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 *Базаров Дмитро Миколайович*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

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

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
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Базаров Дмитро Миколайович*** **академічної групи** ***125-17-1***
(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 цифрових накопичувачів***

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз технічних каналів витоку та руйнування інформації, а також існуючих підходів до захисту інформації від витоків по каналу побічних електромагнітних випромінювань і наведень.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до захисту інформації від витоку по каналу ПЕМВН з використанням дерева перекриттів маскуючих сигналів та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Базаров Д.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 19 рис., 4 додатки, 30 джерел.

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

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

Мета кваліфікаційної роботи – підвищення коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки.

Наукова новизна результатів полягає у формуванні списку сукупностей файлів, згідно з яким перед передачею сукупності файлів, отриманої в результаті випадкового вибору файлу на кожному накопичувачі, перевіряють їх на приналежність до будь-якої сукупності з вищевказаного списку.

У першому розділі проаналізовано технічні канали витоку та руйнування інформації, а також існуючі підходи до захисту інформації 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 з використанням дерева перекриттів маскуючих сигналів 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.

ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ І НАВЕДЕННЯ, ІМІТАЦІЙНІ ТА МАСКУЮЧІ ЗАВАДИ, ЗАХИСТ ІНФОРМАЦІЇ, АМПЛІТУДНІ СПЕКТРИ, ЗАСОБИ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 72 с., 19 рис., 4 приложения, 30 источников.

Объект разработки – канал побочных электромагнитных излучений и наводок.

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

Цель квалификационной работы – повышение коэффициента перекрытия спектров информативного и неинформативные (маскирующего) сигналов, излучаемых средствами вычислительной техники.

Научная новизна заключается в формировании списка совокупностей файлов, согласно которому перед передачей совокупности файлов, полученной в результате случайного выбора файла на каждом накопителе, проверяют их на принадлежность к любой совокупности из вышеуказанного списка.

В первой главе проанализированы технические каналы утечки и разрушения информации, а также существующие подходы к защите информации 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 с использованием дерева перекрытий маскирующих сигналов 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.

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ, ИМИТАЦИОННЫЕ И МАСКИРУЮЩИЕ ПОМЕХИ, ЗАЩИТА ИНФОРМАЦИИ, АМПЛИТУДНЫЕ СПЕКТРЫ, СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 72, fig. 19, 4 additions, 30 sources.

The object of development is a channel of incidental electromagnetic radiation and guidance.

The subject of development is the approach to information protection from leakage through the channel of spurious electromagnetic radiation and interference from digital storage devices.

The purpose of the qualification work is to increase the overlap coefficient of the spectra of informative and non-informative (masking) signals emitted by computer technology.

The scientific novelty of the results is the formation of a list of sets of files, according to which before transferring a set of files obtained by random selection of a file on each drive, check them for membership in any set from the above list.

The first section analyzes the technical channels of leakage and destruction of information, as well as existing approaches to protect information from leakage through the channel of spurious electromagnetic radiation and guidance.

In a special part of the work, an approach to the protection of information from leakage through the channel of incidental electromagnetic radiation and guidance using a tree of overlapping masking signals and evaluates its effectiveness. Based on the results of research, conclusions were made 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 RADIATIONS AND POINTS, IMITATION AND MASKING INTERFERENCES, INFORMATION PROTECTION, AMPLITUDE SPECTRA, COMPUTER EQUIPMENT, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗІ – Захист інформації;

ЕМВ – Електромагнітні випромінювання;

ЕМКВІ – Електромагнітний канал витоку інформації;

ЕКВІ – Електричні канали витоку інформації;

ЕОМ – Електронна обчислювальна машина;

ЗОТ – Засоби обчислювальної техніки;

ІТС – Інформаційно-телекомунікаційна система;

НСД – Несанкціонований доступ;

ОТЗ – Основний технічний засіб;

ПЕМВ – Побічне електромагнітне випромінювання;

ПЕМВН – Побічні електромагнітні випромінювання і наведення;

СТЗ – Спеціальні технічні засоби;

ТЗР – Технічні засоби розвідки;

ТКВІ – Технічний канал витоку інформації;

ЦП – Центральний процесор.

ЗМІСТ

ВСТУП

Аналіз практики протидії технічним розвідкам, що склалася на сьогоднішній день, дозволяє виявити важливу особливість, характерну для перехоплення інформації оперативного характеру. Якщо раніше найбільший обсяг відомостей порушник отримував в результаті перехоплення технічними засобами розвідки (ТЗР) інформативних сигналів акустичного поля (мовних сигналів) [1-12], то наразі інтенсивне впровадження в практику інформаційної діяльності систем електронного документообігу призвело до того, що найбільш інформаційно ємними стають відомості електронних документів, в яких концентровано представлена вся інформація з потрібних порушнику питань.

З огляду на той факт, що технологічним середовищем систем електронного документообігу є інфокомунікаційна середа, серйозну загрозу став представляти витік інформації по каналах побічних електромагнітних випромінювань і наведень (ПЕМВН) від засобів обчислювальної техніки (ЗОТ).

Технологія перехоплення інформативних сигналів ПЕМВН від засобів обчислювальної техніки почала розвиватися з початку 2000-х років. В цей час в США була розроблена система перехоплення комп'ютерної інформації 4625-COMINT, яка могла відновлювати інформацію, оброблювану засобами обчислювальної техніки, за рахунок перехоплення ПЕМВН. Система мала 100 каналів пам'яті, в яких накопичувалася і аналізувалася перехоплена інформація. Після обробки перехоплена інформація відновлювалася в тому вигляді, в якому вона виводилася на екран дисплея ЗОТ. Система мала наступні характеристики: діапазон робочих частот – 25 МГц ... 2 ГГц, чутливість приймального пристрою – 0,15 мкв. Існуючі наразі засоби перехоплення ПЕМВН від засобів обчислювальної техніки мають кращі характеристики.

Тому все більш актуальною стає проблема забезпечення захисту інформації від витоку по таким каналам. Результатом цілеспрямованого і системного застосування технологій безпеки в цій галузі стало вдосконалення

способів виявлення каналів витоку інформації через ПЕМВН від засобів обчислювальної техніки.

При цьому очевидно, що існуючий традиційний підхід до вирішення проблеми виявлення каналів витоку інформації через ПЕМВН, заснований на виявленні окремих ознак витоку, не може забезпечити повноту виявлення такого роду погроз. Це пов'язано з низькою вірогідністю фактів виявлення, а також зі складністю ідентифікації трьох найбільш важливих для такого роду погроз станів, а саме:

• етапу дій порушника;

• прогнозованого обсягу інформації, що розкривається в процесі перехоплення на момент виявлення каналу;

• поточного рівня загрози безпеці інформації.

Таким чином, вдосконалення підходів до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень наразі є актуальною задачею.

Метою роботи є підвищення коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки.

Постановка задачі:

• проаналізувати технічні канали витоку та руйнування інформації;

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

• запропонувати підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1.1 Технічні канали витоку та руйнування інформації

Захист інформації від витоку технічними каналами – це комплекс організаційно-технічних заходів, що виключають або ослабляють безконтрольний вихід конфіденційної інформації за межі контрольованої зони [1-8].

Слід пам'ятати, що:

• безпечних технічних засобів немає;

• джерелами утворення технічних каналів витоку інформації є фізичні перетворювачі;

• будь-який електронний елемент за певних умов може стати джерелом утворення каналу витоку інформації;

• будь-який канал витоку інформації може бути виявлений і локалізований;

• канал витоку інформації легше локалізувати, ніж виявити.

Витік – це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким вона довірена. Утворюється за рахунок неконтрольованих фізичних полів (акустичних, світлових, електромагнітних, радіаційних, теплових тощо) [1].

Технічний канал витоку інформації – фізичний шлях від джерела інформації до порушника, за допомогою якого може бути здійснений несанкціонований доступ (НСД) до відомостей, що охороняються. Технічні канали витоку підрозділяються на візуально-оптичні, акустичні, електромагнітні, матеріально-речові та інші (рис. 1.1).

Сигнали є матеріальними носіями інформації. По своїй фізичній природі сигнали можуть бути електричними, електромагнітними, акустичними і т.д., тобто сигналами, як правило, являються електромагнітні, механічні та інші

види коливань (хвиль), причому інформація міститься в їх параметрах, що змінюються.

Рисунок 1.1 – Класифікація технічних каналів витоку інформації

Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути газові (повітря), рідинні (водні) і тверді середовища. Наприклад повітряний простір, конструкції будівель, сполучні лінії і струмопровідні елементи, грунт (земля) і т.п.

Технічні засоби розвідки служать для прийому і виміру параметрів сигналів. Вони використовуються для перехоплення інформації, що обробляється в технічних засобах, акустичної (мовної) інформації, а також як засоби прихованого відеоспостереження і зйомки.

1.1.1 Характеристика способів прихованого відеоспостереження і зйомки

Важливим джерелом конфіденційних відомостей є видова інформація, що отримується технічними засобами розвідки порушника у вигляді зображень об'єктів або документів. Залежно від характеру інформації й її призначення виділяють наступні способи її отримання: спостереження за об'єктом, зйомка об'єкту, зйомка (зняття копій) документів.

Спостереження за об'єктом організовується протягом певного (у ряді випадків тривалого) часу. Залежно від умов спостереження і освітлення для спостереження об'єктом можуть використовуватися різні технічні засоби: для спостереження вдень – оптичні прилади (монокуляри, підзорні труби, бінокли, телескопи і т.д.), телевізійні системи; для спостереження вночі – прилади нічного бачення, телевізійні системи, тепловізори; для спостереження з великої відстані використовуються засоби з довгофокусними оптичними системами, а при спостереженні зблизька – встановлені телевізійні камери, що камуфлюють потайно. Причому відеозображення з телевізійних камер може передаватися на монітори як по кабелю, так і по радіоканалу

Зйомка об'єктів проводиться для документування результатів спостереження і детальнішого вивчення об'єктів з використанням телевізійних і фотографічних засобів. Причому фотоапарати використовуються у разі, коли необхідно отримати окремі зображення, наприклад, зовнішній вигляд об'єкту або фотознімок співробітника, а телевізійні – коли необхідно отримати зображення динамічного процесу, наприклад технологічного циклу, або дій окремих осіб.

1.1.1.2 Характеристика технічних каналів витоку акустичної інформації

Під акустичною розуміється інформація, носієм якої є акустичні сигнали. У тому випадку, якщо джерелом інформації є людська мова, акустична інформація називається мовною.

Акустичний сигнал є обуреннями пружного середовища, що проявляються у виникненні акустичних коливань різної форми і тривалості.

Акустичними називаються механічні коливання часток пружного середовища, що поширюються від джерела коливань в навколишній простір у вигляді хвиль різної довжини.

Первинними джерелами акустичних коливань є механічні коливальні системи, наприклад, органи мови людини, а вторинними – перетворювачі

різного типу, у тому числі електроакустичні. Останні є пристроями, призначеними для перетворення акустичних коливань в електричні. До них відносяться пьезоелементи, мікрофони, телефони, гучномовці та інші пристрої.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення технічні канали витоку акустичної (мовний) інформації можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронний і параметричні (рис. 1.2).

У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря і для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони. Мініатюрні мікрофони об'єднуються (або з'єднуються) з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Автономні пристрої, що конструкційно об'єднують мініатюрні мікрофони і передавачі, називають акустичними закладками.

У вібраційних (структурних) технічних каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалювання, каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони (стетоскопи). Контактні мікрофони, сполучені з електронним підсилювачем називають електронними стетоскопами.

Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні і включають перехоплення акустичних коливань через ДТЗС, що мають «мікрофонний ефект», а також шляхом «високочастотного нав'язування».

Рисунок 1.2 – Класифікація технічних каналів витоку акустичної інформації

Деякі елементи ДТЗС (трансформатори, котушки індуктивності, електромагніти вторинного електрогодинника, дзвінків телефонних апаратів, дроселі ламп денного світла, електрореле і т.п.) мають властивість змінювати свої параметри (місткість, індуктивність, опір) під дією акустичного поля, що створюється джерелом акустичних коливань. Зміна параметрів призводить або до появи на цих елементах електрорушійної сили, що змінюється за законом впливаючого інформаційного акустичного поля, або до модуляції струмів, що протікають по цих елементах, інформаційним сигналом.

Оптико-електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відзеркалювальних поверхонь (стекол вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді і фазі (за законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація. Причому лазер і приймач оптичного випромінювання можуть бути встановлений в одному або різних місцях (приміщеннях).

В результаті дії акустичного поля міняється тиск на усі елементи високочастотних генераторів технічних засобів обробки інформації (ТЗОІ) і допоміжних технічних засобів і систем (ДТЗС). При цьому змінюється (трохи) взаємне розташування елементів схем, дротів в котушках індуктивності, дроселів і т.п., що може привести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації називається параметричним. Це обумовлено тим, що незначна зміна взаємного розташування, наприклад, дротів в котушках індуктивності (міжвиткової відстані) призводить до зміни їх індуктивності, а, отже, до зміни частоти випромінювання генератора, тобто до частотної модуляції сигналу. Або дія акустичного поля на конденсатори призводить до зміни відстані між пластинами і, отже, до зміни його місткості, що, у свою чергу, також призводить до частотної модуляції високочастотного сигналу генератора. Найчастіше спостерігається паразитна модуляція інформаційним сигналом

випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, що знаходяться у виділених приміщеннях і мають конденсатори змінної ємності з повітряним діелектриком в коливальних контурах гетеродинів. Промодульовані інформаційним сигналом високочастотні коливання випромінюються в навколишній простір і можуть бути перехоплені і детектовані засобами радіорозвідки.

1.1.3 Технічні канали витоку інформації, що обробляється технічними засобами обробки інформації

ТЗОІ обмеженого доступу:

- засоби обчислювальної техніки (ЗОТ) – технічні засоби інформаційно-телекомунікаційних систем (ІТС), електронних обчислювальних машин (ЕОМ) та їх окремі елементи;
- засоби виготовлення і розмноження документів;
- апаратура звукопідсилення, звукозапису, звуковідтворення і синхронного перекладу;
- системи внутрішнього телебачення;
- системи відеозапису і відеовідтворення;
- системи оперативно-командного зв'язку;
- системи внутрішнього автоматичного телефонного зв'язку та інші.

З точки зору захисту ці технічні засоби і системи називаються основними технічними засобами (ОТЗ).

Технічний канал витоку інформації (ТКВІ) – сукупність джерела інформативного сигналу (наприклад, ТЗОІ), технічного засобу, що здійснює перехоплення інформації, і фізичного середовища, в якому поширюється інформативний сигнал.

Порушники для перехоплення інформації використовують технічні засоби розвідки (ТЗР). Інші зацікавлені суб'єкти (юридичні особи, групи фізичних осіб, окремі фізичні особи) для перехоплення інформації

використовують спеціальні технічні засоби (СТЗ), пристосовані або допрацьовані для негласного отримання інформації.

Перехоплення інформації, що обробляється ЗОТ, може здійснюватися шляхом:

- перехоплення ПЕМВ, що виникають при роботі ЗОТ;
- перехоплення наведень інформативних сигналів із сполучних ліній ДТЗС і сторонніх провідників;
- перехоплення наведень інформативних сигналів з ліній електроживлення і заземлення ЗОТ;
- «високочастотного опромінення» ЗОТ;
- впровадження у ЗОТ закладних пристроїв.

1.1.4 Електромагнітні канали витоку інформації

В електромагнітних каналах витоку інформації (ЕМКВІ) носієм небезпечної інформації є електромагнітні випромінювання (ЕМВ), що виникають при обробці інформації ТЗОІ.

У деяких ТЗОІ (наприклад, системах звукопідсилення) носієм інформації є електричний струм, параметри якого (сила струму, напруга, частота і фаза) змінюються за законом зміни інформаційного мовного сигналу. При протіканні електричного струму струмоведучими елементами ТЗОІ та їх сполучними лініями в просторі, що оточує їх, виникає змінне електричне і магнітне поле. Через це елементи ТЗОІ є випромінювачами електромагнітного поля, яке модулюється за законом зміни інформаційного сигналу.

Ініціаторами виникнення ПЕМВ можуть бути різного роду високочастотні генератори:

- задаючі генератори;
- генератори тактової частоти;
- генератори стирання і підмагнічування магнітофонів;
- гетеродини радіоприймальних і телевізійних пристроїв;

- генератори вимірювальних приладів і т.д.

Рис. 1.3 ілюструє можливі режими роботи обчислювальної техніки, в яких виникають ПЕМВ. Діапазон можливих частот ПЕМВ ЗОТ може складати 10 кГц – 2 ГГц.

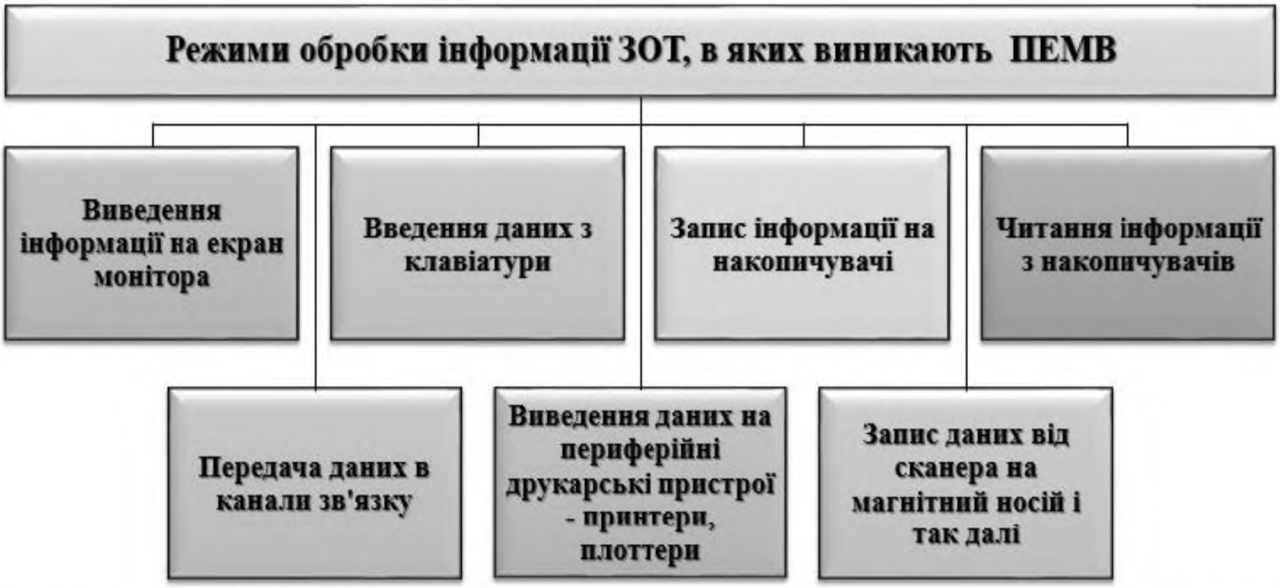


Рисунок 1.3 – Режими оброблення інформації в ЗОТ, в яких виникають ПЕМВ

Паразитне електромагнітне випромінювання ТЗОІ – це побічне радіовипромінювання, що виникає в результаті самозбудження генераторних або підсилювальних блоків ТЗОІ із-за паразитних зв'язків. Найчастіше такі зв'язки виникають за рахунок випадкових перетворень негативних зворотних зв'язків (індуктивних або ємнісних) в паразитні позитивні, що призводить до переводу підсилювача з режиму посилення в режим автогенерації сигналів. Частота автогенерації (самозбудження) лежить в межах робочих частот нелінійних елементів підсилювачів (наприклад, напівпровідникових приладів, електровакуумних ламп і т.п.).

У ряді випадків паразитне електромагнітне випромінювання модулюється інформативним сигналом відповідно до змін параметрів інформативного сигналу, що впливають на нього.

Для перехоплення ПЕМВ ТЗОІ використовуються спеціальні стаціонарні, переносимі та перевозимі приймальні пристрої, які називаються технічними засобами розвідки побічних електромагнітних випромінювань і наведень.

Перехоплення побічних електромагнітних випромінювань ТЗОІ технічними засобами розвідки показано на рис. 1.4.

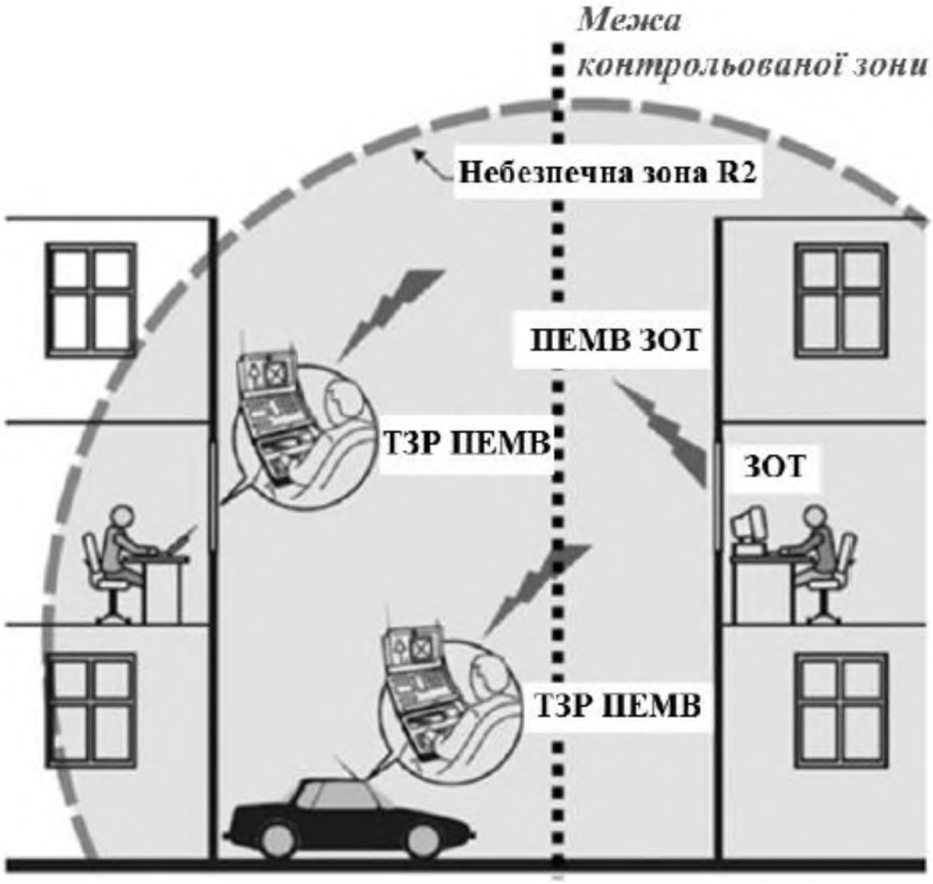


Рисунок 1.4 – Приклади перехоплення ПЕМВ технічними засобами розвідки

Простір навколо ТЗОІ, на межі і за межами якого напруженість електричної (Е) або магнітної (Н) складової електромагнітного поля не перевищує допустимого (нормованого) значення ($E \leq E_H$; $H \leq H_H$) називається небезпечною зоною 2 (R2) (рис. 1.4).

Умови для виникнення електромагнітного каналу витоку інформації (рис. 1.5):

1) відстань від ТЗОІ до межі контрольованої зони має бути менш зони R2 (R< R2);

2) в межах зони R2 можливе розміщення стаціонарних або перевозимих (переносимих) засобів розвідки ПЕМВН

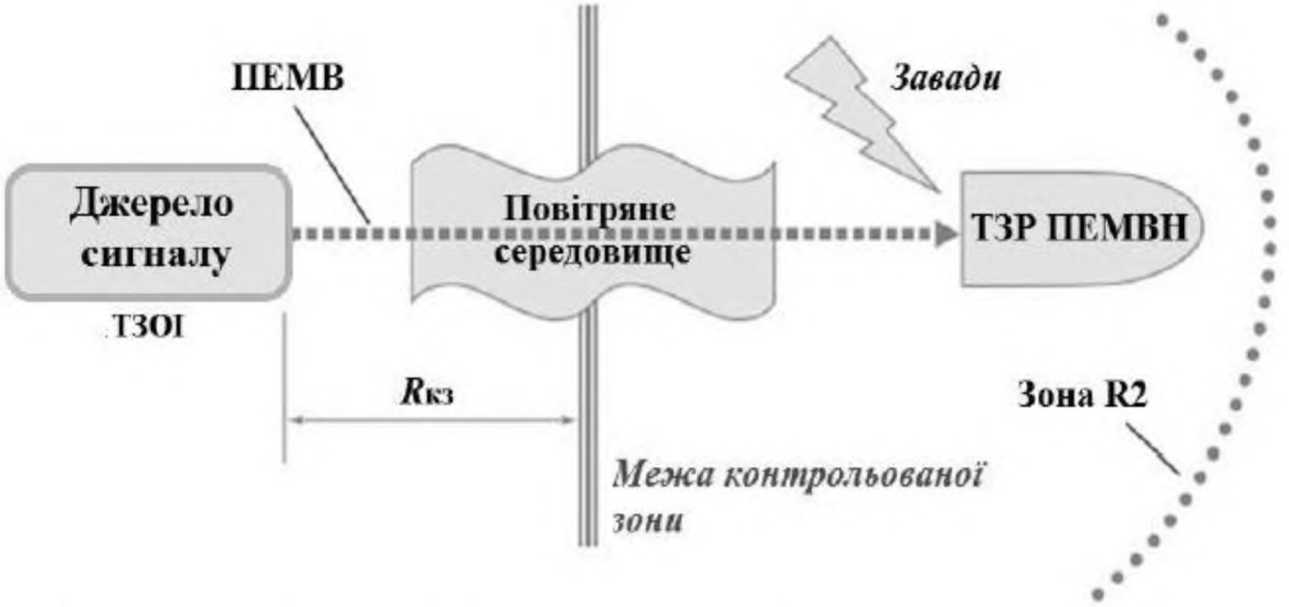


Рисунок 1.5 – Умови для виникнення електромагнітного каналу витоку інформації

1.1.5 Електричні канали витоку інформації

Причинами виникнення електричних каналів витоку інформації ЕКВІ є наведення інформативних сигналів.

Наведення інформативних сигналів – це струми і напруга в струмопровідних елементах, викликані побічними електромагнітними випромінюваннями, ємнісними та індуктивними зв'язками елементів електронних схем.

Де виникають наведення інформативних сигналів:

- у лініях електроживлення ТЗОІ;

- у лініях електроживлення і сполучних лініях ДТЗС;

- у ланцюгах заземлення ТЗОІ і ДТЗС;

- у сторонніх провідниках (металевих трубах систем опалювання, водопостачання, металоконструкціях і т.д.).

Поява інформаційних сигналів в ланцюзі електроживлення ТЗОІ можливо як за рахунок ПЕМВ, так і за наявності внутрішніх паразитних ємнісних і (або) індуктивних зв'язків випрямного облаштування блоку живлення ТЗОІ. Наприклад, в підсилювачі низької частоти струми посилюваних сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі падіння напруги, яка при недостатньому загасанні у фільтрі випрямного пристрою може бути виявлена в лінії електроживлення за наявності магнітного зв'язку між вихідним трансформатором підсилювача і трансформатором випрямного пристрою.

Окрім заземляючих провідників, що служать для безпосереднього з'єднання ТЗОІ з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий дріт мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалювання і водопостачання, металева арматура залізобетонних конструкцій і т.д. Усі ці провідники спільно із заземляючим пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали.

Крім того, в ґрунті навколо заземляючого пристрою виникає електромагнітне поле, яке також є джерелом інформації.

Різні допоміжні технічні засоби, їх сполучні лінії, а також лінії електроживлення, сторонні провідники і ланцюги заземлення грають роль випадкових антен, при безпосередньому (через струмознімач або індукційний датчик) підключенні до яких засоби розвідки ПЕМВН можливе перехоплення інформаційних сигналів.

Залежно від причин виникнення наведення інформативних сигналів можна розділити на:

- наведення в електричних ланцюгах ТЗОІ, викликані інформативними побічними і (або) паразитними електромагнітними випромінюваннями ТЗОІ;

- наведення в сполучних лініях ДТЗС і сторонніх провідниках, викликані інформативними побічними і (чи) паразитними електромагнітними випромінюваннями ТЗОІ;

- наведення в електричних ланцюгах ТЗОІ, викликані внутрішніми ємнісними і (або) індуктивними зв'язками («просочування» інформативних сигналів в ланцюзі електроживлення через блоки живлення ТЗОІ);

- наведення в ланцюгах заземлення ТЗОІ, викликані інформативними ПЕМВ ТЗОІ, а також гальванічним зв'язком схемної (робочої) землі і блоків ТЗОІ.

Приклад перехоплення наведень інформативних сигналів з інженерних комунікацій технічним засобом розвідки ПЕМВН показаний на рис. 1.6.

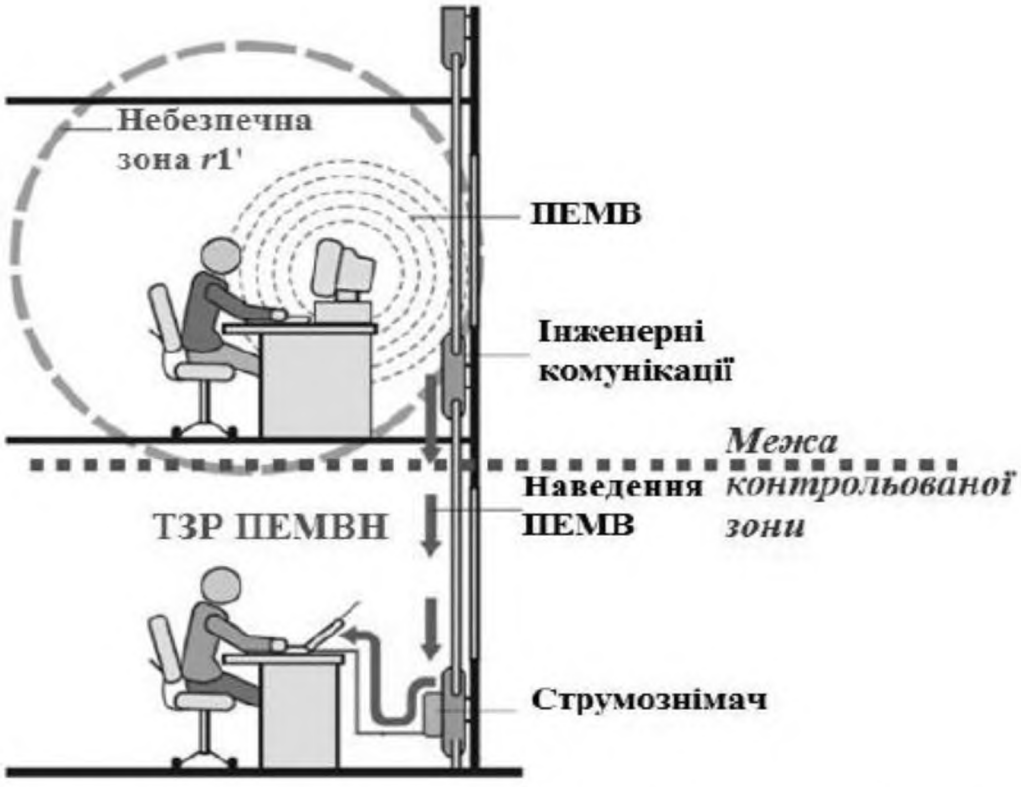


Рисунок 1.6 – Перехоплення наведень інформативних сигналів з інженерних комунікацій

Таким чином, перехоплення інформації, що обробляється технічними засобами, може здійснюватися шляхом (рис. 1.7):

- перехоплення ПЕМВ, що виникають при роботі технічних засобів;

- перехоплення наведень інформаційних сигналів із сполучних ліній ДТЗС і сторонніх провідників;

- перехоплення наведень інформаційних сигналів з ліній електроживлення і заземлення ТЗОІ;

- «високочастотного опромінення» ТЗОІ;

- впровадження в ТЗОІ закладних пристроїв.

1.2 Способи забезпечення захисту інформації від витоку через побічні електромагнітні випромінювання

До способів забезпечення захисту інформації від витоку через ПЕМВ слід віднести наступні.

1. Електромагнітне екранування приміщень в широкому діапазоні частот. Це складне технічне завдання, вимагає значних капітальних витрат, постійного контролю і не завжди можливо з естетичних і ергономічних міркувань.

2. Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ. 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. Здійснюється організаціями, що мають відповідні ліцензії.

3. Криптографічне закриття інформації, або шифрування. Це радикальний спосіб захисту, здійснюється або програмно, або апаратно за допомогою вбудованих засобів. Такий спосіб 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.

4. Активне радіотехнічне маскування. Передбачає формування і випромінювання маскуючого сигналу в безпосередній близькості від засобу,

який захищається. Наразі існує декілька методів активного радіотехнічного маскування: енергетичні методи; метод «синфазної завади»; статистичний метод.

При енергетичному маскуванні 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.

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.

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 на кордоні мінімально допустимої зони безпеки. Однак через відсутність апаратури для безпосереднього вимірювання цієї величини пропонується перерахувати граничну повну ймовірність похибки в необхідне співвідношення сигнал / завада.

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

Відомий підхід до захисту інформації в лінії зв'язку [26] відноситься до техніки електричного зв'язку і призначений для захисту конфіденційної інформації від несанкціонованого зчитування при її передачі двопровідними лініями зв'язку. Досягнутий технічний результат – підвищення ступеня захисту інформації в двопроводній лінії зв'язку без зниження швидкості передачі цифрових даних.

Відомий підхід до захисту інформації в лінії зв'язку [26], заснований на накладенні додаткового сигналу на основний сигнал і на тому, що в момент початку передачі основного сигналу формують додатковий сигнал на приймальній стороні лінії зв'язку, який передають назустріч основному сигналу. При цьому амплітуду і середню частоту передачі додаткового сигналу встановлюють приблизно рівними амплітуді і середній частоті основного сигналу, а для відновлення основного сигналу на приймальній стороні лінії зв'язку формують допоміжну напругу зі струму, що протікає в лінії зв'язку, множать його на коефіцієнт, пропорційний опору лінії зв'язку, і підсумовують з додатковим сигналом.

В якості додаткового сигналу використовують послідовність імпульсів з псевдовипадковою змінною шпаруватістю, миттєву частоту f_2 передачі яких

модулюють на величину $\Delta f_2 << f_2$ в околиці середньої частоти $f_{1.ср}$ основного сигналу при виконанні умови $(f_2 \pm \Delta f_2)_{ср} \approx f_{1.ср}$.

Крім того, в якості додаткового сигналу використовують інформаційне повідомлення, час передачі якого встановлюють менше часу передачі основного сигналу. По закінченню даного повідомлення аж до моменту закінчення циклу передачі основного сигналу формують послідовність імпульсів з псевдовипадково модульованою скважністю і миттєвою частотою, середню частоту передачі яких по лінії зв'язку встановлюють приблизно рівною середній частоті основного сигналу.

На рис. 1.8 наведена функціональна схема пристрою, що реалізує відомий підхід до захисту інформації в лінії зв'язку [26].

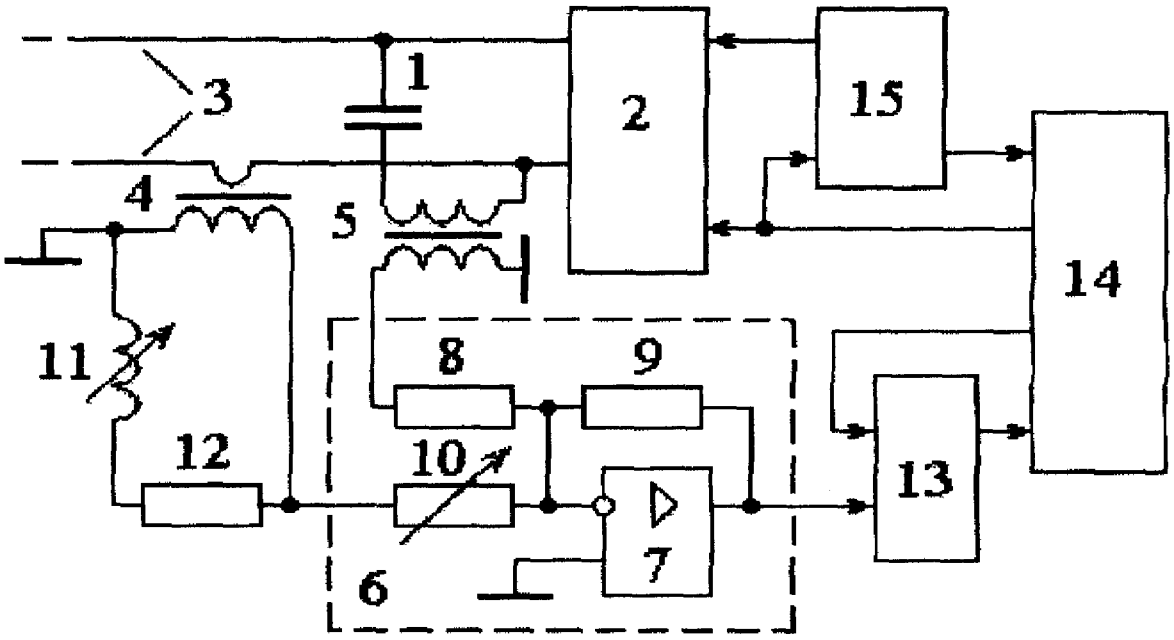


Рисунок 1.7 – Функціональна схема пристрою, що реалізує відомий підхід до захисту інформації в лінії зв'язку [26]

У схемі пристрою (рис. 1.7) застосовані розділовий конденсатор 1, блок сполучення 2, що забезпечує узгодження з лінією зв'язку 3. До проводів лінії зв'язку 3 через трансформатор струму 4 і трансформатор напруги 5 підключені входи аналогового суматора 6 на основі підсилювача 7 з резисторами 8, 9 і

потенціометром 10. Вторинна обмотка трансформатора струму 4 зашунтувана послідовно з'єднаними котушкою змінної індуктивності 11 і резистором 12. Вихід аналогового суматора 6 через один послідовно-паралельний регістр 13 підключений до мікропроцесора 14, який через другий регістр 15 з'єднаний з блоком сполучення 2. Мікропроцесор 14 формує команди керування і є вихідним блоком пристрою.

Недоліком відомого підходу до захисту інформації в лінії зв'язку [26] є те, що існує можливість відновлення інформації по «портрету» побічного електромагнітного випромінювання (ПЕМВ) за рахунок можливого відмінності частот основного і додаткового сигналу.

Відомий підхід до захисту інформації в лінії зв'язку від витоку за рахунок побічних електромагнітних випромінювань і наведень, що реалізовується в відомому пристрої [27], заснований на перетворенні інформаційного сигналу на передавальній стороні безпосередньо перед передачею з послідовного коду в паралельний, передачі його по лінії зв'язку, що є паралельним інтерфейсом, на приймальну сторону і перетворенні сигналу на приймальній стороні з паралельного коду знову в початковий послідовний код перед подачею його безпосередньо в приймач.

Технічним результатом, на досягнення якого спрямований відомий підхід [27], є підвищення ефективності захисту інформації, що циркулює в каналах системи обробки інформації, від витоку за рахунок ПЕМВН. Даний технічний результат досягається за рахунок того, що клавіатура для захисту інформації, що циркулює в системі обробки інформації, містить розташовану на корпусі панель, на якій розміщена, щонайменше, одна клавіша, підключена електричними виводами до входів формувача скан-кодів, з'єднаного виходом з входом перетворювача послідовного коду в паралельний, виходи якого через багаторозрядну лінію зв'язку з'єднані з входами перетворювача паралельного коду в послідовний, генератор тактової частоти, вихід якого з'єднаний з синхровходами перетворювача послідовного коду в паралельний, перетворювача паралельного коду в послідовний і формувача скан-кодів, а

також за рахунок того, що формувач кодів виконаний у вигляді формувача скан-кодів, а також за рахунок того, що перетворювач паралельного коду в послідовний виконаний з можливістю підключення до материнської плати системного блоку персональної ЕОМ, і за рахунок того, що перетворювач паралельного коду в послідовний виконаний з можливістю установки на материнській платі системного блоку персональної ЕОМ.

Даний технічний результат досягається також за рахунок того, що перетворювач паралельного коду в послідовний виконаний з можливістю установки всередині системного блоку персональної ЕОМ, і за рахунок того, що багаторозрядна лінія зв'язку виконана з можливістю використання однієї частини розрядів кабелю для передачі інформативних логічних цифрових сигналів, а інший її частини – для передачі закодованих логічних цифрових сигналів, і, крім того, за рахунок того, що формувач скан-кодів і перетворювач послідовного коду в паралельний розміщені в одному корпусі.

Недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок побічних електромагнітних випромінювань і наведень, що реалізовується в відомому пристрої [27] є можливість відновлення інформації для послідовних інтерфейсів, розрядність посилок яких мала.

Відомий підхід до захисту інформації в лінії зв'язку від витоку за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН) [28], що належить до обчислювальної техніки і може бути використаний в комп'ютерних технологіях в системах обробки і передачі інформації для захисту переданої інформації. Технічним результатом є підвищення ефективності захисту інформації, що циркулює в каналах системи обробки інформації, від витоку за рахунок ПЕМВН. Технічний результат досягається шляхом зниження ймовірності розпізнавання переданої інформації в лінії зв'язку.

Відомий підхід до захисту інформації в лінії зв'язку від витоку за рахунок ПЕМВН [28] заснований на накладенні додаткового сигналу на основний сигнал і на те, що припиняють передачу цифрових сигналів по лінії зв'язку,

доповнюють цю лінію додатковою лінією і синхронно разом із передачею по лінії, що захищається, передають по цій додатковій лінії сигнали, амплітудні і частотно-часові параметри яких підібрані таким чином, щоб портрет сумарного ПЕМВ від обох ліній, що виникає в навколишньому просторі при передачі інформації, був ідентичний для кожного такту передачі.

Крім того, може бути доцільно додатково перетворити цифровий сигнал, який передається, з початкового послідовного коду в паралельний для додаткового ускладнення завдання відновлення інформації по можливо перехоплених ПЕМВ.

При цьому лінія зв'язку може бути виконана протяжною в просторі.

В окремому випадку для передачі інформації в якості лінії зв'язку може використовуватися симетрична лінія або набір з паралельних симетричних ліній, оскільки застосування відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок ПЕМВН [28] технічно можливо і в симетричних лініях зв'язку.

Реалізація відомого підходу до захисту інформації [28], що циркулює в системі обробки інформації з використанням електронних цифрових пристроїв, полягає в доповненні основної лінії передачі додатковою лінією і синхронною передачею по цій додатковій лінії спеціальних сигналів, амплітудні і частотно-часові параметри яких підібрані таким чином, щоб портрет ПЕМВН від обох ліній в цілому, що виникає в навколишньому просторі при передачі інформації, був ідентичний для кожного такту передачі (див. рис.1.8).

На рис. 1.8-1.9 введено такі позначення:

1 – електронний цифровий пристрій на передавальній стороні інформаційного ланцюга;

2 – електронний цифровий пристрій на приймальній стороні інформаційного ланцюга;

3 – основна лінія передачі;

4 – додаткова лінія передачі.

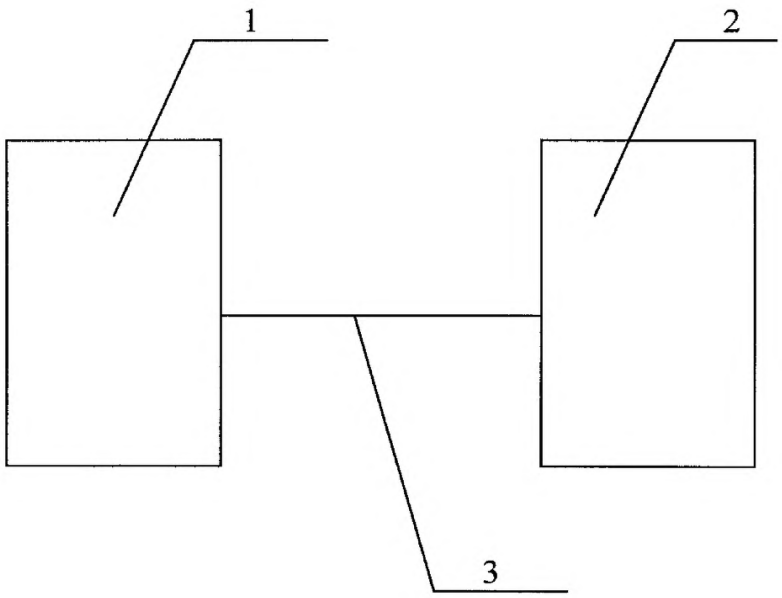
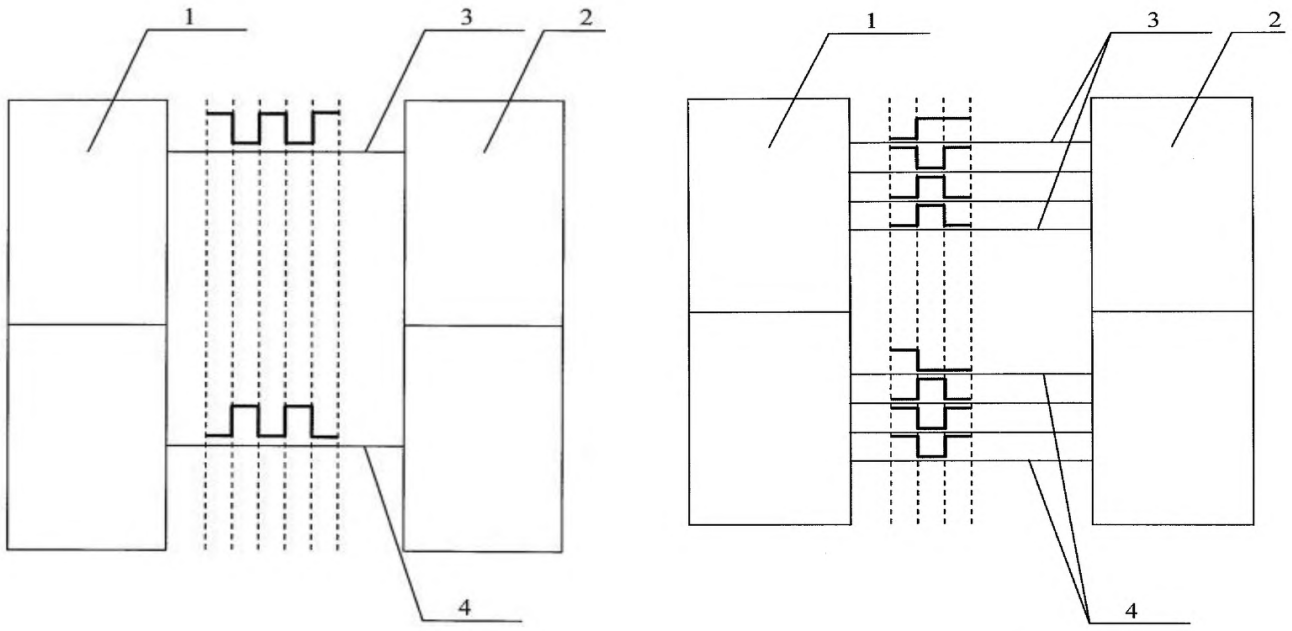


Рисунок 1.8 – Схема з'єднання двох електронних цифрових пристроїв за допомогою лінії зв'язку, яку можна розривати для призупинення зв'язку між цими пристроями



а б

Рисунок 1.9 – Принцип формування сигналів в додатковій лінії, якщо основною лінією є: однорозрядний послідовний уніполярний інтерфейс (а), багаторозрядний паралельний уніполярний інтерфейс (б)

Недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок ПЕМВН [28] є висока складність технічної реалізації і зниження швидкості роботи ЗОТ, перші внесенням в нього додаткових змін. Інший недолік відомого підходу полягає в неможливості повного перекриття в частотної області ПЕМВ від основної та додаткової лінії через використання в обох лініях однотипних і рівних по потужності сигналів.

Найбільш близьким за технічною сутністю до запропонованого підходу і обраним як прототип є підхід до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [29], що полягає 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. 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 і ті ж файли багаторазово записують на одне і те ж місце в цифрових накопичувачах для виконання умови неперевищення сумарного розміру всіх файлів, які копіюються, розміру пам'яті цифрового накопичувача, на якому записані сформовані файли. При проходженні сформованих файлів по з'єднувальним лініям типових вузлів і блоків засобів обчислювальної техніки виникають власні неінформативні побічні електромагнітні випромінювання. При цьому 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.

Відомий підхід до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [29] 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 підходу підхід до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [29] показана на рис. 1.10.

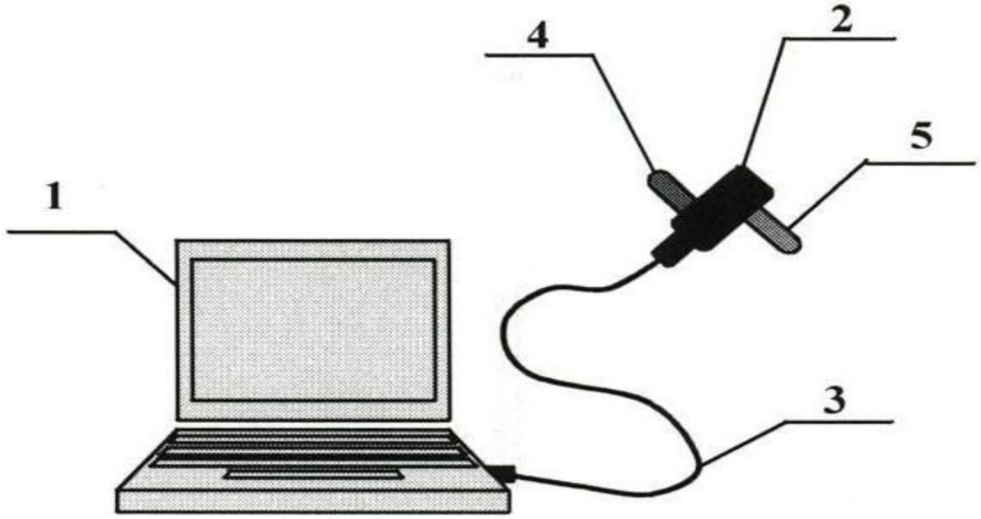


Рисунок 1.10 – Схема розміщення обладнання для реалізації відомого підходу до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [29]

На рис. 1.10 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.

На рис. 1.11 показано головне вікно управління додатком для операційної системи Windows «Пристрій для формування маскуючих завад», а на рис. 1.12 – можливий вид вікна керування вбудованим генератором неінформативних файлів.

Після запуску програми користувач (власник інформації, що захищається) в поле вибору 6 допоміжного флеш-накопичувача 5 головного вікна керування додатком (рис. 1.11) повинен вибрати його зі списку підключених флеш-накопичувачів. Неінформативні файли, які будуть копіюватися з накопичувача на накопичувач, користувач вибирає в списку 7 «Передані файли». Праворуч від списку розташовані кнопки управління його вмістом. Кнопка 9 призначена для заповнення списку усіма файлами, які знаходяться в одній директорії з виконуваним файлом програми.

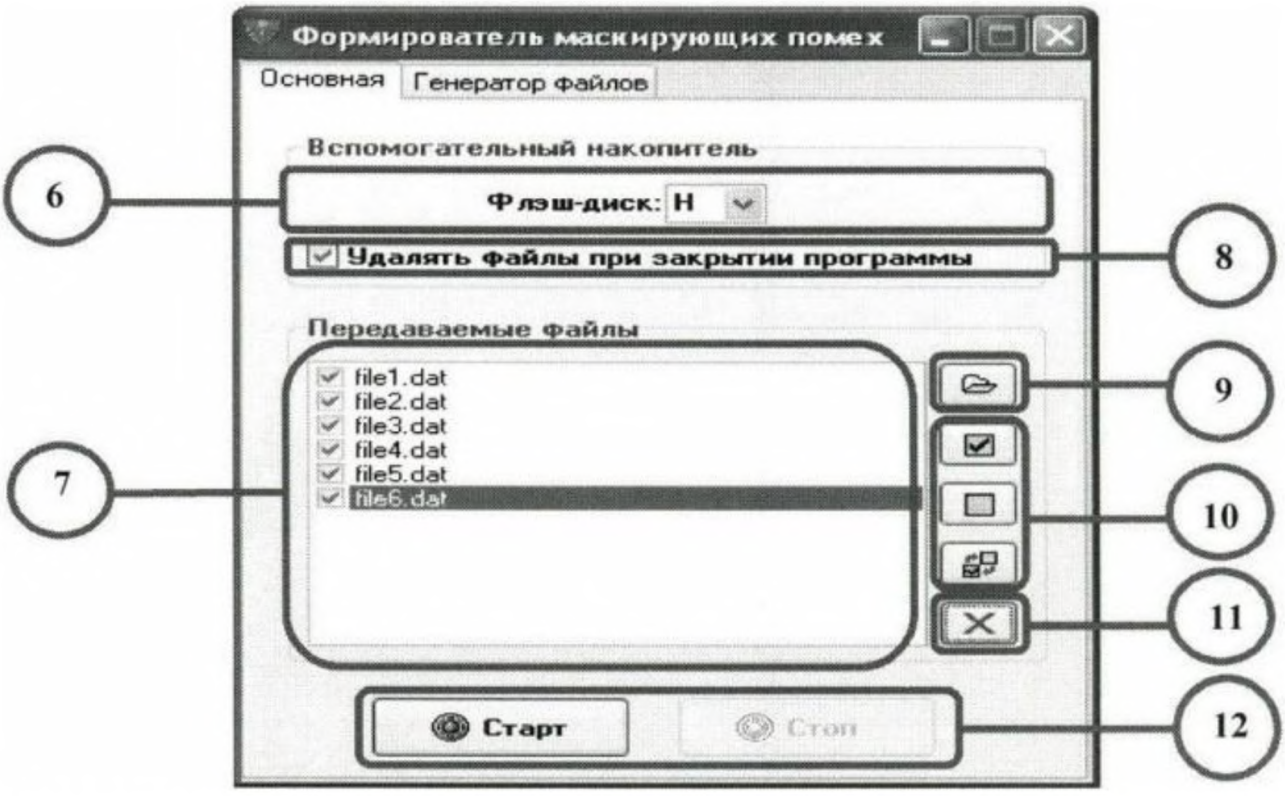


Рисунок 1.11 – Головне вікно управління додатком для операційної системи Windows «Пристрій для формування маскуючих завад»

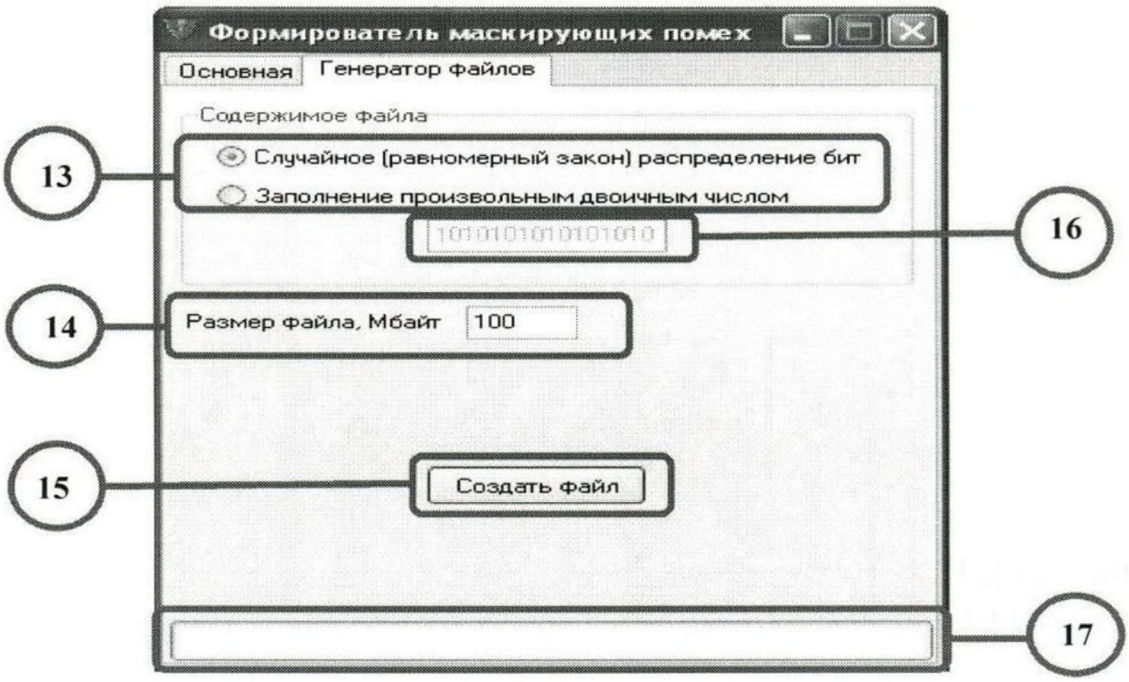


Рисунок 1.12 – Можливий вид вікна керування вбудованим генератором неінформативних файлів

Для прискорення роботи з прапорцями призначені кнопки 10, вони дозволяють встановити прапорці у всіх файлів в списку, прибрати прапорці у всіх файлів в списку (рис. 1.11). В копіюванні братимуть участь всі файли, зазначені в списку, незалежно від стану прапорців, тому після їх установки слід натиснути на кнопку 11, яка призначена для видалення зі списку файлів, не зазначених прапорцями. Для зупинки процесу формування завад слід натиснути на кнопку 12 «Стоп», після чого програма переходить в режим закінчення роботи, який триватиме до тих пір, поки не завершиться процес копіювання останнього файлу. Після закриття програми неінформативні файли, скопійовані на допоміжний накопичувач 5, можуть бути автоматично видалені або залишитися, в залежності від стану прапорця 8 «Видаляти файли при закритті програми».

Вибір вмісту формованого файлу здійснюється за допомогою перемикача 13 вікна керування вбудованим генератором неінформативних файлів (рис. 1.12). Якщо обрана позиція «Заповнення довільним двійковим числом», то стає доступним поле 16, призначене для введення двійковій маски. Вибір розміру неінформативного файлу здійснюється за допомогою перемикача 14 вікна управління вбудованим генератором неінформативних файлів. Для запуску формування файлу слід натиснути на кнопку 15 «Створити файл». Про стан процесу формування файлу можна судити по індикатору прогресу 17, який розташований в нижній частині вікна програми.

Отже, в якості неінформативних файлів можуть бути використані спеціальні файли, сформовані за допомогою вбудованого генератора файлів, що представляють собою послідовність байтів, які зчитуються або записуються, що несуть інформацію, яка потребує захисту, і розміщені на спеціальному флеш-накопичувачі F1.

Переваги відомого підходу до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень [29] полягають в наступному:

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

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

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

• реалізація підходу 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 підхід забезпечить підвищення рівня захищеності інформації від витоку за рахунок ПЕМВН.

Недоліком підходу до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень (прототипу) [29] є низький коефіцієнт перекриття спектрів інформативного і неінформативного сигналів, обумовлений наступними факторами:

1) в підході-прототипі за рахунок зміни способу формування бітових послідовностей не можна домогтися точного співпадіння частотних спектрів маскуючого і інформативного сигналів;

2) можливість періодичної корекції огинаючої спектра в режимі реального часу за рахунок зміни структури бітової послідовності означає вимір випромінювання ЗОТ, яке в процесі роботи вже буде містити неінформативне випромінювання.

1.4 Висновок. Постановка задачі

В розділі проаналізовано технічні канали витоку та руйнування інформації. Встановлено, що найбільшу небезпеку витоку інформації через ПЕМВН представляють вузли та внутрішнього облаштування ПЕОМ, які опрацьовують інформацію в послідовному коді. Інформативні випромінювання

в паралельному коді наразі розшифровці не піддаються, оскільки через електромагнітні випромінювання неможливо визначити належність випроміненого імпульсу до якогось розряду коду. Дослідженню на ПЕМВН підлягають наступні пристрої: відеопідсистема; накопичувачі на жорстких і гнучких дисках; пристрої CD, CD-R, CD-RW, DVD, DVD-RW; клавіатура; послідовні порти; принтери.

В розділі проаналізовано існуючі підходи до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень. Встановлено, що недоліком відомого підходу до захисту інформації в лінії зв'язку [26] є те, що існує можливість відновлення інформації по «портрету» побічного електромагнітного випромінювання (ПЕМВ) за рахунок можливої відмінності частот основного і додаткового сигналу.

Встановлено, що недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок побічних електромагнітних випромінювань і наведень, що реалізовується в відомому пристрої [27] є можливість відновлення інформації для послідовних інтерфейсів, розрядність посилок яких мала.

Встановлено, що недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок ПЕМВН [28] є висока складність технічної реалізації і зниження швидкості роботи ЗОТ, перші внесенням в нього додаткових змін. Інший недолік відомого підходу полягає в неможливості повного перекриття в частотної області ПЕМВ від основної та додаткової лінії через використання в обох лініях однотипних і рівних по потужності сигналів.

Встановлено, що недоліком підходу до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень (прототипу) [29] є низький коефіцієнт перекриття спектрів інформативного і неінформативного сигналів, обумовлений наступними факторами:

1) в підході-прототипі за рахунок зміни способу формування бітових послідовностей не можна домогтися точного співпадіння частотних спектрів маскуючого і інформативного сигналів;

2) можливість періодичної корекції огинаючої спектра в режимі реального часу за рахунок зміни структури бітової послідовності означає вимір випромінювання ЗОТ, яке в процесі роботи вже буде містити неінформативне випромінювання.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів

Запропонований підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів відноситься до області обчислювальної техніки і може бути використаний для захисту інформації, що обробляється засобами обчислювальної техніки, зокрема, від витоку по каналу побічних електромагнітних випромінювань і наведень. Технічний результат – підвищення коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки. У запропонованому підході до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень здійснюють формування N файлів, потім подальше їх розбиття на M частин, причому кожна з них містить файли, що утворюють при проходженні по з'єднувальним лініям і вузлам засобу обчислювальної техніки сигнали з певним частотним спектром потужності. Далі відбувається копіювання цих частин файлів на M цифрових накопичувачів і одночасне зчитування файлів, обраних зі списку на кожному накопичувачі за випадковим законом, з M цифрових накопичувачів і їх запис в область внутрішньої пам'яті засобу обчислювальної техніки, після цього багато разів повторюється зчитування і запис файлів протягом часу, необхідного для маскування інформативного сигналу.

Частотний спектр сигналу, що формується при проходженні неінформативних файлів по з'єднувальним лініям, розбивають на K частотних смуг і обчислюють інтегральне значення потужності $U^{(p)}$ цього сигналу в p-й смузі ($1 \le p \le K$). Коефіцієнт перекриття спектрів неінформативного і інформативного сигналу в p-й частотній смузі дорівнює:

$$S^{(p)} = \begin{cases} 1, U^{(p)} \geq Z^{(p)}; \\ 0, U^{(p)} < Z^{(p)}. \end{cases} \quad (2.1)$$

де $U^{(p)}$ – інтегральне значення потужності неінформативного сигналу в р-й частотній смузі; $Z^{(p)}$ – інтегральне значення потужності інформативного сигналу в р-й частотній смузі.

Коефіцієнт перекриття спектрів неінформативного і інформативного сигналу у всьому діапазоні частот S дорівнює:

$$S = \frac{1}{K} \sum_{p=1}^{M} S^{(p)}, \quad (2.2)$$

при цьому якщо $S \geq 0.95$, то неінформативний сигнал буде забезпечувати перекриття сигналу у всьому спектрі.

У запропонованому підході до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів це завдання вирішується тим, що формують N файлів, вміст яких не потрібно захищати, запис і зчитування файлів здійснюють багаторазово протягом часу, необхідного для маскування інформативного сигналу. При проходженні файлів по з'єднувальним лініям типових вузлів і блоків засобів обчислювальної техніки виникають власні неінформативні побічні електромагнітні випромінювання, при цьому 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 файлах, що формуються. Додатково до цього після того як формують N файлів, ділять їх на M частин, кожна з яких містить файли, що утворюють сигнали з певним частотним спектром потужності. Кожну частину файлів із загального списку записують на окремий цифровий накопичувач. Після цього одночасно з і-го (i=1...M) цифрового накопичувача зчитують файл, обраний зі списку за випадковим законом, і записують його в область внутрішньої пам'яті ЗОТ. При цьому одні й ті ж файли багаторазово записують

на одне й те ж місце в області внутрішньої пам'яті ЗОТ для виконання умови неперевищення сумарного розміру всіх файлів, що копіюються, розміру області внутрішньої пам'яті, в яку записуються сформовані файли.

Крім того, корекцію огинаючої спектра неінформативних побічних електромагнітних випромінювань забезпечують за рахунок зміни порядку запису (зчитування) M частин файлів на M цифрових накопичувачів.

В якості цифрових накопичувачів розглядаються флеш-накопичувачі, підключені до ПЕОМ через USB-концентратори і інтерфейсні кабелі. У загальному випадку їх кількість M обмежується кількістю вільних портів інтерфейсів в ЗОТ і кількістю приймально-передавальних пар інтерфейсних кабелів.

Запропонований підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів реалізується у такий спосіб (рис. 2.1).

Формують N неінформативних файлів розміром 1 Мбайт, що представляють собою бітові послідовності, за допомогою програмно-реалізованого генератора псевдовипадкових чисел або з використанням 16-розрядної бітової маски. При формуванні файлу з використанням 16-розрядної бітової маски її поєднання біт буде періодично повторюватися. Зміст файлів не вимагає захисту. Характер розподілу біт в файлі впливає на параметри спектра (інтенсивність і ширину спектра) маскуючих сигналів, які формуються. Крім того, інтенсивність спектра визначається також характеристиками кабелю.

З огляду на невизначеність взаємного положення спектра інформативного сигналу і максимальної інтенсивності спектра неінформативного сигналу можлива ситуація, коли максимум інтенсивності спектра маскуючого сигналу не збігається з частотою інформативного сигналу. Це призводить до зниження коефіцієнта перекриття спектрів неінформативного і інформативного сигналу у всьому діапазоні частот.

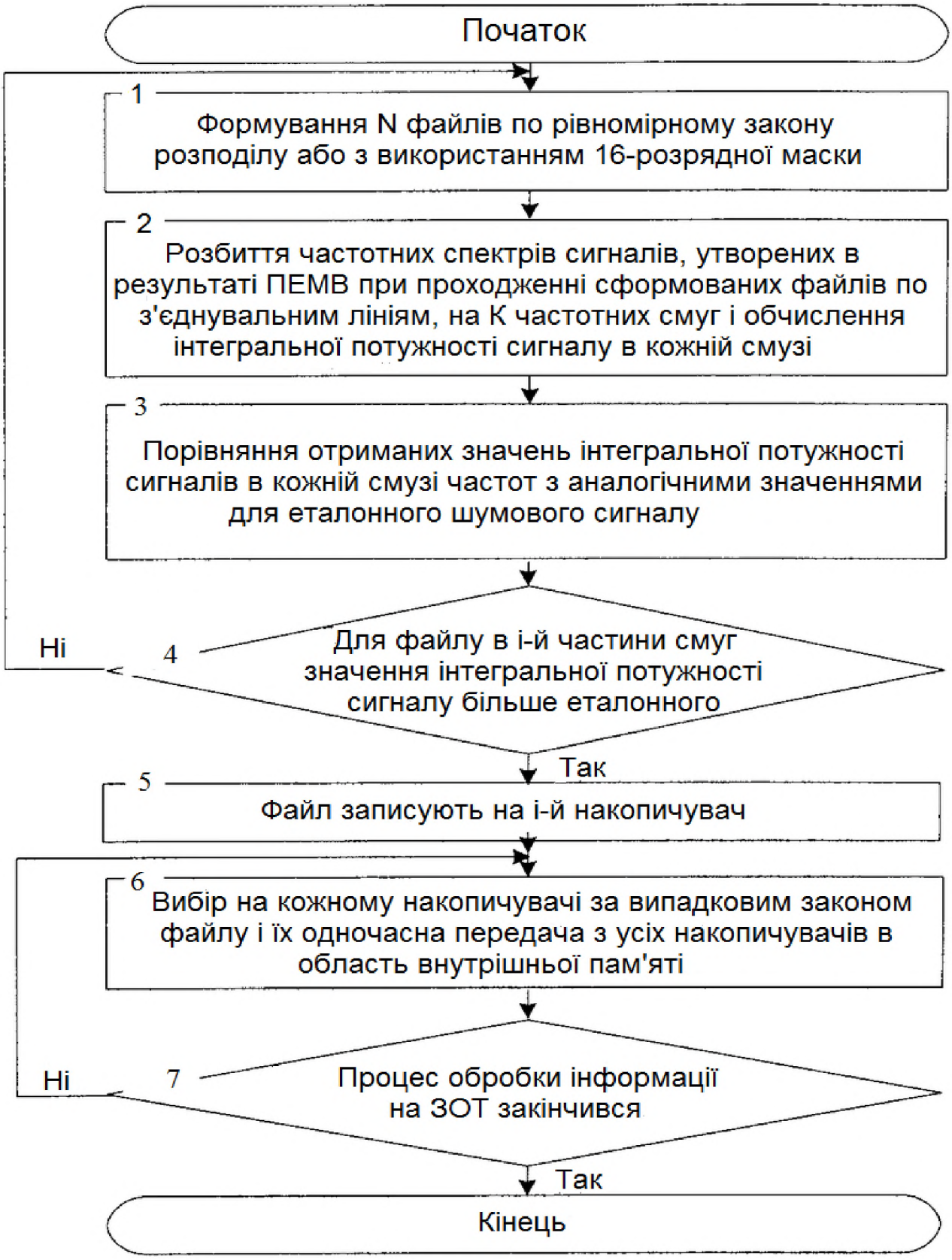


Рисунок 2.1 – Алгоритм формування маскуючих сигналів згідно запропонованого підходу

Керування інтенсивністю спектра маскуючого сигналу можливо шляхом корекції огинаючої спектра маскуючого сигналу за рахунок зміни структури бітової послідовності неінформативних файлів. Структура бітової послідовності неінформативних файлів залежить від використовуваного способу їх формування.

Розбивають частотні спектри сигналів, утворених в результаті проходження кожного сформованого файлу по з'єднувальним лініям, на K частотних смуг і обчислюють інтегральне значення потужності $U^{(p)}$ цього сигналу в p-й смузі ($1 \le p \le K$).

Порівнюють $U^{(p)}$ зі значенням інтегральної потужності необхідного шумового сигналу $V^{(p)}$. Необхідний шумовий сигнал виходить в результаті аналізу випромінюючих властивостей ЗОТ або вказується в документації.

Потім розбивають N файлів на M частин наступним чином. Файл, який формує сигнал при проходженні по з'єднувальним лініям типових вузлів і блоків засобів обчислювальної техніки, записують на i-й (i=1...M) накопичувач, якщо нерівність $U^{(p)} \ge V^{(p)}$ виконується для всіх p таких, що

$$1+\frac{K}{M}\ (i-1) \le p \le \frac{K}{M} \cdot i\,. \qquad (2.3)$$

Якщо жоден зі сформованих файлів не записаний на i-й носій, то процес формування файлів повторюють.

Після цього одночасно з i-го (i=1...M) цифрового накопичувача зчитують файл, обраний зі списку за випадковим законом, і записують його в область внутрішньої пам'яті ЗОТ. Одночасна передача більш 2 файлів можлива при наявності декількох Hub-пристроїв для використовуваного інтерфейсу.

При продовженні процесу обробки інформації на ЗОТ зчитування і запис файлів здійснюють багаторазово протягом часу, необхідного для маскування інформативного сигналу. Повторно неінформативні файли копіюються на одне і те ж місце в області внутрішньої пам'яті ЗОТ, тому обсяг займаної внутрішньої пам'яті не перевищує сумарного обсягу всіх файлів, що

копіюються. Ємність носіїв не менше 4 Гбайт, що дозволяє зберігати достатню для забезпечення випадковості переданого сигналу кількості файлів.

При реалізації запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів виникає ситуація, коли інтегральні значення потужності шумових сигналів, випромінюваних при проходженні файлів, що знаходяться на різних носіях, в межах однієї і тієї ж смуги частот перевищують значення необхідного шумового сигналу, тобто при записі і зчитуванні цього файлу. Таким чином, при великій кількості носіїв інформації M виникають ситуації, коли необхідне сумарне неінформативне випромінювання утворюється надмірною кількістю одночасно переданих файлів, від яких прямо пропорційно залежить завантаженість центрального процесора (ЦП). Для зниження задіяного апаратного ресурсу (завантаженість ЦП) необхідно здійснити наступні кроки до запису та зчитування файлів, як показано на рис. 2.2.

Формують дерево графів наступним чином (рис.3), на кожному рівні i залишають вузли $U_{bc}^{(p)}$, якщо інтегральне значення енергії сигналу, який формується при проходженні c-го файлу з b-го накопичувача в смузі частот p більше, ніж у необхідного шумового сигналу $V^{(p)}$. Вузли на сусідніх рівнях з'єднуються, причому в кожній з гілок утвореного дерева може перебувати тільки по одному файлу з кожного накопичувача.

Привласнюють вагу кожного вузла в графі наступним чином: якщо в гілці дерева вузол U_{bc} зустрічається в перший раз, йому присвоюється вага 1, якщо повторно, то 0.

Здійснюють пошук в глибину по дереву починаючи з кореня. По зворотному маршруту від нижнього рівня до кореня встановлюють, які файли необхідно передавати одночасно для досягнення необхідного рівня захищеності інформації. Кількість файлів, що одночасно передаються, D дорівнює сумі ваг усіх вузлів на шляху від кореня до нижнього рівня.

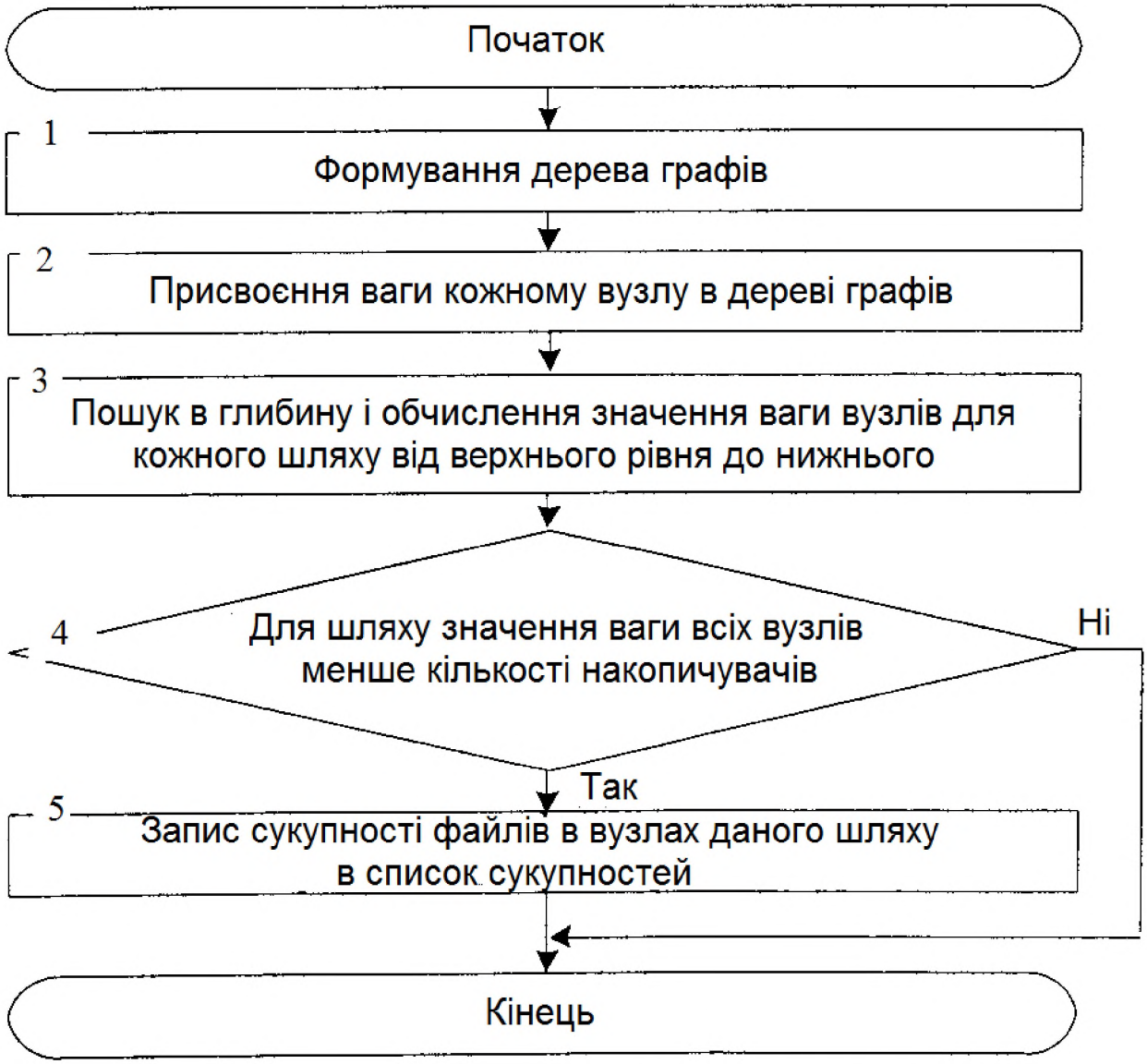


Рисунок 2.2 – Алгоритм формування списку сукупностей файлів

Якщо D<M, то сукупність файлів, які необхідно одночасно передавати, заносять в список.

Таким чином, перед передачею сукупності файлів, отриманої в результаті випадкового вибору файлу на кожному накопичувачі, перевіряють їх на приналежність до будь-якої сукупності файлів з вищевказаного списку. Якщо вся сукупність файлів зі списку входить до складу сукупності файлів, що перевіряються перед передачею, то файли, які не потрапили в сукупність в списку, не передаються. Причому порівняння відбувається спочатку з сукупностей в списку, що мають найменшу кількість елементів.

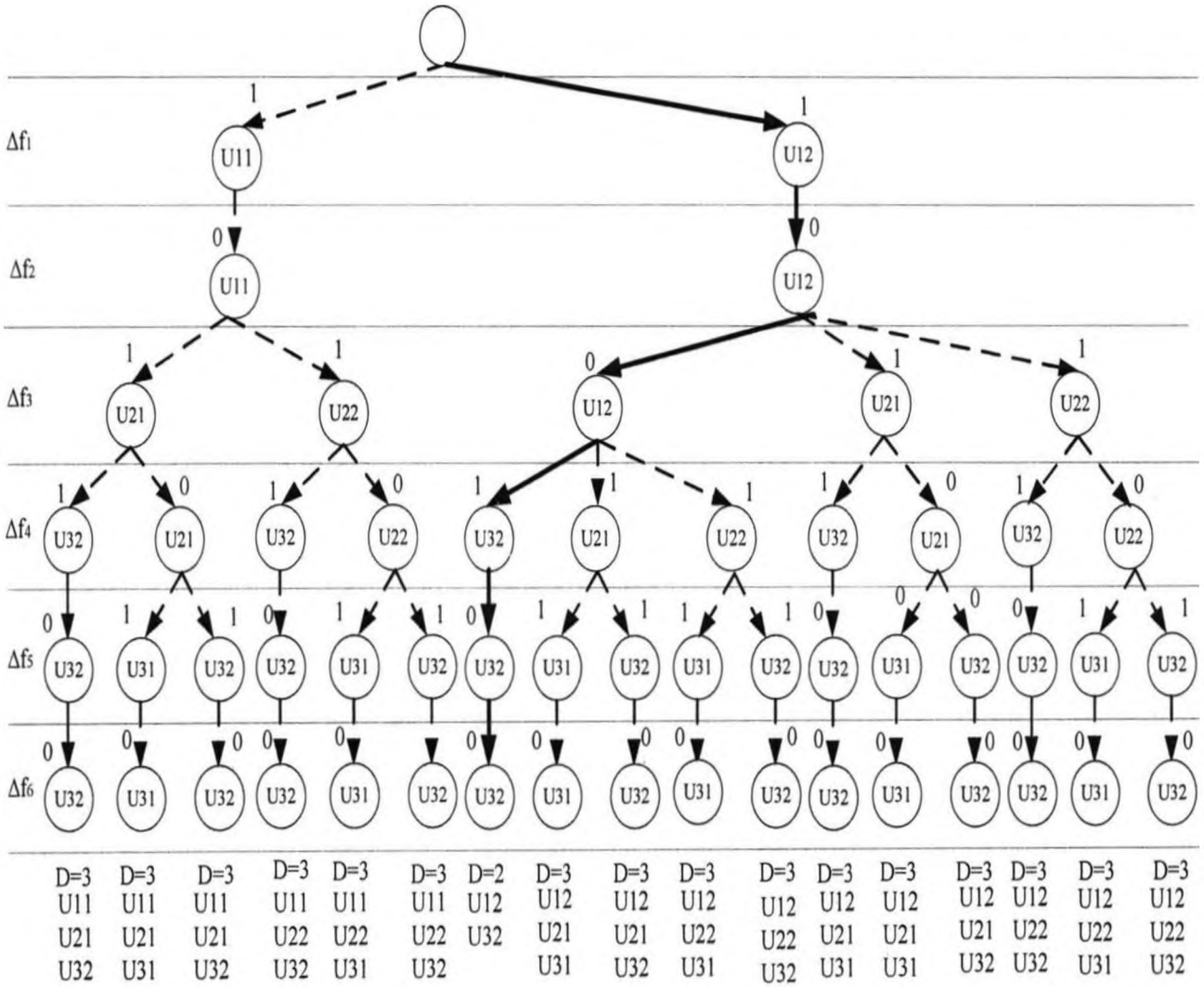


Рисунок 2.3 – Дерево перекриттів маскуючих сигналів, реалізованих згідно запропонованого підходу, і потрібного маскуючого сигналу

Процес зміни порядку запису і зчитування файлів пояснюється на прикладі для 3-х накопичувачів (M=3) і при розподілі спектрів сигналів на 6 смуг (K=6). На кожному носії записано по два файли. Для першого файлу на першому накопичувачі справедливо, що інтегральне значення потужності сигналу, утвореного при проходженні цього файлу по з'єднувальним лініям і вузлам ЗОТ, більше еталонного в 1 і 2 смузі частот:

$U_{11}^{(p)} \geq V^{(p)}$ для $p \in [1; 2]$.

Аналогічно для інших файлів:

$U_{12}^{(p)} \geq V^{(p)}$ для $p \in [1; 3]$;

$U_{21}^{(p)} \geq V^{(p)}$ для $p \in [3; 4]$;

$U_{22}^{(p)} \geq V^{(p)}$ для $p \in [3; 4]$;

$U_{31}^{(p)} \geq V^{(p)}$ для $p \in [5; 6]$;

$U_{32}^{(p)} \geq V^{(p)}$ для $p \in [4; 6]$.

Після складання дерева графів (рис. 2.3) і обчислення ваг шляхів, сукупність файлів (U_{12}, U_{32}) заносять в список, оскільки вага шляху з вузлами U_{12} і U_{32} дорівнює 2 (D=2). Якщо в результаті випадкового вибору файлу на кожному носії необхідно копіювати одночасно сукупність файлів (U_{12}, U_{21}, U_{32}) або (U_{12}, U_{22}, U_{32}), то копіювання файлів з другого носія не здійснюють. Таким чином, відбувається корекція огинаючої спектра неінформативних побічних електромагнітних випромінювань за рахунок зміни порядку запису і зчитування неінформативних файлів в область внутрішньої пам'яті.

При реалізації запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів досягається результат, еквівалентний підвищенню коефіцієнта перекриття інформативних і неінформативних (маскуючих) сигналів випромінюваних ЗОТ, що в значній мірі ускладнює або виключає прийняття рішення про виявлення і розпізнавання (класифікації) інформативних ПЕМВ, які надходять на вхід приймача перехоплення. Інтенсивність неінформативних завад не перевищує норм на промислові завади.

2.2 Оцінка ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів

В якості підтвердження ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів було проведено моделювання в середовищі Matlab / Simulink [35].

Структура імітаційної моделі реалізації запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів представлена на рис. 2.4.

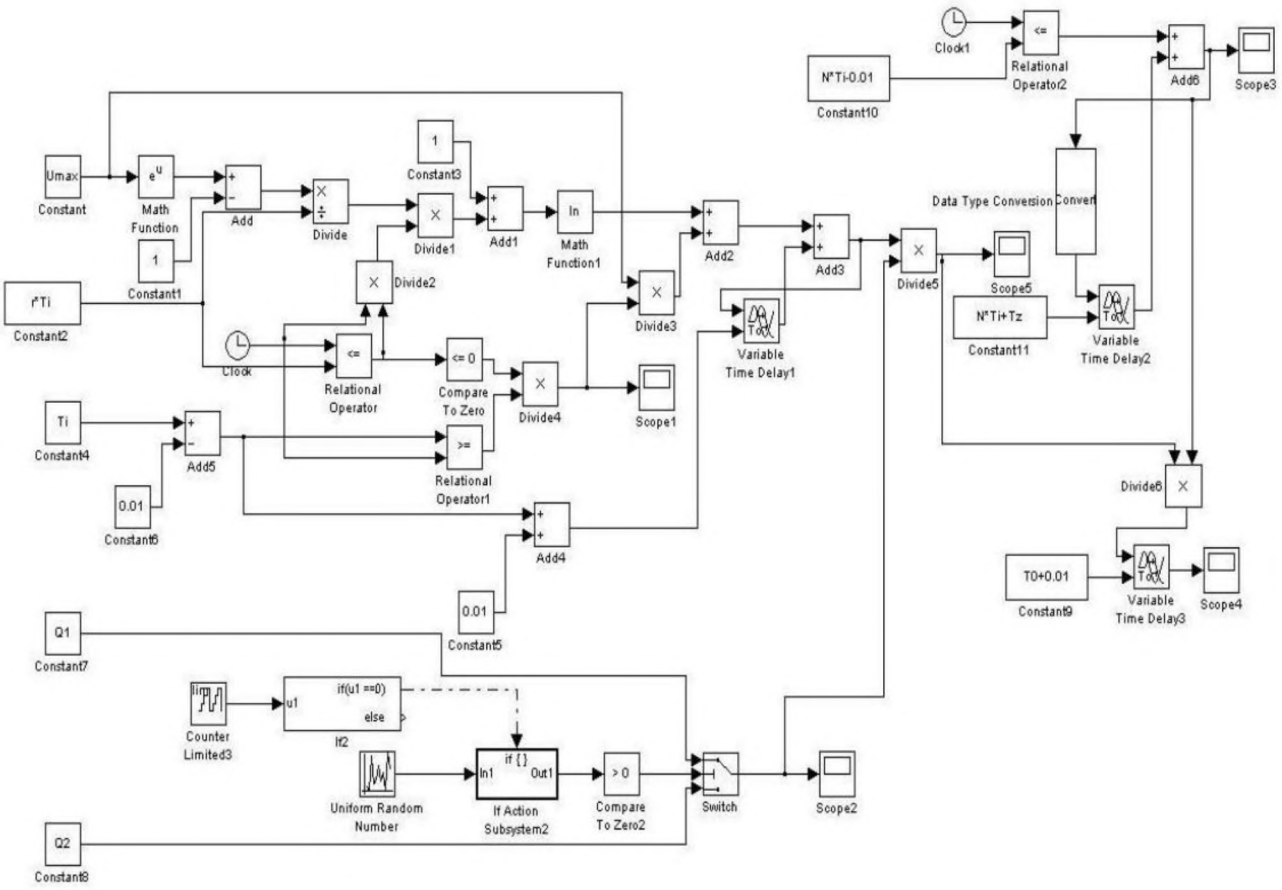


Рисунок 2.4 – – Структура імітаційної моделі для оцінки ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів

При моделюванні були встановлені наступні умови: коефіцієнт загасання не менше 60 дБ, діапазон частот від 1 Гц до 480 МГц. Зазначені спектри діляться на 128 рівнів смуги частот в діапазоні від 1 до 480 МГц і обчислюється коефіцієнт перекриття інформативного і неінформативного сигналу у всьому спектрі.

На рис. 2.5 показаний частотний спектр випромінюваного ЗОТ інформативного сигналу.

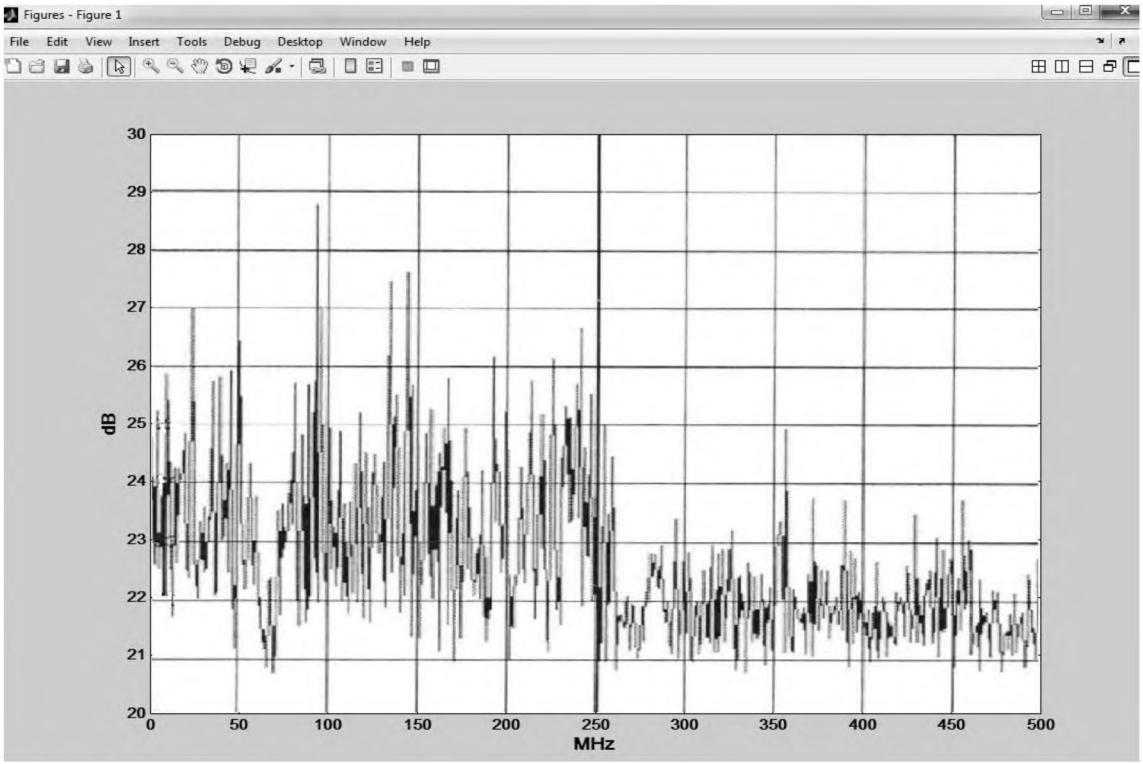


Рисунок 2.5 – Частотний спектр інформативного сигналу, випромінюваного ЗОТ

На рис. 2.6 показаний частотний спектр маскуючого сигналу, отриманого в результаті моделювання відомого підходу-прототипу, а на рис. 2.7 – частотний спектр маскуючого сигналу, отриманого в результаті моделювання запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів для 2 цифрових накопичувачів.

Для представлених на рис. 2.4 і рис. 2.5 спектрів коефіцієнт перекриття склав S_1=0,82031. Отриманий результат свідчить про недостатню міру перекриття інформаційного сигналу маскуючим, що дозволяє зробити висновок про недостатню захищеність інформації, яка оброблюється ЗОТ. Для спектрів на рис. 2.4 і рис. 2.6 коефіцієнт перекриття дорівнює S_2=0,974375.

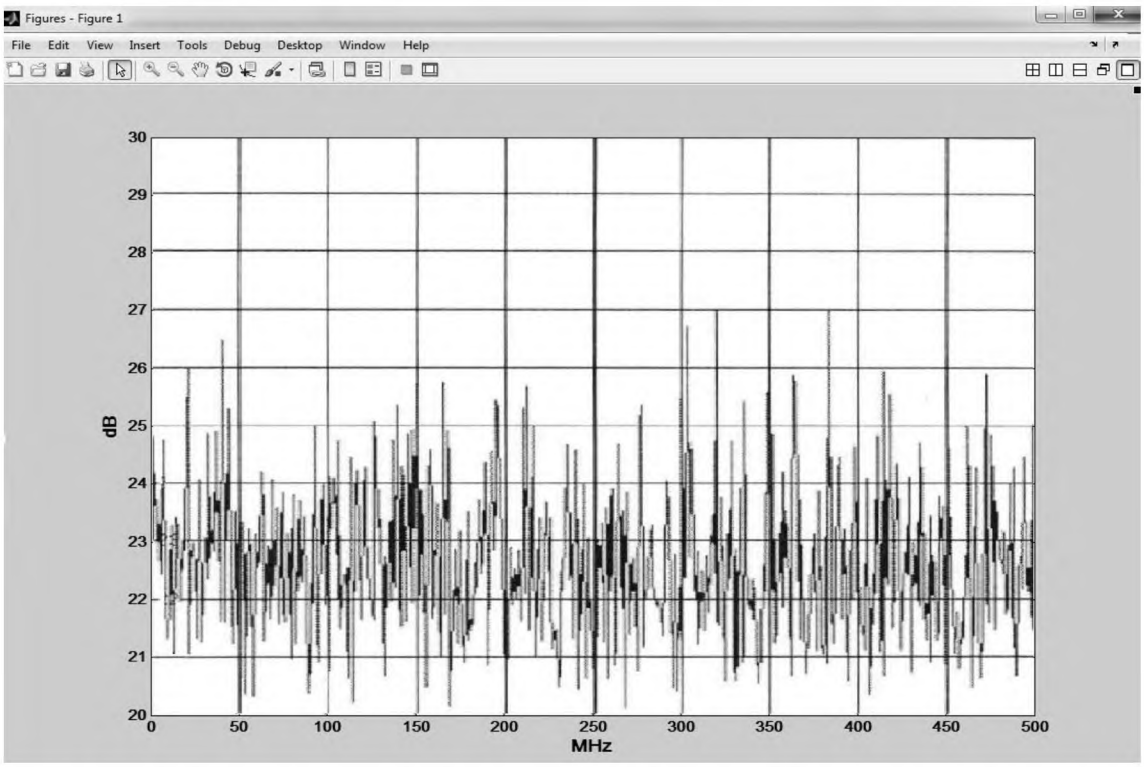


Рисунок 2.6 – Частотний спектр маскуючого сигналу, реалізованого відповідно до підходу-прототипу

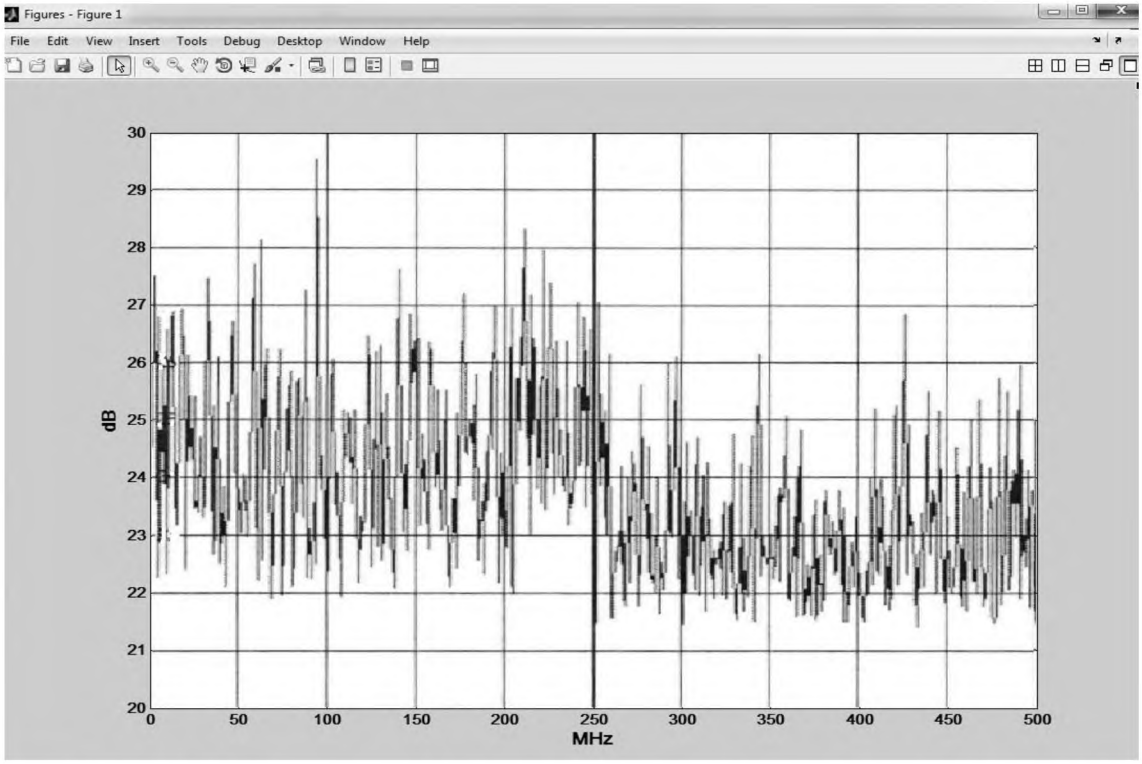


Рисунок 2.7 – Частотний спектр маскуючого сигналу, реалізованого відповідно до запропонованого підходу

Виграш в коефіцієнті перекриття для запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів відносно підходу-прототипу склав (тут S_1 і S_2 обчислювались згідно (2.2)):

$$R = \left(\frac{S_2}{S_1} - 1 \right) \cdot 100\% \approx 18{,}8\% \tag{2.4}$$

Отже, мета кваліфікаційної роботи досягнута.

Переваги запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів полягають в наступному:

- при функціонуванні ЗОТ забезпечується підвищення рівня захищеності інформації в необхідному діапазоні частот сигналу від витоку за рахунок ПЕМВН;

- не використовується ключова інформація;

- його реалізація не вимагає конструктивних змін вузлів і блоків ЗОТ і здійснюється при незначному залученні ресурсу центрального процесора.

Таким чином, запропонований підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів дозволяє при незначних фінансових витратах підвищити рівень захищеності інформації ЗОТ у всьому діапазоні частот від витоку за рахунок побічних електромагнітних випромінювань і наведень.

2.3 Висновки

Запропонований підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів відноситься до області обчислювальної техніки і може бути використаний для захисту інформації, що обробляється ЗОТ, зокрема, від витоку по каналу ПЕМВН. Технічний результат – підвищення

коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки.

У запропонованому підході до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень здійснюють формування N файлів, потім подальше їх розбиття на M частин, причому кожна з них містить файли, що утворюють при проходженні по з'єднувальним лініям і вузлам засобу обчислювальної техніки сигнали з певним частотним спектром потужності. Далі відбувається копіювання цих частин файлів на M цифрових накопичувачів і одночасне зчитування файлів, обраних зі списку на кожному накопичувачі за випадковим законом, з M цифрових накопичувачів і їх запис в область внутрішньої пам'яті засобу обчислювальної техніки, після цього багато разів повторюється зчитування і запис файлів протягом часу, необхідного для маскування інформативного сигналу.

З огляду на невизначеність взаємного положення спектра інформативного сигналу і максимальної інтенсивності спектра неінформативного сигналу можлива ситуація, коли максимум інтенсивності спектра маскуючого сигналу не збігається з частотою інформативного сигналу. Це призводить до зниження коефіцієнта перекриття спектрів неінформативного і інформативного сигналу у всьому діапазоні частот. Керування інтенсивністю спектра маскуючого сигналу можливо шляхом корекції огинаючої спектра маскуючого сигналу за рахунок зміни структури бітової послідовності неінформативних файлів. Структура бітової послідовності неінформативних файлів залежить від використовуваного способу їх формування.

При реалізації запропонованого підходу виникає ситуація, коли інтегральні значення потужності шумових сигналів, випромінюваних при проходженні файлів, що знаходяться на різних носіях, в межах однієї і тієї ж смуги частот перевищують значення необхідного шумового сигналу, тобто при записі і зчитуванні цього файлу.

Запропоновано, перед передачею сукупності файлів, отриманої в результаті випадкового вибору файлу на кожному накопичувачі, перевіряють їх

на приналежність до будь-якої сукупності файлів з вищевказаного списку. Якщо вся сукупність файлів зі списку входить до складу сукупності файлів, що перевіряються перед передачею, то файли, які не потрапили в сукупність в списку, не передаються. Причому порівняння відбувається спочатку з сукупностей в списку, що мають найменшу кількість елементів.

При реалізації запропонованого підходу досягається результат, еквівалентний підвищенню коефіцієнта перекриття інформативних і неінформативних (маскуючих) сигналів випромінюваних ЗОТ, що в значній мірі ускладнює або виключає прийняття рішення про виявлення і розпізнавання (класифікації) інформативних ПЕМВ, які надходять на вхід приймача перехоплення. Інтенсивність неінформативних завад не перевищує норм на промислові завади.

Оцінка ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що виграш в коефіцієнті перекриття для запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів відносно підходу-прототипу склав R=18,8%.

Отже, перевагами запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів є наступні:

- при функціонуванні ЗОТ забезпечується підвищення рівня захищеності інформації в необхідному діапазоні частот сигналу від витоку за рахунок ПЕМВН;

- не використовується ключова інформація;

- його реалізація не вимагає конструктивних змін вузлів і блоків ЗОТ і здійснюється при незначному залученні ресурсу центрального процесора.

3 ЕКОНОМІЧНА ЧАСТИНА

Захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів потребує економічного обґрунтування, що є метою даного розділу. Для досягнення цієї мети необхідно виконати 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 впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

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

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів, $t_{тз}=18$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=36$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=27$;

$t_р$ – тривалість розробки підходу щодо захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів, $t_м=46$;

$t_д$ – тривалість підготовки технічної документації, $t_д=10$.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 18+36+27+46+10 = 137 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 20824+628,83 = 21452,83 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 137*152 = 20824 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 153*4,11 = 628,83 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,9 \cdot 2 \cdot 1,55 + \frac{5900 \cdot 0,25}{1920} + \frac{3560 \cdot 0,3}{1920} = 4,11 \text{ грн.}$$

Запропонований підхід щодо захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів передбачає здійснення оцінки рівня побічних електромагнітних випромінювань за допомогою аналізатору спектру FSP-30 з активною штирьовою антеною SAS-550-1B, вартість якого складає 633389 грн. Також необхідно здійснити витрати щодо перевірки цього апаратного забезпечення, які складають 7852 грн. Отже, вартість закупівлі апаратного забезпечення та допоміжних матеріалів становить:

$$К_{аз} = 633389+7852 = 641241 \text{ грн.}$$

В якості підтвердження ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів було проведено моделювання в середовищі Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 4000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

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

$$= 21452,83+641241+4000 = 666693,83 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

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

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

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.).

Оскільки середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів, вже використовується на підприємстві, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

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 сукупною величиною витрат на організаційні заходи, яка складає 5000 грн.

Придбане апаратне забезпечення відповідно до чинного законодавства України підлягає амортизації. Амортизаційні відрахування визначатимуться прямолінійним методом, виходячи зі строку корисного використання 10 років та первісного вартості аналізатору спектру FSP-30 з активною штирьовою

антеною SAS-550-1B, яка складає 641241 грн. Таким чином, річні амортизаційні відрахування складуть:

$$С_а = 641241/10 = 64124,10 \text{ грн.}$$

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 15400 грн. Додаткова заробітна плата – 9% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (15400*12 + 15400*12*0,09)*0,25= 50358 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 50358*0,22 = 11078,76 \text{ грн.}$$

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

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

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

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

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

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

$$С_{ел} = 0,9*2*1920*1,55 = 5356,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 666693,83*0,02=13333,88 грн).

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

Ск = 5000+64124,10+50358+11078,76+5356,8+13333,88 = 149251,54 грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

С = 149251,54 грн.

3.2 Оцінка можливого збитку

Запропонований підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів відноситься до області обчислювальної техніки і може бути використаний для захисту інформації, що обробляється ЗОТ, зокрема, від витоку по каналу ПЕМВН.

Оцінка величини можливого збитку визначатиметься для умовного підприємства, яке може мати загрози інформаційній безпеці, зокрема, виток інформації, що обробляється ЗОТ, по каналу ПЕМВН. Вартість інформації потенційно складає 600000 грн. Вірогідність реалізації загроз (R) щодо витоку інформації, що обробляється ЗОТ, по каналу ПЕМВН, складає 80%.

Отже, можлива величина збитку (В) на рік від загроз щодо витоку інформації по каналу ПЕМВН, становитиме:

В = 600000*0,8 = 480000 грн.

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації загрози (80%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 480000 - 149251,54 = 330748,46 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{330748,46}{666693,83} = 0,5, \quad \text{частки одиниці,}$$

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, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,5 > (6 - 5)/100 = 0,5 > 0,01.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,5} = 2 \text{ роки.}$$

3.4 Висновок

Виходячи з наведених розрахунків, захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів можна вважати економічно доцільним. У разі використання запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів можна окупити первісні інвестиції (капітальні витрати), які складають 666693,83 грн. за 2 роки. При цьому економічний ефект складатиме 330748,46 грн. при щорічних експлуатаційних витратах 149251,54 грн. Коефіцієнт повернення інвестицій має значення 0,5 грн./грн., тобто 0,5 грн. економічного ефекту на 1 грн. капітальних витрат.

ВИСНОВКИ

1. В результаті аналізу технічних каналів витоку та руйнування інформації встановлено, що найбільшу небезпеку витоку інформації через ПЕМВН представляють вузли та внутрішнього облаштування ПЕОМ, які опрацьовують інформацію в послідовному коді. Інформативні випромінювання в паралельному коді наразі розшифровці не піддаються, оскільки через електромагнітні випромінювання неможливо визначити належність випроміненого імпульсу до якогось розряду коду. Дослідженню на ПЕМВН підлягають наступні пристрої: відеопідсистема; накопичувачі на жорстких і гнучких дисках; пристрої CD, CD-R, CD-RW, DVD, DVD-RW; клавіатура; послідовні порти; принтери.

2. В результаті аналізу існуючих підходів до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень встановлено їх недоліки. Недоліком відомого підходу до захисту інформації в лінії зв'язку [26] є те, що існує можливість відновлення інформації по «портрету» ПЕМВ за рахунок можливої відмінності частот основного і додаткового сигналу. Недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок побічних електромагнітних випромінювань і наведень, що реалізовується в відомому пристрої [27] є можливість відновлення інформації для послідовних інтерфейсів, розрядність посилок яких мала. Недоліком відомого підходу до захисту інформації в лінії зв'язку від витоку за рахунок ПЕМВН [28] є висока складність технічної реалізації і зниження швидкості роботи ЗОТ, перші внесенням в нього додаткових змін. Інший недолік відомого підходу полягає в неможливості повного перекриття в частотної області ПЕМВ від основної та додаткової лінії через використання в обох лініях однотипних і рівних по потужності сигналів. Недоліком підходу до захисту ЗОТ від витоку інформації по каналу побічних електромагнітних випромінювань і наведень (прототипу) [29] є низький коефіцієнт перекриття спектрів інформативного і неінформативного сигналів, обумовлений

наступними факторами: 1) в підході-прототипі за рахунок зміни способу формування бітових послідовностей не можна домогтися точного співпадіння частотних спектрів маскуючого і інформативного сигналів; 2) можливість періодичної корекції огинаючої спектра в режимі реального часу за рахунок зміни структури бітової послідовності означає вимір випромінювання ЗОТ, яке в процесі роботи вже буде містити неінформативне випромінювання.

3. Запропоновано підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів, з метою підвищення коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки. Це досягається шляхом здійснення наступних кроків: перед передачею сукупності файлів, отриманої в результаті випадкового вибору файлу на кожному накопичувачі, перевіряють їх на приналежність до будь-якої сукупності файлів з вищевказаного списку; якщо вся сукупність файлів зі списку входить до складу сукупності файлів, що перевіряються перед передачею, то файли, які не потрапили в сукупність в списку, не передаються; при цьому порівняння відбувається спочатку з сукупностей в списку, що мають найменшу кількість елементів. Встановлено, що перевагами запропонованого підходу є наступні: при функціонуванні ЗОТ забезпечується підвищення рівня захищеності інформації в необхідному діапазоні частот сигналу від витоку за рахунок ПЕМВН; не використовується ключова інформація; його реалізація не вимагає конструктивних змін вузлів і блоків ЗОТ і здійснюється при незначному залученні ресурсу центрального процесора.

4. В результаті оцінки ефективності запропонованого підходу до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів встановлено, що виграш в коефіцієнті перекриття для запропонованого підходу відносно підходу-прототипу склав R=18,8%.

ПЕРЕЛІК ПОСИЛАНЬ

1. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

2. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М.Паук, В.Г.Потапов. – К.: «МК-Пресс», 2005. – 288 с.

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

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

5. 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.

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

7. 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.

8. 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.

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

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

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

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

13. 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.

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

15. 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.

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

17. 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.

18. 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.

19. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.

20. 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.

21. 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.

22. 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.

23. 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.

24. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие / А.А.Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

25. Блавацька Н.М. Програмне забезпечення систем захисту інформації: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.

26. Патент РФ 2237371. Способ защиты информации в линии святи / Н.Г. Богданов, Ю.Б. Иванов – заявл. 25.02.2003, опубл. 27.09.2004.

27. Патент РФ 74722. Клавиатура для защиты информации, циркулирующей в системе обработки информации с использованием электронных цифровых устройств / Е.М. Фокин, С.В. Чижов, С.А. Косогов, В.М. Лазарев – заявл. 21.03.2008, опубл. 10.07.2008.

28. Патент РФ 2427903. Способ защиты информации в линии связи от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) / С.В. Чижов – заявл. 03.03.2010, опубл. 27.08.2011.

29. 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.

30. 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	29	
6	А4	Спеціальна частина	15	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	4	
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 Базаров.ppt

2 Диплом Базаров.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 125-17-1 Базарова Д.М. на тему: «Захист інформації від витоку по каналу побічних електромагнітних випромінювань і наведень цифрових накопичувачів»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 72 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення коефіцієнта перекриття спектрів інформативного і неінформативного (маскуючого) сигналів, що випромінюються засобами обчислювальної техніки.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу технічних каналів витоку та руйнування інформації, а також існуючих підходів до захисту інформації від витоків по каналу побічних електромагнітних випромінювань і наведень в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до захисту інформації від витоку по каналу побічних електромагнітних випромінювань і наведень з використанням дерева перекриттів маскуючих сигналів та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід дозволяє підвищити рівень захищеності інформації ЗОТ у всьому діапазоні частот від витоку за рахунок ПЕМВН.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

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

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