ. спец. «Комп'ютерні науки», «Комп'ютерна інженерія», «Прикладна математика», «Інформаційна безпека» вищ. навч. закл. / І.Д. Горбенко, Т.О. Гріненко. – Х.: Харківський національний університет радіоелектроніки, 2004. – 368 с.

14. Термінологічний довідник з питань технічного захисту інформації. / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков; за ред. В.О. Хорошка. – 4-е вид., доп. і перероб. – К. : ДУІКТ, 2007. – 365 с.

15. Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки: Підручник / за ред. проф. В.О. Хорошка – К.: Вид. ДУІКТ, 2009. – 292 с.

16. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібн. / А.О. Антонюк. – К.: Видавн. дім. «КМ Академія», 2003. – 244 с.

17. Рибальський О.В. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

18. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / О.В. Рибальський, В.Г. Хахановський, В.В. Шорошев, О.І. Грищенко, С.В. Сторожев, М.В. Кобець. – К.: НАВСУ, 2003. – 160 с.

19. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

20. Максименко Г.А. Методи виявлення, обробки й ідентифікації сигналів радіозакладних пристроїв. / Г.А.Максименко, В.А. Хорошко. – К: ТОВ "Полиграфконсалтинг" , 2004. – 317 с.

21. Патент РФ 2519565. Генератор шумовых сигналов / Ю.П. Лепеха – заявл. 20.07.2011, опубл. 27.01.2013, бюл. № 3.

22. Патент РФ 2493594. Способ защиты обрабатываемой информации средствами вычислительной техники путем зашумления информативных побочных электромагнитных излучений и наводок, устройство защиты информации для реализации способа / Ю.П. Лепеха – заявл. 20.12.2011, опубл. 27.06.2013.

23. Патент РФ 2479022. Способ защиты средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений и наводок / Д.В. Долниковский, В.И. Маслов – заявл. 20.01.2012, опубл. 10.04.2013.

24. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	27	
6	А4	Спеціальна частина	15	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Зайончковський.ppt

2 Диплом Зайончковський.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-16-2 Зайончковського О.Д. на тему: «Захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень монітора»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 69 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення ефективності використання енергії завади за рахунок її адаптивності по ширині спектра, рівню і часу випромінювання відносно інформативного сигналу.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу каналів витоку інформації при експлуатації персональних комп'ютерів, а також існуючих підходів до ЗІ від витоків по каналу ПЕМВН сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до захисту інформації від витоку по каналу ПЕМВН монітора з використанням імітаційних та маскуючих завад та оцінено його ефективність.

Практична цінність роботи полягає в тому, що запропонований підхід може бути використаний в відеосистемах, які функціонують на основі стандартів DVI, VGA, Display Port, HDMI тощо.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Зайончковський О.Д. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**