Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____

Кафедра ___ _____Безпеки інформаційних технологій_____

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____МОНІТОРИНГ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ_____
_____ЛІНІЙ ЗВ'ЯЗКУ НА ВИТОК ІНФОРМАЦІЇ_____
(тема)

Виконав:

студент 2 курсу, групи __БІКСзм – 19 – 1_____

_____Пепа Ю.В._____

Спеціальність ___125 «Кібербезпека»_____
(код і повна назва спеціальності)

Тип програми ___освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма _«Безпека інформаційних__

і комунікаційних систем»_____
(повна назва освітньої програми)

Керівник ____доцент Федюшин О.І._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З._____
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 «Кібербезпека»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 2020 р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

Студентові Пепі Юрію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Моніторинг інформаційно-комунікаційних ліній зв'язку на виток інформації»
затверджена наказом університету від 26.10.2020 року № 166 Стз
2. Термін подання студентом роботи до екзаменаційної комісії 24.12.2020 р.
3. Вихідні дані до роботи: 3.1. Обладнання для дослідження (персональний комп'ютер, що під'єднаний до мережі Інтернет з інтерфейсними лініями зв'язку);
3.2. Сучасне апаратно-програмне обладнання для виявлення витоку інформації з ліній зв'язку, їх характеристики;
3.3. Інтерфейси: E-SATA, HDMI та ETHERNET.
4. Перелік питань, що потрібно опрацювати в роботі 4.1. Огляд небезпеки від витоку через канали ПЕМВН;
4.2. Аналіз методик проведення досліджень щодо вимірювань електромагнітних випромінювань;
4.3. Вибір методу вимірювання небезпечних рівнів ПЕМВН від інтерфейсів персонального комп'ютера;

4.4. Отримання результатів вимірювань, їх аналіз, обробка та рекомендації щодо захисту інформації, яка циркулює в інформаційно-комунікаційних лініях зв'язку.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) ____презентація.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1.	Аналіз завдання на атестаційну роботу	01.11.2020 р.	
2.	Аналітичний огляд методів дослідження	03.11.2020 р. – 08.11.2020 р.	
3.	Порівняння та вибір методів вимірювання електромагнітних параметрів	09.11.2020 р. – 17.11.2020 р.	
4.	Вибір методики тестування ліній зв'язку	18.11.2020 р.	
5.	Отримання практичних результатів	19.11.2020 р. – 04.12.2020 р.	
6.	Підготовка тез на конференцію	05.12.2020 р. – 06.12.2020 р.	
7.	Підготовка наукової статті	07.12.2020 р. – 14.12.2020 р.	
8.	Оформлення пояснювальної записки	15.12.2020 р. – 20.12.2020 р.	
9.	Підготовка презентації	21.12.2020 р.	
10.	Подання роботи до захисту	22.12.2020 р.	

Дата видачі завдання 29 листопада 2020 року

Студент _____
(підпис)

Керівник роботи _____доцент Федюшин О.І.
(підпис) (посада, прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка складається з: 71 с. (з додатками 105 с.), 24 рис., 17 табл., 20 джерел.

НЕБЕЗПЕЧНИЙ СИГНАЛ, ЗАХИСТ ІНФОРМАЦІЇ, ВИТОК ІНФОРМАЦІЙ, АКТИВНИЙ ЗАХИСТ, ПАСИВНИЙ ЗАХИСТ, КАНАЛ ВИТОКУ, ТЕХНІЧНИЙ КОНТРОЛЬ, СПЕЦІАЛЬНІ ДОСЛІДЖЕННЯ.

Об’єкт дослідження – канал витоку інформації через побічні електромагнітні випромінювання та наведення.

Предмет дослідження – комплексна система захисту інформації від витоку через побічні електромагнітні випромінювання та наведення.

Мета роботи – дослідити небезпечні рівні інформаційних сигналів від електронно-обчислювальної техніки та запропонувати система захисту від побічних електромагнітних випромінювань та наведень.

Розглянуті причини виникнення технічного каналу витоку інформації через побічні електромагнітні випромінювання та наведення, проаналізовані сучасні методики досліджень та вимірювань, проведено оцінку ефективності запропонованих засобів захисту інформації на об’єкті інформаційної діяльності.

Результати роботи можуть використовуватися для аналізу впливу інших засобів електронно-обчислювальної техніки на ефективність методів захисту та при побудові комплексу захисних заходів щодо зменшення чи унеможливлення витоку інформації з обмеженим доступом за межі контрольованої зони.

ABSTRACT

Explanatory note consists of: 71 p. (105 p. with applications), 24 Fig., 17 table, 20 sources.

DANGEROUS SIGNAL, INFORMATION PROTECTION, INFORMATION LEAKS, ACTIVE PROTECTION, PASSIVE PROTECTION, LEAKAGE CHANNEL, TECHNICAL CONTROL, SPECIAL RESEARCH.

The object of research is the channel of information leakage through incidental electromagnetic radiation and guidance.

The subject of research – a comprehensive system of protection of information from leakage through spurious electromagnetic radiation and guidance.

The purpose of the work is to investigate dangerous levels of information signals from electronic computers and to offer a system of protection against incidental electromagnetic radiation and guidance.

The reasons for the technical channel of information leakage due to incidental electromagnetic radiation and guidance are considered, modern methods of research and measurements are analyzed, the effectiveness of the proposed means of information protection at the object of information activities is evaluated.

The results can be used to analyze the impact of other electronic computing devices on the effectiveness of protection methods and in building a set of protective measures to reduce or prevent leakage of information with limited access outside the controlled area.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДТЗС – допоміжні технічні засоби і системи;

ЗОТ – засоби обчислювальної техніки;

ЕОМ – електронно-обчислювальна машина;

ЕОТ – електронно-обчислювальна техніка;

КСЗІ – комплексна система захисту інформації;

ПЕМВН – побічні електромагнітні випромінювання та наведення;

ТЗІ – технічний захист інформації;

ТЗПІ – технічні засоби передачі інформації.

ВСТУП

У процесі функціонування засобів обчислювальної техніки в конструктивних елементах та кабельних з’єднаннях циркулюють електричні струми інформативних сигналів, у результаті чого формуються електромагнітні поля, рівні яких можуть бути достатніми для приймання сигналів і здобування інформації за допомогою спеціальної апаратури через канали побічних електромагнітних випромінювань та наведень (ПЕМВН) [1].

Наразі, засоби електронно-обчислювальної техніки все частіше використовуються для обробки інформації з обмеженим доступом. ПЕМВН можуть виникати самочинно, за рахунок недосконалості елементної бази та схемних рішень, а також через зловмисні дії і створювати інші технічні канали витоку інформації. Тому не втрачає своєї актуальності проблема визначення рівнів ПЕМВН від інформаційних ліній зв’язку та комп’ютерних інтерфейсів, а також контролю ефективності інших засобів протидії виникненню каналу витоку інформації через ПЕМВН.

Атестаційна робота присвячена оцінці захищеності інформації, що обробляється в засобах електронно-обчислювальної техніки, від витоку за рахунок ПЕМВН. Проведені теоретичні розрахунки дозволяють попередньо оцінити можливі загрози і в подальшому зменшити їх чи унеможливити. Отримані експериментальні вимірювання рівнів випромінювань комп’ютерних інтерфейсних ліній передачі даних та інформаційно-комунікаційних ліній зв’язку за різними методиками і їх аналіз як раз вказують на можливі види загроз і дозволяють в подальшому ефективніше побудувати систему захисту інформації.

1 УТВОРЕННЯ КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПЕМВН

1.1 Причини виникнення ПЕМВН

Фізичну основу небезпечних сигналів, що виникають під час роботи у виділеному приміщенні радіозасобів і електричних приладів, складають ПЕМВН [2].

Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відображення інформації технічних засобів передачі інформації (ТЗПІ), а також допоміжних технічних засобів і систем (ДТЗС) [3].

До ТЗПІ відносяться:

- засоби і системи телефонного, телеграфного, директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв’язку;

- засоби і системи звукопідсилення, звукозапису та звуковідтворення;

- пристрої, що утворюють дискретні канали зв’язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна тощо;

- апаратура перетворення, оброблення, пересилання і приймання відеоканалів, що містять факсимільну інформацію.

ТЗПІ можуть бути захищеними і незахищеними.

До допоміжних технічних засобів і систем відносяться:

- засоби і системи спеціальної охоронної сигналізації (на відкриття дверей, вікон та проникнення до приміщення сторонніх осіб), пожежної сигналізації (з датчиками, що реагують на дим, світло, тепло, звук);

- система дзвінкової сигналізації (виклик секретаря, вхідна сигналізація);

- контрольно-вимірювальна апаратура;

- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);

- засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення (абонентські гучномовці системи радіомовлення та оповіщення, радіоприймачі та телевізори);

- засоби і системи годинофікації (електронні годинники, вторинні електрогодинники);

- засоби і системи електроосвітлення та побутового електрообладнання (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, провідна мережа електроосвітлення);

- електронна та електрична оргтехніка [4].

Функціонування будь-якого технічного засобу інформації пов’язане з протіканням по його струмоведучих елементах електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні й електричні поля, що називають побічними електромагнітними випромінюваннями [2].

Побічні електромагнітні випромінювання виникають внаслідок непередбачуваної схемою або конструкцією технічного засобу передачі інформації по паразитним зв’язкам напруги, струму, заряду або магнітного поля.

Під паразитним зв’язком розуміють зв’язок по електричним або магнітним ланцюгах, що з’являється незалежно від бажання конструктора. В залежності від фізичної природи елементів паразитних електричних ланцюгів, розрізняють паразитні зв’язки через загальний повний опір, ємнісний або індуктивний паразитний зв’язок [5].

Правомірно припустити, що утворенню технічних каналів витоку інформації сприяють певні обставини і причини технічного характеру (рис. 1.1). До них можна віднести недосконаліть елементної бази та схемних рішень, прийнятих для даної категорії технічних засобів, експлуатаційний знос елементів виробу, а також зловмисні дії [5].

Рисунок 1.1 – Причини утворення технічних каналів витоку інформації

При організації захисту інформації ТЗПІ необхідно розглядати як систему, що включає основне (стаціонарне) обладнання, кінцеві пристрої, сполучні лінії (сукупність проводів і кабелів, що прокладаються між окремими ТЗПІ та його елементами), розподільні й комутаційні пристрої, системи електроживлення, системи заземлення [2].

Під час пересилання інформації з обмеженим доступом в елементах схем, конструкцій, підвідних і з’єднувальних проводах технічних засобів протікають струми інформативних (небезпечних) сигналів. Електромагнітні поля, що виникають при цьому, можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації.

Джерелами виникнення електромагнітних полів у ТЗПІ та ДТЗС можуть бути неекрановані проводи, розімкнуті контури, елементи контрольно-вимірювальних приладів, контрольні гнізда на підсилювальних блоках і пультах, неекрановані кінцеві пристрої, підсилювачі потужності та лінійні підсилювачі, трансформатори, дроселі, з'єднувальні проводи з великими струмами, роз'єми, гребінки, гучномовці, кабельні лінії [6].

В якості елементів каналів витоку інформації найбільший інтерес представляють ТЗПІ та ДТЗС, що мають вихід за межі контрольованої зони, тобто зони, в якій виключена поява осіб і транспортних засобів, які не мають постійних або тимчасових перепусток [2].

Крім з'єднувальних ліній ТЗПІ та ДТЗС за межі контрольованої зони можуть виходити дроти та кабелі, до них не відносяться, але проходять через приміщення, де встановлено технічні засоби, а також металеві труби систем опалення, водопостачання та інші струмопровідні металоконструкції. Такі дроти, кабелі і струмопровідні елементи називаються сторонніми провідниками.

Зона, у якій можливі перехоплення (за допомогою розвідувального приймача) побічних електромагнітних випромінювань і подальша розшифровка інформації, що міститься в них (тобто зона, в межах якої відношення «інформаційний сигнал/шум» перевищує допустимий нормоване значення), називається (небезпечною) зоною 2. Простір навколо ТЗПІ, в межах якого на випадкових антенах наводиться інформаційний сигнал вище припустимого (нормованого) рівня, називається (небезпечною) зоною 1 [3].

Випадкової антеною є ланцюги технічних засобів або сторонні провідники, здатні приймати побічні електромагнітні випромінювання [2].

Елементи ТЗПІ та ДТЗС можуть являти собою зосереджені випадкові антени (апаратура та її блоки) або розподілені випадкові антени (кабельні лінії та проводи).

Зазначеними елементами можуть бути [6]:

- кінцеві технічні засоби і прилади;

- кабельні мережі та розводки, що з`єднують пристрої та обладнання;

- комутаційні пристрої (комутатори, кроси, бокси тощо);

- елементи заземлення та електроживлення.

Інформативні (небезпечні) сигнали можуть виникати на елементах технічних засобів, чутливих до впливу [6]:

- електричного поля (неекрановані проводи та елементи технічних засобів);

- магнітного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле);

- акустичного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле).

За наявності в технічних засобах елементів, здатних перетворювати ці поля в електричні сигнали, можливий витік інформації незахищеними колами абонентських ліній зв`язку, електроживлення, заземлення, керування, сигналізації [6].

1.2 Організаційні заходи захисту від витоку інформації

До основних організаційних і режимних заходів відносяться [3, 7]:

- залучення до проведення робіт по захисту інформації організацій, що мають ліцензію на діяльність в області захисту інформації, видану відповідними органами;

- категорування і атестація об’єктів ТЗПІ і виділених для проведення закритих заходів приміщень (далі виділених приміщень) по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеня секретності;

- використання на об’єкті сертифікованих ТЗПІ і ДТЗС;

- встановлення контрольованої зони навколо об’єкту;

- залучення до робіт по будівництву, реконструкції об’єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

- організація контролю і обмеження доступу на об’єкти ТЗПІ і у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і тимчасових обмежень в режимах використання технічних засобів, що підлягають захисту;

- відключення на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів, від ліній зв’язку і таке інше.

1.3 Технічні заходи

Технічні заходи направлені на закриття каналів витоку інформації шляхом ослаблення рівня інформаційних сигналів або зменшенням відношення сигнал/шум в місцях можливого розміщення портативних засобів розвідки або їх датчиків до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки, і проводяться з використанням активних і пасивних засобів.

До заходів з використанням пасивних засобів відносяться [1, 4]:

Контроль і обмеження доступу на об’єкти ТЗПІ і у виділені приміщення:

- установка на об’єктах ТЗПІ і у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу.

Локалізація випромінювань:

- екранування ТЗПІ і їх сполучних ліній;

- заземлення ТЗПІ і екранів їх сполучних ліній;

- екранування виділених приміщень.

Розв’язування інформаційних сигналів:

- установка спеціальних засобів захисту в ДТЗС, що володіють «мікрофонним ефектом» і що мають вихід за межі контрольованої зони;

- установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання каналізації, що мають вихід за межі контрольованої зони;

- установка автономних або стабілізованих джерел електроживлення;

- установка пристроїв гарантованого живлення ТЗПІ;

- установка в ланцюгах електроживлення ТЗПІ, а також в мережі електроживлення виділених приміщень завадопридушуючих фільтрів [1].

До заходів з використанням активних засобів відносяться:

Просторове зашумлення:

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних перешкод (при виявленні і визначенні частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТЗПІ);

- створення акустичних і вібраційних перешкод з використанням генераторів акустичного шуму;

- придушення диктофонів в режимі запису з використанням придушувачів диктофонів.

Лінійне зашумлення:

- лінійне зашумлення ліній електроживлення;

- лінійне зашумлення сторонніх провідників і сполучних ліній ДТЗС, що мають вихід за межі контрольованої зони.

Знищення закладних пристроїв.

Знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів «жучків») [8].

Виявлення портативних електронних пристроїв перехоплення інформації (закладних пристроїв) здійснюється проведенням спеціальних обстежень, а також спеціальних перевірок об’єктів ТЗПІ і виділених приміщень.

1.4 Захист інформації із застосуванням пасивних методів

Пасивні методи захисту інформації направлені на:

- ослаблення побічних електромагнітних випромінювань інформаційних сигналів ТЗПІ на межі контрольованої зони до величин, що забезпечують неможливість їх виділення засобом розвідки на тлі природних шумів;

- ослаблення наведень побічних електромагнітних випромінювань інформаційних сигналів ТЗПІ в сторонніх провідниках і сполучних лініях ДТЗС, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їх виділення засобом розвідки на тлі природних шумів;

- виключення (ослаблення) витоку інформаційних сигналів ТЗПІ в ланцюги електроживлення, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їх виділення засобом розвідки фоні природних та індустріальних шумів.

Ослаблення побічних електромагнітних випромінювань ТЗПІ і їх наведень в сторонніх провідниках здійснюється шляхом екранування і заземлення ТЗПІ і їх сполучних ліній.

Виключення чи ослаблення витоку інформаційних сигналів ТЗПІ в ланцюзі електроживлення досягається шляхом фільтрації інформаційних сигналів.

Функціонування будь-якого технічного засобу інформації пов’язане з протіканням по його струмоведучим елементах електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні і електричні поля, так звані побічні електромагнітні випромінювання.

Змінні електричне і магнітне поля створюються також в просторі, що оточує сполучні лінії (дроти, кабелі) ТЗПІ.

Побічні електромагнітні випромінювання ТЗПІ є причиною виникнення електромагнітних каналів витоку інформації, а також можуть виявитися причиною виникнення наведення інформаційних сигналів в сторонніх струмоведучих лініях і конструкціях. Тому зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня ПЕВМН є екранування їх джерел. Розрізняють наступні способи екранування [2]:

- електростатичне;

- магнітостатичне;

- електромагнітне.

Електростатичне і магнітостатичне екранування засновані на замиканні екраном (що володіє, в першому випадку, високою електропровідністю, а в другому – магнітопровідністю) відповідно електричного і магнітного полів.

Електростатичне екранування за суттю зводиться до замикання електростатичного поля на поверхню металевого екрану і відведення електричних зарядів у землю чи на корпус приладу. Заземлення електростатичного екрану є необхідним елементом при реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля. При використанні діелектричних екранів, щільно прилеглих до елементу, що екранується, можна ослабити поле джерела наведення в ε разів, де ε – відносна діелектрична проникність матеріалу екрану.

Екранування високочастотного магнітного поля засноване на використанні магнітної індукції, що створює в екрані змінні індукційні вихрові струми (струми Фуко). Магнітне поле цих струмів усередині екрану буде направлено в протилежну сторону відносно поля, що його породило, і за його межами – в ту ж сторону, що і поле збудження. Результуюче поле виявляється ослабленим усередині екрану і посиленим поза ним. Вихрові струми в екрані розподіляються нерівномірно по його перетину (товщині). Це викликається явищем поверхневого ефекту, суть якого полягає в тому, що змінне магнітне поле слабшає у міру проникнення в глиб металу, оскільки внутрішні шари екрануються вихровими струмами, циркулюючими в поверхневих шарах [2].

Ефективність магнітного екранування залежить від частоти і електричних властивостей матеріалу екрану. Чим нижче частота, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту.

При екрануванні магнітного поля заземлення екрану не змінює величини порушуваних в екрані струмів і, отже, на ефективність магнітного екранування не впливає.

На високих частотах застосовується виключно електромагнітне екранування. Дія електромагнітного екрану заснована на тому, що високочастотне електромагнітне поле ослабляється їм же створеним (завдяки тим, що утворюються в товщі екрану вихровим струмам) полем зворотного напряму.

Теорія і практика показують, що, з погляду вартості матеріалу і простоти виготовлення, переваги на стороні екранованого сталевого приміщення. Проте при застосуванні сітчастого екрану можуть значно спроститися питання вентиляції і освітлення приміщення. У зв’язку з цим сітчасті екрани також знаходять широке застосування.

Разом з тим при екрануванні дротів з’єднання оболонки дроту з корпусом в одній точці не ослабляє в навколишньому просторі магнітне поле, що створюється струмом, який протікає по дроту. Для екранування магнітного поля необхідно створити поле такої ж величини і зворотного напряму. З цією метою необхідно весь зворотний струм ланцюга, що екранується, направити через екрануюче обплетення дроту. Для повного здійснення цього принципу необхідно, щоб екрануюча оболонка була єдиним шляхом для протікання зворотного струму.

Висока ефективність екранування забезпечується при використанні витої пари, захищеною екрануючою оболонкою [1].

На низьких частотах доводиться використовувати складніші схеми екранування – коаксіальні кабелі з подвійним обплетенням.

На вищих частотах, коли товщина екрану значно перевищує глибину проникнення поля, необхідність в подвійному екрануванні відпадає. В цьому випадку зовнішня поверхня грає роль електричного екрану, а по внутрішній поверхні протікають зворотні струми.

Застосування екрануючої оболонки істотно збільшує ємність між дротом і корпусом, що в більшості випадків небажано. Екрановані дроти громіздкі і незручні при монтажі, вимагають оберігання від випадкових з’єднань із сторонніми елементами і конструкціями.

Екрануватися можуть не тільки окремі блоки чи вузли апаратури і їх сполучні лінії, але і приміщення в цілому.

У звичайних не екранованих приміщеннях основний екрануючий ефект забезпечують залізобетонні стіни будинків. Екрануючі властивості дверей і вікон гірші. Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, зокрема [1]:

- струмопровідні лакофарбні покриття або шпалери;

- штори з металізованої тканини;

- металізоване скло (наприклад з двоокису олова), що встановлюються в металеві або металізовані рами.

У приміщенні екрануються стіни, двері і вікна. При закритті дверей повинен забезпечуватися надійний електричний контакт із стінками приміщення (з дверною рамою) по всьому периметру не рідше чим через 10 – 15 мм. Для цього може бути застосована пружинна гребінка з фосфористої бронзи, яку укріплюють по всьому внутрішньому периметру дверної рами.

Вікна повинні бути затягнуті одним або двома шарами мідної сітки з чарункою не більш 2 мм, причому відстань між шарами сітки повинна бути не менше 50 мм. Обидва шаруючи сітки повинні мати хороший електричний контакт із стінками приміщення (з рамою) по всьому периметру. Сітки зручніше робити знімними, і металеве обрамлення знімної частини також повинне мати пружні контакти з фосфористої бронзи [2]. При проведенні робіт з ретельного екранування подібних приміщень необхідно одночасно забезпечити нормальні умови для людини, що працює в ньому, перш за все вентиляцію повітря.

Заземлення комунікаційних технічних засобів.

Необхідно пам’ятати, що екранування ТЗПІ і сполучних ліній ефективно тільки при правильному їх заземленні. Тому однією з найважливіших умов по захисту ТЗПІ є правильне заземлення цих пристроїв. Найчастіше використовуються одноточкові, багатоточкові і комбіновані (гібридні) схеми.

Як правило, одноточкове заземлення застосовується на низьких частотах при невеликих розмірах пристроїв, що заземляються. На високих частотах при великих розмірах пристроїв, що заземляються, і значних відстанях між ними використовується багатоточкова система заземлення. У проміжних випадках ефективна комбінована (гібридна) система заземлення, що є різними поєднаннями одноточкової і багатоточкової заземлюючих систем.

Заземлення технічних засобів систем інформатизації і зв'язку повинне бути виконане відповідно до певних правил. Основні вимоги, що пред'являються до системи заземлення, полягають в наступному [1, 6]:

- система заземлення повинна включати загальний заземлювач, що заземлює кабель, шини і дроти, які сполучають заземлювач з об'єктом;

- опори заземлюючих провідників, а також земляних шин повинні бути мінімальними;

- кожен елемент, що заземлюється, повинен бути приєднаний до заземлення або до заземлюючої магістралі за допомогою окремого відгалуження. Послідовне включення в заземлюючий провідник декількох елементів, що заземляються, забороняється;

- у системі заземлення повинні бути відсутніми замкнуті контури, утворені з'єднаннями або небажаними зв'язками між сигнальними ланцюгами і корпусами пристроїв, між корпусами пристроїв і землею;

- слід уникати використання загальних провідників в системах екранування, заземлення і сигнальних ланцюгів;

- якість електричних з'єднань в системі заземлення повинна забезпечувати мінімальний опір контакту, надійність і механічну міцність контакту в умовах кліматичних дій і вібрації;

- контактні з'єднання повинні виключати можливість утворення оксидних плівок на контактних поверхнях і пов'язаних з цими плівками нелінійних явищ;

- контактні з'єднання повинні виключати можливість утворення гальванічних пар для запобігання корозії в ланцюгах заземлення;

- забороняється використовувати в якості заземлюючого пристрою «нульові» дроти електромереж, металоконструкції будівель, що мають з’єднання з землею, металеві оболонки підземних кабелів, металеві труби систем опалювання, водопостачання, каналізації тощо [2];

- заземлювальні дроти повинні бути виконані з мідного дроту (кабеля) з перехідним опором з’єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом [1].

1.5 Захист інформації із застосуванням активних методів і засобів

Реалізація пасивних методів захисту, заснованих на застосуванні екранування і фільтрації, приводить до ослаблення рівнів ПЕМВН (небезпечних сигналів) ТЗПІ і тим самим до зменшення відношення сигнал/шум. Проте у ряді випадків, не дивлячись на застосування пасивних методів захисту, на межі контрольованої зони відношення сигнал/шум перевищує допустиме значення. В цьому випадку застосовуються активні заходи захисту, засновані на створенні перешкод засобам розвідки, що також призводить до зменшення відношення сигнал/шум (дод. Б).

Активні методи захисту інформації направлені на:

- створення маскувальних просторових електромагнітних перешкод в цілях зменшення відношення сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ТЗПІ;

- створення маскувальних електромагнітних перешкод в сторонніх провідниках і сполучних лініях ДТЗС в цілях зменшення відношення сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ТЗПІ.

Просторове і лінійне електромагнітні зашумлення.

Для виключення перехоплення ПЕМВН через електромагнітний канал використовується просторове зашумлення, а для виключення знімання

наведень інформаційних сигналів із сторонніх провідників і сполучних ліній ДТЗС – лінійне зашумлення.

До системи просторового зашумлення пред'являються наступні вимоги:

- система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;

- створювані перешкоди повинні бути нерегулярної структури;

- рівень створюваних перешкод (як за електричною, так і за магнітною складовою поля) повинен забезпечити відношення сигнал/шум на межі контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;

- перешкоди повинні бути як з горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);

- на межі контрольованої зони рівень перешкод, що створюються системою просторового зашумлення, не повинен перевищувати необхідних норм електромагнітної сумісності.

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечного сигнал/шум на межі контрольованої зони не перевищує деякого допустимого значення, що розраховується за спеціальними методиками для кожної частоти – інформаційного (небезпечного) побічного електромагнітного випромінювання ТЗПІ [2].

У системах просторового зашумлення в основному використовуються перешкоди типу «білий шум» або «синфазні перешкоди».

Системи, що реалізовують метод «синфазної перешкоди», в основному застосовуються для захисту електронно-обчислювальних машин (ЕОМ). У них в якості маскувального сигналу використовуються імпульси випадкової амплітуди, співпадаючі (синхронізовані) за формою і часом існування з імпульсами корисного сигналу. Внаслідок цього за своїм спектральним складом маскувальний сигнал аналогічний спектру побічних електромагнітних

випромінювань ЕОМ, тобто система зашумлення генерує «імітаційну перешкоду», за спектральним складом відповідну приховуваному сигналу.

В даний час застосовуються системи просторового зашумлення, що використовують перешкоди типу «білий шум» з рівнями побічних електромагнітних завад, що істотно перевищують випромінювання корисного сигналу [1, 9]. Такі системи застосовуються для захисту широкого класу технічних засобів: ЕОМ, систем звукопідсилення і звукового супроводу, систем внутрішнього телебачення тощо.

У простому випадку система лінійного зашумлення є генератором шумового сигналу, що формує шумову (маскувальну) напругу із заданими спектральними, часовими і енергетичними характеристиками, який гальванічно під’єднується до інформаційно-комунікаційної лінії зв’язку або є окремим (стороннім) провідником. На практиці найчастіше подібні системи використовуються для зашумлення ліній електроживлення.

При використанні систем просторового зашумлення необхідно пам’ятати, що разом з перешкодами засобам розвідки створюються перешкоди і іншим радіоелектронним засобам (наприклад, системам телебачення, радіозв’язку і таке інше). Тому при введенні в експлуатацію системи просторового зашумлення необхідно проводити спеціальні дослідження за вимогами забезпечення електромагнітної сумісності. Крім того, рівні перешкод, що створюються системою зашумлення, повинні відповідати санітарно-гігієнічним нормам.

Просторове зашумлення ефективне не тільки для закриття електромагнітного, але і електричного каналів витоку інформації, оскільки шумовий сигнал при випромінюванні наводиться в сполучних лініях ДТЗС і сторонніх провідниках, що виходять за межі контрольованої зони.

2 ПЕМВН ВІД ЦИФРОВИХ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

2.1 Параметри сигналів від цифрових засобів обчислюваної техніки

Для визначення параметрів інформаційних ПЕМВН від засобів обчислюваної техніки (ЗОТ) розглядається форма подання і характеристики цифрової інформації, тобто тієї інформації, яка у вигляді цифрових кодів циркулює у вузлах, блоках, пристроях та лініях ЗОТ, які обробляють конфіденційну інформацію, тобто які використовуються як основні технічні засоби.

Розглянемо деякі теоретичні основи, без розуміння яких неможливо уявити які побічні випромінювання слід очікувати від деякого узагальненого сигналу в ланцюгах ЕОМ.

Початкова постановка завдання «від імені» потенційного зловмисника полягає у вирішенні найпростішої бінарної задачі – що передавалося в даний момент, «нуль» або «одиниця», тобто задача вирішується для одного двійкового розряду. При цьому передбачається, що потенційний зловмисник точно знає структуру пристрою, алгоритм обробки інформації, види кодування і таке інше [10].

Розглянемо поодинокий прямокутний імпульс кінцевої тривалості (рис. 2.1).

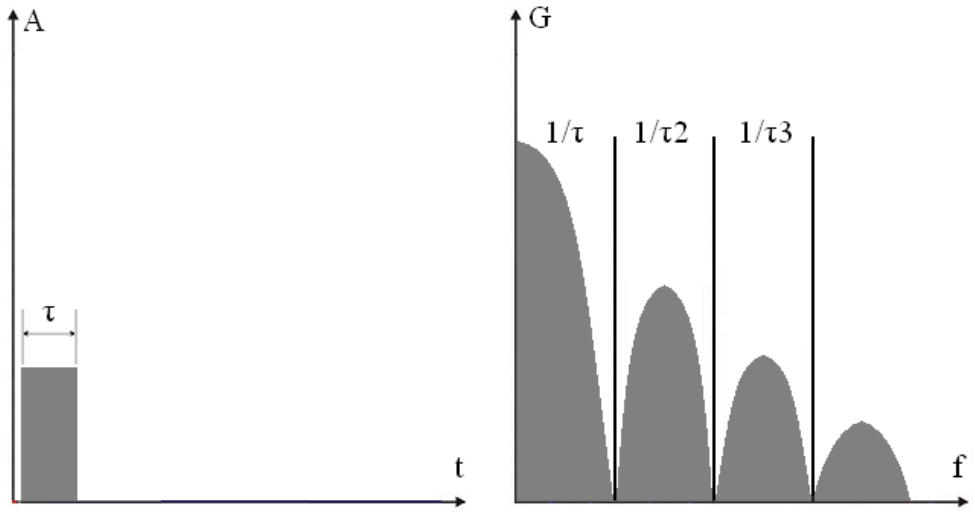


Рисунок 2.1 – Прямокутний імпульс кінцевої тривалості і його спектр

Обвідна спектру є нерівномірною і описується виразом:

$$G = U'\tau_E \frac{\sin x}{x}.$$

Наступним кроком при наближенні моделі до реальних сигналів є опис нескінченної послідовності імпульсів кінцевої тривалості. Такий сигнал і його спектр наведено на рис. 2.2.

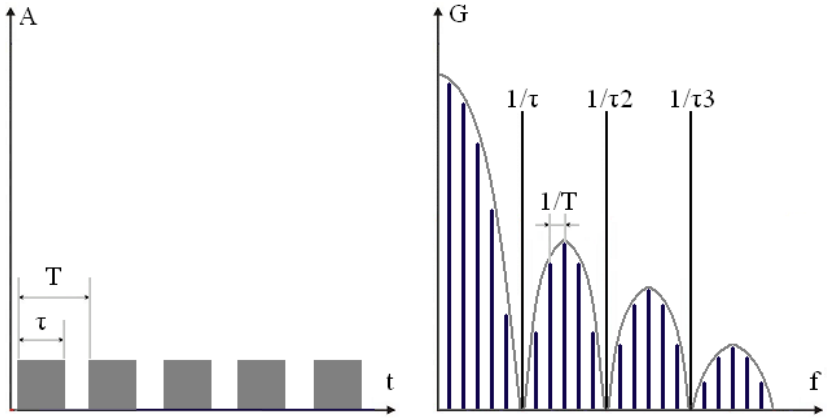


Рисунок 2.2 – Спектр нескінченної послідовності імпульсів

Слід зазначити, що амплітуда імпульсів менша, ніж амплітуда одиночного імпульсу на рис. 2.1, а амплітуди гармонічних складових спектру навіть зросли. Ця властивість спектру імпульсної послідовності випливає із існуючих спеціальних методів вимірювань:

$$\left|E_{\text{п}}\right| = 2A\frac{\sin\left(\frac{n\omega\tau_{\text{імп}}}{2}\right)}{\pi n}.$$

Таким чином, спектр послідовності імпульсів стає «лінійчатим», зберігаючи обвідну одиночного імпульсу («пелюстки» обвідної як і раніше мають «ширину» 1/τ). При цьому «крок» гармонік за частотою обернений періоду проходження імпульсів. Амплітуда гармонічних складових зросла. Це дозволяє швидко покращити співвідношення сигнал/шум при прийомі сигналів ПЕМВН.

Наведені спектри ілюструють гранично ідеалізовану картину. В реальних пристроях імпульсні послідовності не бувають нескінченними. Майже без винятків будь-яке пересилання, обробка і т.д. виконується «пакетами». Тому,

найбільш реальною моделлю сигналу в ланцюгах ЕОМ буде послідовність пакетів, в яких довжина окремого пакету істотно більше тривалості одного імпульсу. Така модель і її спектр зображена на рис. 2.3.

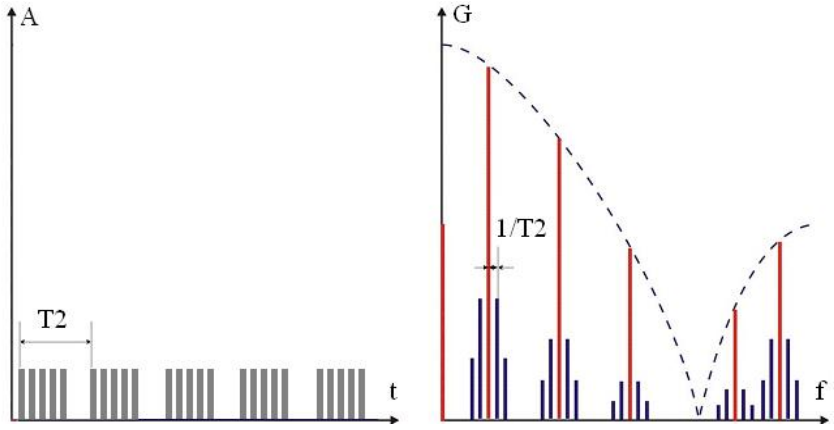


Рисунок 2.3 – Спектр послідовності пакетів імпульсів

Поблизу кожної спектральної складової, обумовленої самими імпульсами, з'явилися бічні складові, обумовлені частотою проходження пакетів [11].

Частину спектру такого сигналу з аналізатора спектру приведено на рис. 2.4.

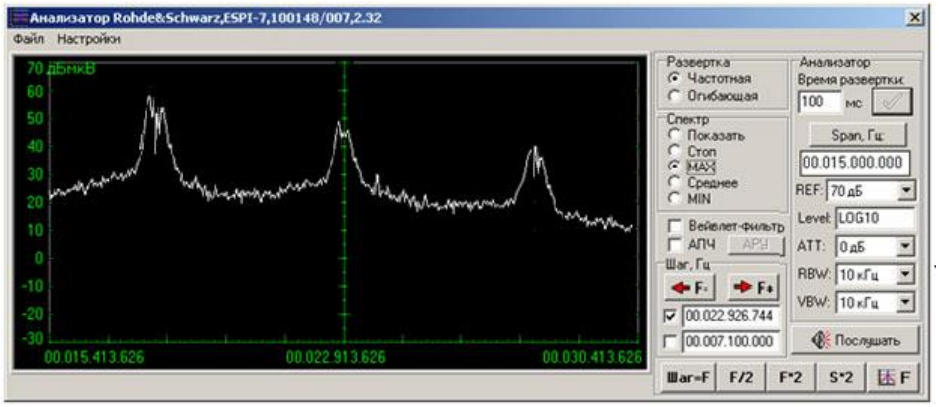


Рисунок 2.4 – Спектр послідовності пакетів імпульсів

У лівій частині екрану зображена одна з гармонік тактової частоти проходження імпульсів, а правіше – перша та друга верхні бічні частоти з кроком, що дорівнює частоті рядкової розгортки дисплею спектроаналізатора.

Як приклад розглянемо типовий випадок – ПЕМВН відеопідсистеми ЕОМ. Стандартний режим для засобів вимірювання цього пристрою –

виведення на екран відеосигналу, що представляє собою чергування прямокутних імпульсів з такими ж часовими інтервалами між ними (сигнал типу меандр). Кожен рядок растру при цьому є пакетом імпульсів. Кількість імпульсів в пакеті дорівнює половині розділової здатності екрану по горизонталі (512 імпульсів для режиму 1024x768 пікселів). Далі пауза, обумовлена зворотнім ходом рядкової розгортки, і новий пакет.

2.2 ПЕМВН від персонального комп'ютера ЗОТ

Досліджуючи ПЕМВН електронного цифрового обладнання, слід зазначити, що не всі складові спектру ПЕМВН є небезпечними з точки зору можливого витоку інформації.

ПЕМВН, що генеруються електронними пристроями, обумовлені протіканням струму в їх електричних ланцюгах. Умовно весь спектр випромінювання від ЗОТ поділяється на потенційно інформативні і неінформативні випромінювання.

Сукупність складових спектру ПЕМВН, що виникає при протіканні струму в ланцюгах, через які передаються сигнали, що містять конфіденційну (секретну, комерційну і т.д.) інформацію, назвемо потенційно-інформативними випромінюваннями.

Для персонального комп'ютера ЗОТ потенційно-інформативними ПЕМВН є випромінювання, що формуються наступними ланцюгами [12]:

- ланцюг, через який передаються сигнали від контролера клавіатури до порту введення-виведення на материнській платі;

- ланцюги, через які передається відеосигнал від відеоадаптера до відеопідсилювачів монітору ЕОТ;

- ланцюги, що формують шину даних системної шини комп'ютера;

- ланцюги, що формують шину відеоданих у середині відеопроцесора, контролера шини і таке інше.

Майже в кожному цифровому обладнанні існують ланцюги, які виконують допоміжні функції, через які ніколи не передаються сигнали, що

містять закриту інформацію. Випромінювання, що породжують струм, який протікає у таких ланцюгах, є безпечними стосовно витоку інформації. Для таких випромінювань цілком підходить термін неінформативні випромінювання. З точки зору захисту інформації неінформативні випромінювання можуть мати позитивний характер, виступаючи у разі збігу частотного діапазону у вигляді перешкоди прийому інформативних ПЕМВН як «взаємна перешкода».

Для персонального комп'ютера неінформативними ПЕМВН є випромінювання, що формуються наступними ланцюгами:

- ланцюги формування та передачі сигналів синхронізації;

- ланцюги, що формують шину управління і шину адреси системної шини;

- ланцюги, що передають сигнали апаратних переривань;

- внутрішні ланцюги блоку живлення комп'ютера, фільтри окремих вузлів [13].

Потенційно інформативні ПЕМВН, виділення корисної інформації з яких неможливе при будь-якому рівні цих випромінювань, називають безпечними інформативними випромінюваннями. Відповідно, потенційно інформативні випромінювання, для яких не існує причин, які б однозначно виключали можливість відновлення інформації, яка міститься в них, називають принципово-інформативними.

Так, наприклад, до принципово-інформативних випромінювань персонального комп'ютера можна віднести випромінювання, що формуються наступними ланцюгами:

- ланцюг, через який передаються сигнали від контролера клавіатури до порту введення-виведення на материнській платі;

- ланцюги, через які передається відеосигнал від відеоадаптера до монітору ЗОТ.

Відновлення інформації при перехопленні випромінювань ланцюгів, через які передається відеосигнал, – це один з тих випадків, коли при

використанні багаторозрядного (мінімум три розряди для кольорового монітору) паралельного коду формат представлення інформації дозволяє відновлювати більшу її частину, не відновлюючи при цьому послідовності значень кожного розряду коду. При цьому втрачається колір відеосигналу, але може бути відновлено смисловий зміст перехопленої інформації.

Аналіз технічної документації показує, що одна і та ж інформація передається через ці ланцюги в абсолютно різному вигляді (тимчасові і частотні характеристики сигналів, формат представлення інформації). У цьому випадку при виборі джерела інформативних випромінювань протидіюча сторона враховує наступні фактори:

- відеосигнал є періодичним сигналом, а сигнал, який передається від клавіатури до системного блоку не періодичний;

- для періодичного сигналу можна реалізувати функцію його накопичення в приймачі, що дозволить підвищити дальність перехоплення і зменшити ймовірність помилки при відновленні інформації;

- в умовах великого міста низькочастотна складова радіодіапазону перевантажена індустріальними радіоперешкодами;

- зі збільшенням частоти сигналу збільшується коефіцієнт корисної дії антени, в якості якого виступає струмовий контур для сигналу [14].

Таким чином, найбільш вірогідним видається перехоплення ПЕМВН ланцюгів, які передають відеосигнал від відеоадаптеру (інформативні ПЕМВН). Для відображення інформації на моніторі перехоплений сигнал не потребує додаткової обробки. Крім того, зображення на екрані монітору і, відповідно, сигнали, які він випромінює, багаторазово повторюються. У професійній апаратурі це використовується для накопичення сигналів і відповідного збільшення дальності ведення розвідки.

Зображення на екрані дисплею формується в основному так само, як і в телевізійному приймачі – воно складається з точок на рядках, які світяться. Відеосигнал є цифровим: сигнал логічної одиниці створює світлову точку, а логічний нуль перешкоджає її появі. Джерелом випромінювання відеосигналу

дисплею можуть бути елементи обробки сигналу зображення перед подачею на матрицю дисплея монітора ЗОТ. На відміну від інших сигналів, які існують в дисплеї, відеосигнал підсилюється до декількох разів для подачі на матрицю. Отже, саме його випромінювання найбільш небезпечне з точки зору захисту інформації [4].

Інформація, яка відображається на екрані дисплею, може бути відновлена в монохромному вигляді за допомогою звичайного телевізійного приймача. Виділення з ПЕМВН корисної інформації про сигнал синхронізації зображення є досить складним технічним завданням. Набагато простіше ця проблема вирішується використанням зовнішніх генераторів синхронізуючих сигналів, які можуть переналаштовуватися. Навіть при використанні звичайних кімнатних антен перехоплення інформації здійснюється на відстані близько 10-15 метрів. При використанні направлених антен з великим коефіцієнтом підсилення дальність перехоплення зростає до 50-80 метрів. При цьому найкраща якість відновлення інформації відповідає текстовим зображень. Сучасний рівень розвитку електроніки дозволяє виготовити подібні пристрої перехоплення інформації невеликих розмірів, що забезпечить необхідну скритність їх роботи [7].

Опираючись на результати експериментів рівень вузькосмугових складових не залежить від розміру екрану. Він визначається системою синхронізації і частотою повторення точок, які світяться. Отже, відеопідсилювач – найбільш потужне джерело широкосмугового випромінювання, а система синхронізації – вузькосмугового. Таким чином, випромінювання дисплеїв, що містять гармоніки відеосигналів, охоплює діапазон дециметрових хвиль [4].

Слід також враховувати, що статистичні параметри інформаційного сигналу відомі зловмиснику і ним можуть застосовуватися приймальні пристрої з оптимальним фільтром.

У складі ЕОМ одночасно функціонує дуже велика кількість залежних і незалежних пристроїв. У кожному з них, наряду з інформаційними, циркулює

велика кількість службових сигналів, тактових частот і т.д. Необхідно досить точно уявляти, які саме сигнали можуть використовуватися для перехоплення закритої інформації.

Опираючись на формулювання задачі перехоплення, випливає, що найбільшу небезпеку становить випромінювання тих пристроїв, в яких критична інформація циркулює у вигляді послідовного коду.

В складі досить типової ЕОМ підпадають під поняття пристрої з послідовним кодуванням [7] наступні:

- відеопідсистема;
- накопичувачі на жорсткому дисках (включаючи зовнішні ZIP, JAZ, FLASH);
- пристрої CD, CD-R, CD-RW; DVD, DVD-RW;
- накопичувальні пристрої зовнішньої пам’яті (зовнішні вінчестери);
- клавіатура;
- послідовний порти (COM, USB, E-SATA);
- паралельний порт (PATA);
- послідовний відеопорт (HDMI, Display-PORT);
- принтери.

Ланцюги запису завжди послідовні і їх тактові частоти і тривалості імпульсів відносно постійні, наприклад CD-RW. Все інше потребує вимірювань. Те ж саме можна сказати і про диски ZIP, JAZ, FLASH. Інтерфейс може бути і паралельним, наприклад – LPT, і послідовним – USB. Оптичні диски різних моделей за інтерфейсом поділяються на паралельні (PATA) та послідовні (SATA), а вузли зчитування/запису – послідовні.

Слід зазначити, що порт за протоколом USB 1.1 працює на частоті 12 МГц, а якщо і порт, і зовнішній пристрій підтримує версію протоколу USB 2.0, то вони самі синхронізуються про взаємний обмін на довільній частоті, значення якої може доходити до 400 МГц. Цю частоту доводиться визначати безпосередніми вимірюваннями в кабелях інтерфейсу, так як

проведення спеціальних досліджень та подальших розрахунків без знання цього значення неможливе [14].

В будь-яких принтерах інтерфейс також знаходиться окремо, а вузол, що друкує, окремо. Стандартний інтерфейс – LPT (8 розрядів). В лазерних принтерах вузол друку (лазерний діод) – це завжди послідовний код. Друкуюча головка матричного, а тим паче струменевого принтера, – паралельна (дуже важливо правильно визначити кількість розрядів). В сфері технічного захисту інформації ігнорувати ці пристрої неприпустимо.

Перехоплення інформації за рахунок випромінювання клавіатури або принтера можливе у ряді випадків навіть з меншими витратами, ніж перехоплення зображення з монітору ЗОТ. Інформація в цих пристроях передається послідовним кодом, всі параметри цього коду стандартизовані і добре відомі [12], а з'єднувальні дроти достатньо довгі. До того ж клавіатура досить низькошвидкісний пристрій (тактова частота знаходиться в діапазоні від 6 до 10 кГц) [14]. Наприклад, код натиснутої клавіші «=» добре помітний навіть на осцилографі (рис. 2.5).

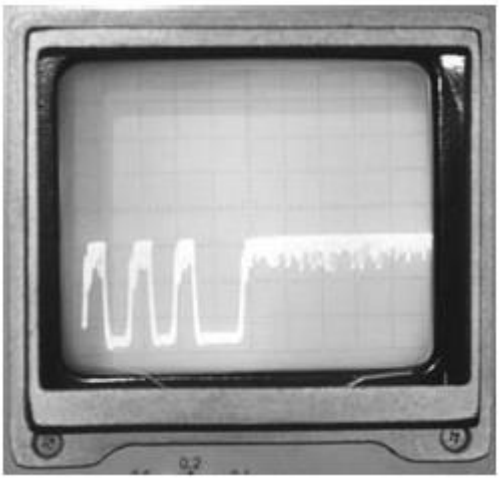


Рисунок 2.5 – Вид осцилограми знаку «=»

Стандартна клавіатура зазвичай має дуже високий рівень випромінювання. В той же час з клавіатури вводяться критичні дані (з точки зору безпеки), наприклад, паролі користувачів та адміністратора системи.

Випромінювання клавіатури займає відносно вузьку смугу і зосереджене зазвичай в області коротких і ультракоротких хвиль.

Для його такого роду випромінювання може використовуватися дуже простий короткохвильовий розвідувальний приймач. Дані, що вводяться з клавіатури, представлені в послідовному коді. Вони можуть бути легко інтерпретовані, і тому випромінювання, які створюються клавіатурою, вважаються найбільш небезпечними.

Наприклад також, ПЕМВН можуть йти від дротів інтерфейсної шини E-SATA, до якої під'єднані накопичувачі на жорстких дисках (рис. 2.6). Розрахунки випромінювань наведені у дод. Б.

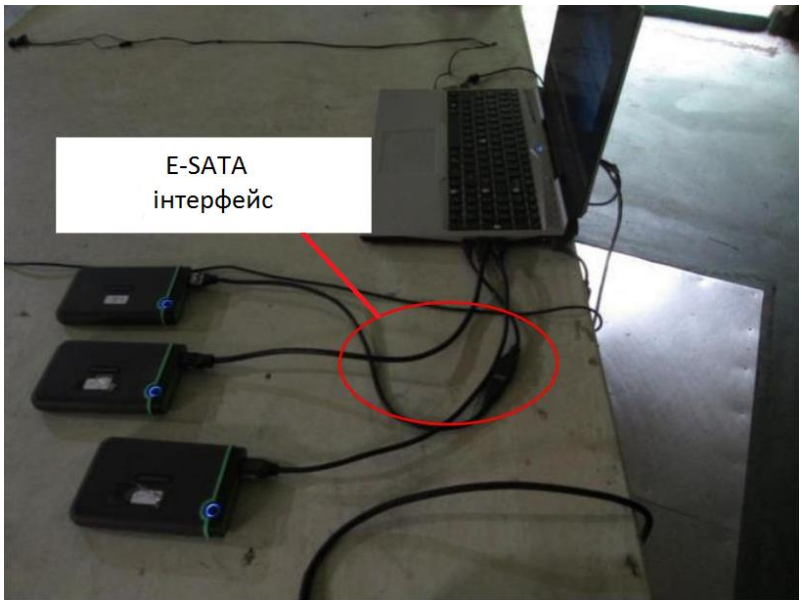
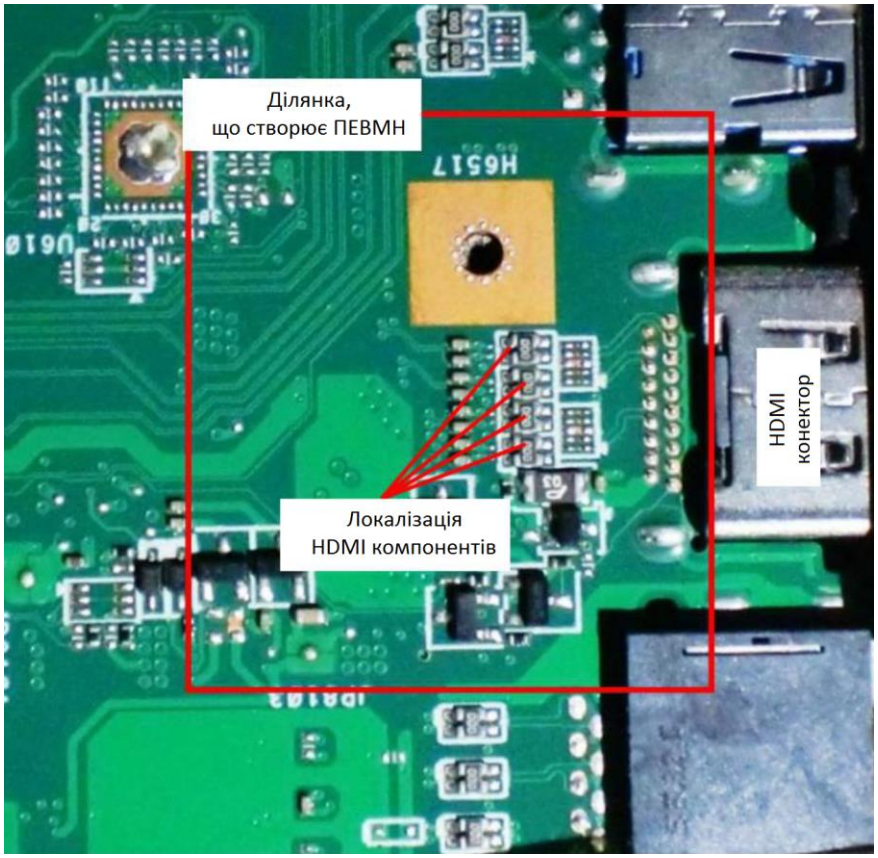
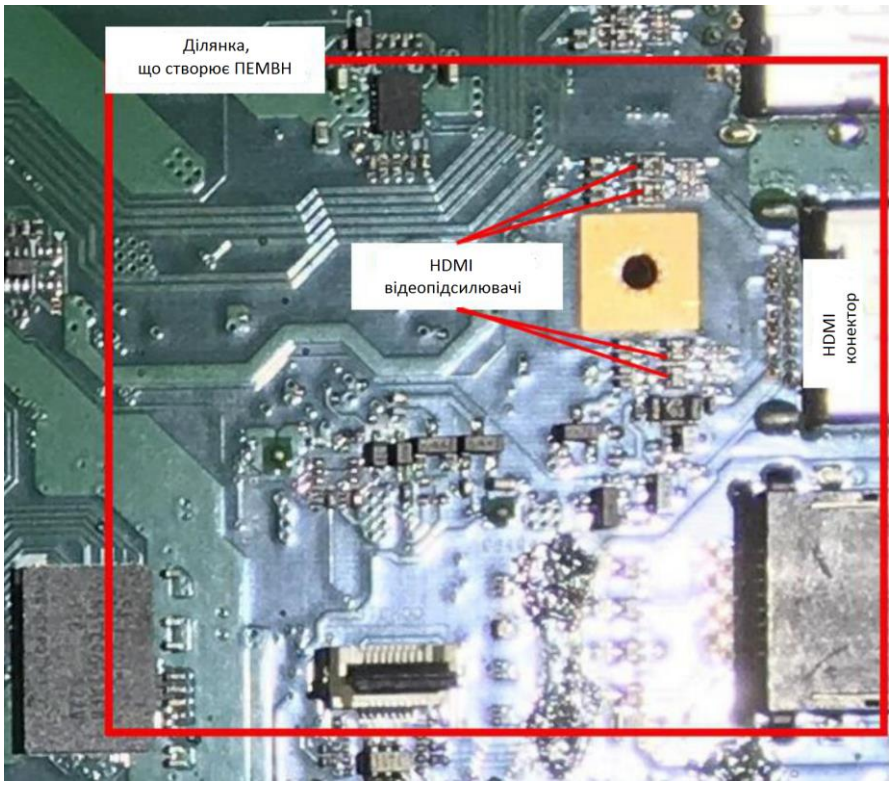


Рисунок 2.6 – З'єднання жорстких дисків з ноутбуком через інтерфейс E-SATA

В США проводились вимірювання ПЕМВН власне ноутбука, а саме відеопідсистеми материнської плати і власне LCD-матриці дисплею (рис. 2.7) [15]. Результати вимірювань представлені в табл. 2.1 [15]. Нажаль марка ноутбука не представлена, як і умови проведення спеціальних вимірювань. Але точно вказані компоненти, які створюють електромагнітні поля в процесі передачі відеоінформації через інтерфейс HDMI від материнської плати до контролера шини HDMI LCD-матриці дисплею ноутбука – це компоненти відеопідсилювачів рівнів сигналів.



а



б

Рисунок 2.7 – Відеопідсистема ноутбука: материнська плата – *а*; плата з відеоконтролером LCD-матриці дисплею ноутбука – *б*

Таблиця 2.1 – Результати вимірювань рівнів напруженості електричного поля від ноутбука

Материнська плата						
Частота, МГц	297		594		891	
Поляризація антени	гориз.	верт.	гориз.	верт.	гориз.	верт.
Результати, дБ|В/м	-8,767	-1,667	-8,441	-11,815	-2,578	-4,728
Плата LCD-матриці						
Частота, МГц	297		594		891	
Поляризація антени	гориз.	верт.	гориз.	верт.	гориз.	верт.
Результати, дБ|В/м	-6,567	-7,767	-9,741	-10,515	-10,777	-7,629

Для прикладу, результати вимірів рівня електричної (рис. 2.8) і магнітної (рис. 2.9) складових, проведених компанією «ЕПОС» спільно з Науково-дослідним інститутом електронно-механічних приладів, показали, що в комп’ютерах з різними корпусами системних блоків, які серійно випускаються, потужність побічних випромінювань від клавіатури може відрізнятися більш ніж у 100 разів [16].

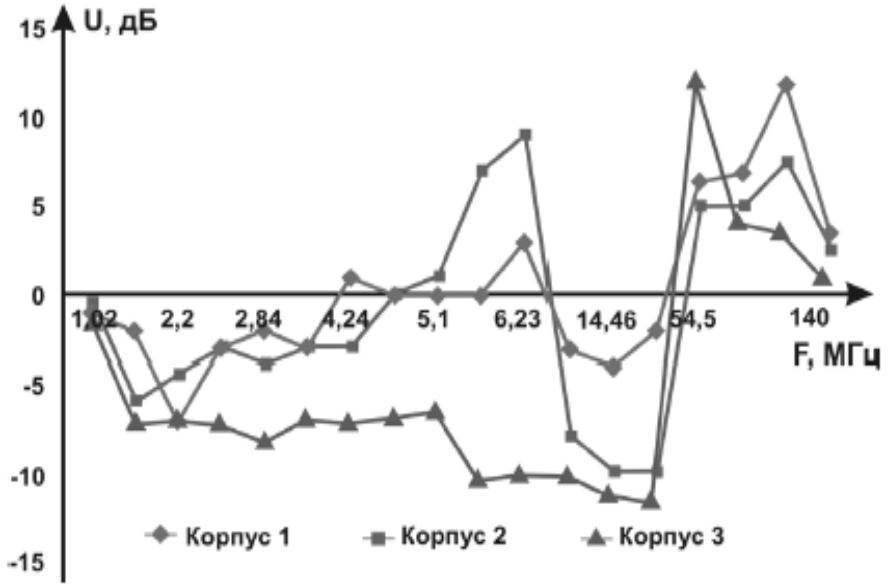


Рисунок 2.8 – Рівні випромінювання електричної складової електромагнітного поля корпусів персональних комп’ютерів

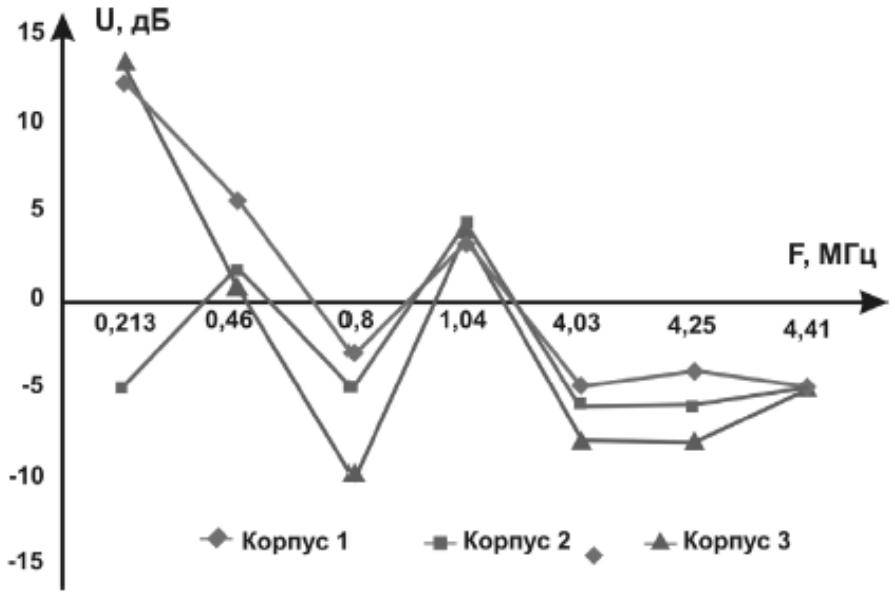


Рисунок 2.9 – Рівні випромінювання магнітної складової електромагнітного поля корпусів персональних комп’ютерів

Аналогічні співвідношення отримуються і для інших пристроїв, які входять до складу ПК.

Одним із потужних джерел випромінювання в ПК є система синхронізації. Однак перехоплення немодульованих гармонік тактової частоти не зацікавить нікого. При використанні для перехоплення ПЕМВН звичайного побутового радіоприймача є можливість розпізнавання на слух моментів зміни режимів роботи персонального комп’ютера, звернення до накопичувачів інформації на жорсткому або CD-RW, натискання клавіш, друк на принтері. Але така інформація використовується зазвичай як допоміжна.

2.3 Перехоплення IP-пакетів в локальних мережах

Одним із способів перехоплення інформації в локальній мережі ETHERNET є безпосереднє під’єднання з метою відгалуження частини пакетів зловмисником чи трафіку в цілому на додаткове обладнання з метою подальшого аналізу перехопленої інформації. Досить часто це роблять зловмисники через персональний комп’ютер в безпосередній близькості в тій же мережі (рис. 2.10) або відповідні спецслужби безпосередньо на стороні

провайдера Інтернет послуг (рис. 2.11) [17]. Розрахунки ПЕМВН від дротів ETHERNET приведені у дод. Б.

Рисунок 2.10 – Атака через хибні запити ARP на хост 2

Розглянемо як зловмисник може скористатися протоколом ARP для виконання перехоплення інформації в мережі між хостами 1 та 2. Для перехоплення мережевого трафіку між хостами 1 та 2 зловмисник нав’язує цим хостам свою IP-адресу, щоб хости 1 та 2 використовували цю сфальсифіковану IP-адресу при обміні повідомленнями. Для нав’язування своєї IP-адреси зловмисник виконує наступні операції:

- зловмисник визначає MAC-адреси хостів 1 та 2, наприклад, за допомогою команди nbtstat з пакету W2RK;

- зловмисник відправляє на виявлені MAC-адреси хостів 1 та 2 повідомлення, які представляють собою сфальсифіковані ARP-відповіді на запити дозволу IP-адрес хостів в MAC-адресах комп’ютерів (хосту 1 повідомляється, що IP-адреса хоста 2 відповідає MAC-адреса комп’ютера зловмисника, тоді як хосту 2 повідомляється, що IP-адреса хоста 1 також відповідає MAC-адреса комп’ютера зловмисника);

- хости 1 та 2 заносять отримані MAC-адреси в свої кеші ARP і потім використовують їх для відправки повідомлень один одному.

Тоді виходить, що IP-адресам 1 та 2 хостів відповідає MAC-адреса комп’ютера зловмисника, а хости 1 та 2, так нічого і не підозрюючи,

спілкуються через посередника, який може з їх повідомленнями робити що завгодно.

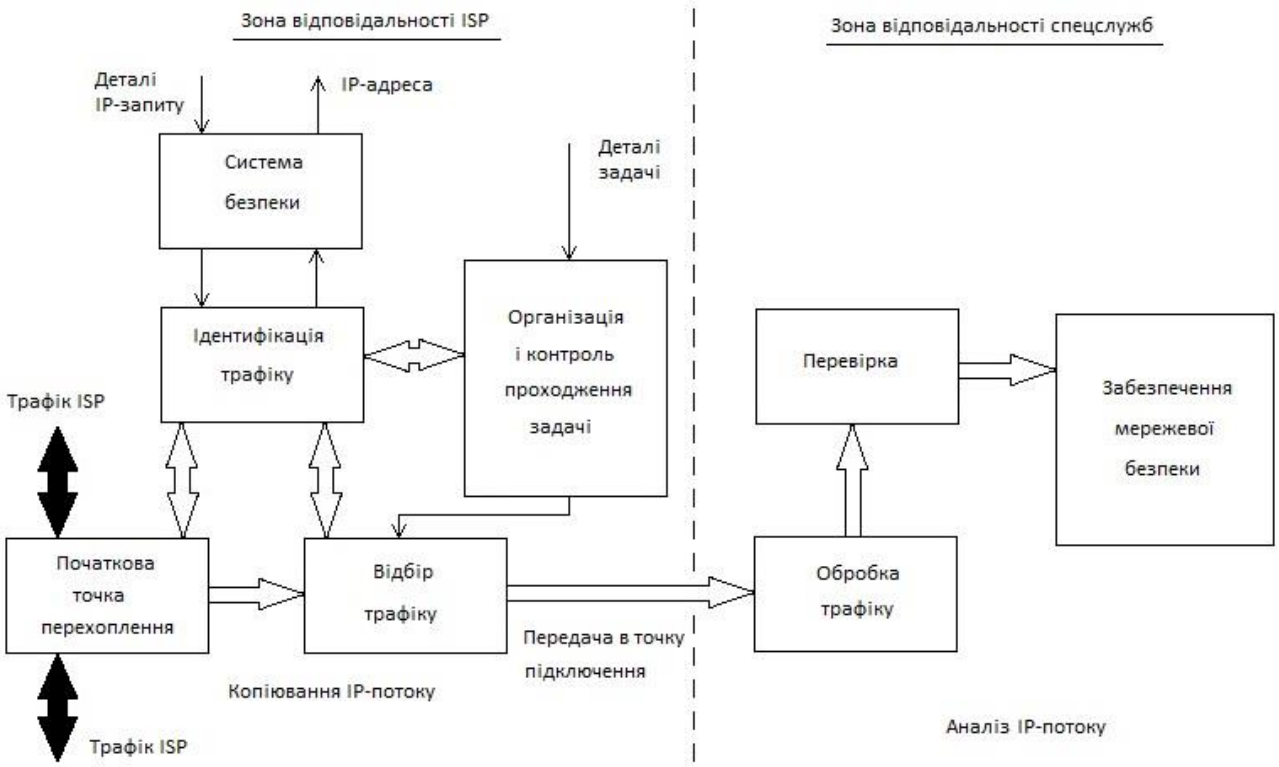


Рисунок 2.11 – Спосіб відгалуження IP-пакетів на стороні провайдера для аналізу відповідними спецслужбами

Системи перехоплення IP-пакетів бувають: активні (складові системи ISP, додаткове програмне забезпечення), напівактивні (динамічне IP-перехоплення, рівень OSI) і пасивні (статичний відвід на IP-рівні всіх комунікацій та запитів, як на рис. 2.11). IP-моніторинг буває зі змінними IP-адресами на комутованих каналах (dial-up) і з постійними IP-адресами (виділений канал, GPRS, LAN, xDSL тощо) [17].

Найбільш «тиха», тобто непомітна для користувача і Інтернет провайдера буде пасивна система моніторингу IP-адрес з розмежуванням повноважень і з можливістю відводу IP-пакетів для їх оперативного поточного аналізу. Цей спосіб є найбільш раціональним рішенням пасивного перехоплення IP-пакетів апаратурою спецслужб для організації відбору трафіку і виявлення протиправних дій з конкретного хоста.

Ще одним зі способів перехоплення трафіку є хибна маршрутизація (рис. 2.12).

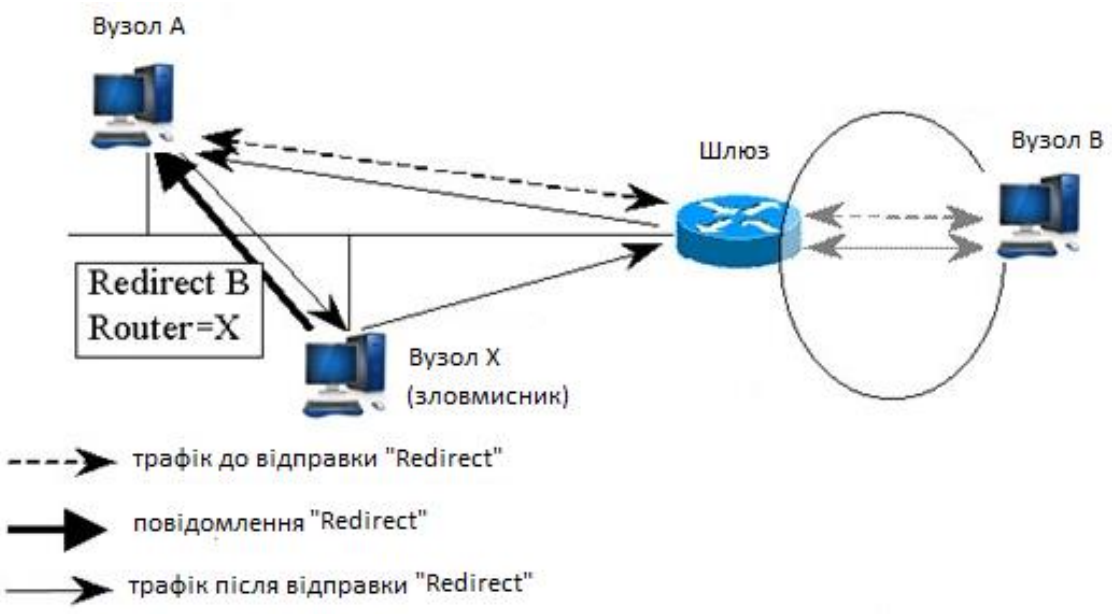


Рисунок 2.12 – Хибна маршрутизація

Щоб перехопити мережевий трафік, зловмисник може підмінити реальну IP-адресу мережевого маршрутизатора своєю IP-адресою, виконавши це, наприклад, за допомогою сфальсифікованих ICMP-повідомлень «Redirect». Отримане повідомлення «Redirect» вузол А повинен сприйняти як відповідь на датаграму, відправлену іншому вузлу В. Свої дії на повідомлення «Redirect» вузол А визначає, виходячи зі змісту отриманого повідомлення «Redirect», і якщо в «Redirect» задати перенаправлення датаграм з А до В за новим маршрутом, то вузол А це і зробить.

Для виконання хибної маршрутизації зловмисник повинен знати деякі подробиці щодо організації локальної мережі, в якій знаходиться вузол А, а саме, IP-адресу маршрутизатора, через який відправляється трафік з вузла А до В. Знаючи це, зловмисник сформує IP-датаграму, в якій IP-адреса відправника визначається як IP-адреса маршрутизатора, а отримувачем буде вказано вузол А. Також в датаграму включається повідомлення ICMP «Redirect» з полем адреси нового маршрутизатора, встановленим як IP-адреса

комп'ютера зловмисника (вузол X). Отримавши таке повідомлення, вузол A буде відправляти всі повідомлення за IP-адресою вузла X.

Існує також можливість захоплення мережевих пакетів за допомогою спеціального програмного модуля (сніфер-програми). Розглянемо популярну програму Wireshark (рис. 2.13), яка використовується для захоплення мережевого трафіку і призначена для збору і аналізу мережевих IP мережевих пакетів/протоколів.

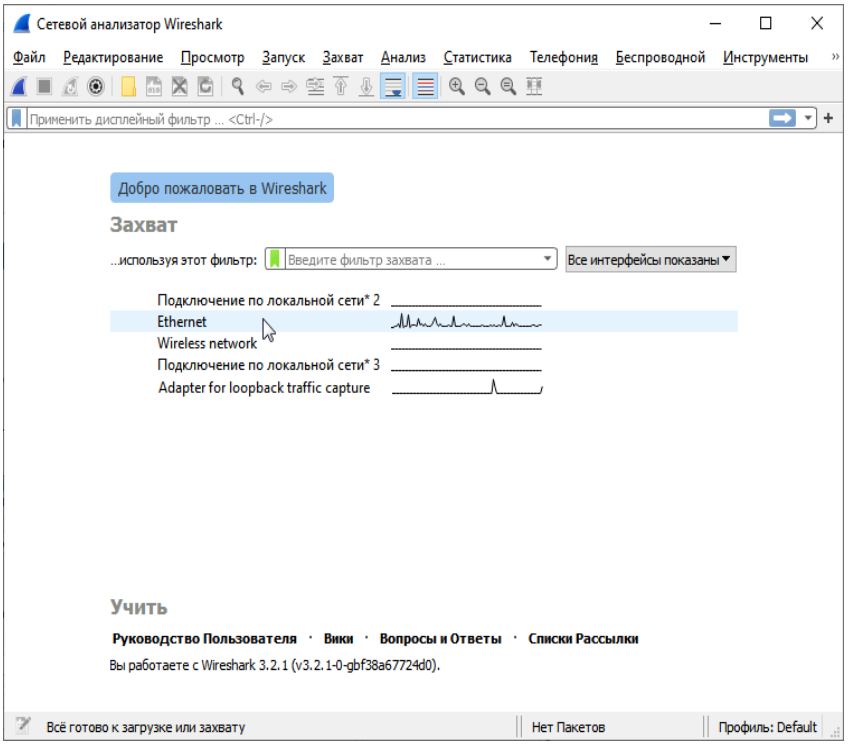
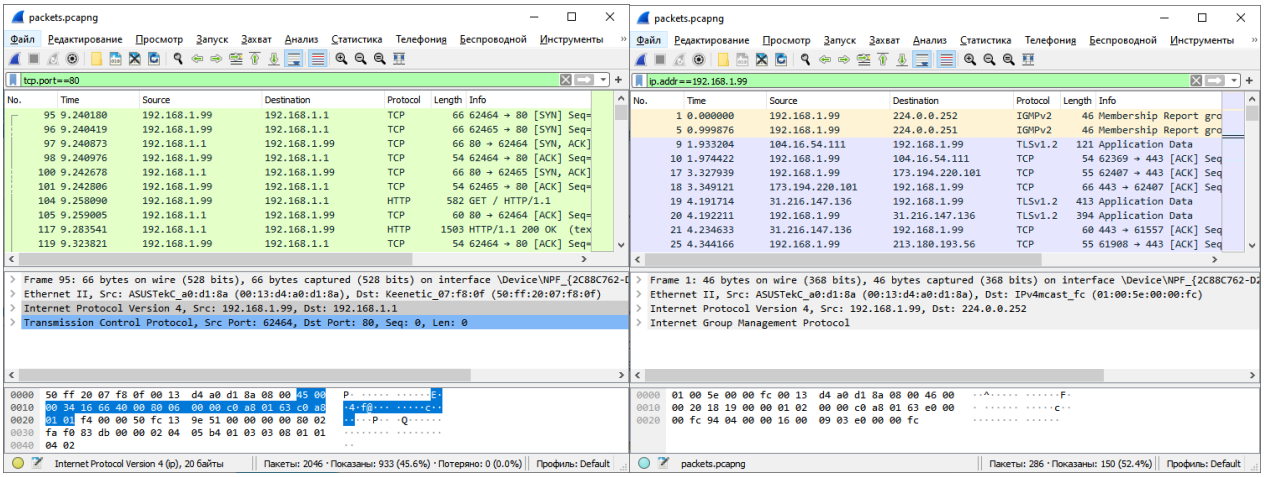


Рисунок 2.13 – Програмний пакет Wireshark

Сніфер розподіляє захоплені IP-пакети за рівнями і протоколами. Деякі пакети можуть навіть розпізнати протокол і відображати перехоплену інформацію. Будь-який сніфер може розпізнати протокол TCP, а серйозніші сніфери вміють визначати, якими програмними додатками згенерований даний трафік. Більшість таких аналізаторів протоколів розпізнають понад 500 різних протоколі і вміють описувати і декодувати їх за іменами.

Наприклад, відскановані мережеві пакети видно в Wireshark (рис. 2.14, а), а декодовані нас цікавлять з IP-адреси 192.168.1.99 (рис. 2.14, б).



а *б*

Рисунок 2.14 – Робота Wireshark: відскановані пакети – *а*;
пакети з IP-адреси 192.168.1.99 – *б*

Єдиним методом захисту від перехоплення мережевого трафіку є використання програм, що реалізують криптографічні алгоритми і протоколи шифрування, і дозволяють унеможливити розкриття чи підміну секретної інформації. Для вирішення таких задач криптографія надає засоби для шифрування, електронного підпису і перевірки справжності повідомлень, що передаються захищеними протоколами.

3 МЕТОДИКИ ВИЗНАЧЕННЯ ЗАХИЩЕННОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ПЕМВН

3.1 Вимоги нормативних документів в сфері технічного захисту інформації

Згідно з вимогами, що встановлюються чинними нормативними документами, роботи з технічного захисту інформації (ТЗІ) в автоматизованих системах (АС) для електронно-обчислювальної техніки (ЕОТ) передбачають:

- обстеження (в тому числі технічний контроль) об’єктів ЕОТ;
- технічний контроль за ефективністю вжитих заходів захисту.

Обстеження (технічний контроль) об’єктів ЕОТ в процесі створення комплексної системи захисту інформації (КСЗІ) проводиться на попередньому етапі робіт. Контроль за ефективністю вжитих заходів захисту проводиться на етапі випробувань і передачі КСЗІ в експлуатацію.

На підставі аналізу матеріалів обстеження та окремих моделей загроз визначаються головні та часткові задачі захисту інформації, розробляються організаційні, первинні та основні технічні заходи щодо ТЗІ та вказівки про порядок їх реалізації.

Остаточний висновок про ефективність заходів ТЗІ, що були вжиті під час створення системи захисту, дається за результатами інструментального контролю.

Рекомендований алгоритм обстеження містить такі процедури:

- аналіз у технічних засобах ЕОТ потоків інформації з обмеженим доступом;
- визначення складу технічних засобів і ДТЗС на об’єкті ЕОТ;
- визначення складу кабельних ліній, що виходять за межі контрольованої зони і мають паралельну прокладку з кабелями АС;
- виявлення комунікацій, що проходять через територію об’єкта ЕОТ і мають вихід за межі контрольованої зони;
- інструментальне вимірювання інформативних ПЕМВН;

- оцінку відповідності рівнів сигналів і параметрів полів, які є носіями інформації з обмеженим доступом, нормам ефективності захисту.

Основними параметрами можливого витоку інформації каналами ПЕМВН є:

- напруженість електричного поля інформативного (небезпечного) сигналу;

- напруженість магнітного поля інформативного (небезпечного) сигналу;

- величина напруги інформативного (небезпечного) сигналу;

- величина напруги наведеного інформативного (небезпечного) сигналу;

- величина напруги шумів (завад);

- величина струму інформативного (небезпечного) сигналу;

- величина чутливості до впливу магнітних полів для точкового джерела;

- величина чутливості апаратури до впливу електричних полів;

- величина чутливості до впливу акустичних полів;

- відношення «інформативний сигнал/шум»;

- відношення напруги небезпечного сигналу до напруги шумів (завад) у діапазоні частот інформативного сигналу.

Зазначені параметри визначаються і розраховуються за результатами вимірювань у заданих точках. Гранично допустимі значення основних параметрів є нормованими величинами і визначаються за відповідними методиками.

Максимально допустиме відношення пікової напруги сигналу до середньоквадратичної напруги шуму визначається відповідно до чинних норм ефективності захисту інформації в АС управління і ЕОТ [5].

У ході контролю перевіряються електромагнітні поля інформативних (небезпечних) сигналів у широкому діапазоні частот навколо апаратури та кабельних з’єднань ЕОТ, наявність інформативних (небезпечних) сигналів у колах, проводах електроживлення та заземленні ТЗПІ та ДТЗС.

Під час спецдосліджень визначається радіус, за межами якого відношення «інформативний сигнал/шум» менше гранично допустимої

величини. Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витоку каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витоку, проводиться порівняння фактичних параметрів з нормованими [18].

У випадку перевищення допустимих значень розробляються захисні заходи, використовуються засоби захисту.

Після проведення спеціальних досліджень та впровадження засобів захисту проводиться контроль за ефективністю застосованих технічних засобів захисту.

У процесі роботи технічних засобів і захищеної техніки, у міру необхідності, проводиться оперативний контроль за ефективністю захисту каналів витоку інформативного (небезпечного) сигналу.

Завдання захисту інформації від витоку технічними каналами потребує вирішення ряду питань, у тому числі вивчення фізичних явищ, що призводять до появи паразитних інформаційних сигналів в навколишньому просторі, розробки конкретних методів і засобів запобігання можливості витоку інформації.

Одним з основних моментів процесу захисту інформації від витоку є розробка критеріїв оцінки захищеності інформації та норм на параметри інформаційних сигналів, тобто сигналів, що несуть інформацію, виконання яких не дозволить здійснити перехоплення інформації [16].

Випробування ЕОТ на відповідність вимогам також проводять:

- при розробці (попередні, приймальні та сертифікаційні випробування);

- при постановці на виробництво (кваліфікаційні та сертифікаційні випробування);

- при серійному виготовленні і моделюванні (періодичні, типові і сертифікаційні випробування);

- для засобів, на які отримують експертні висновки або сертифікати відповідності нормам захисту інформації;

- при атестації приміщень, на яких встановлені ЕОТ, і в процесі експлуатації ЕОТ (об’єктові випробування).

Випробування ЕОТ на відповідність вимогам включають:

- перевірку виконання вимог до розмірів зон 1, 2;

- перевірку наявності в ЕОТ паразитної генерації.

Всі випробування, крім об’єктових, проводять в безехових камерах, радіопрозорих павільйонах (приміщеннях) або на відкритих майданчиках, що задовольняють вимогам відповідних методик. Допускається проводити випробування в спеціально обладнаних екранованих приміщеннях.

Результати об’єктових випробувань ЕОТ на відповідність вимогам щодо захисту інформації, що обробляється, вважають позитивними, якщо отримані значення їх радіусів зон 1 та 2 не перевищують заданих значень, і в ЕОТ відсутня паразитна генерація.

3.2 Модель каналу витоку інформації за рахунок ПЕМВН

Завданням спеціальних досліджень є виявлення та вимірювання величин інформаційних сигналів в каналах можливого витоку інформації – «небезпечних» сигналів. Причому, як правило, перша частина завдання є визначальною. Помилка на цьому етапі незмінно призводить або до «пропуску» небезпечних сигналів, або до завищення результатів.

Для розуміння фізичного змісту задачі розглянемо найпростішу модель довільного технічного каналу витоку (рис. 3.1).

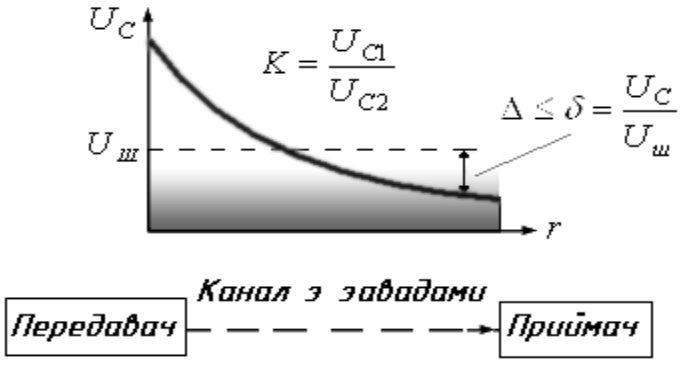


Рисунок 3.1 – Модель каналу витоку

Як і будь-який інший канал зв’язку, канал витоку складається з передавача, каналу і приймача. Канал, в загальному випадку, це якесь матеріальне середовище, в якому відбувається поширення сигналу передавача. Канал витоку, як і всякий канал зв’язку і має дві основні характеристики – погонне загасання і якийсь рівень шумів. Реалізацією такого узагальненого каналу може служити тверде тіло (стіна, труба), провідна лінія, область простору (для електромагнітної хвилі) і т.д.

Приймач в даній моделі – це потенційний противник разом з якимись технічними засобами перехоплення інформації або без них.

Якщо розглянути задачу захисту інформації від можливого витоку в поняттях наведеної моделі, то в точці розміщення потенційного противника необхідно забезпечити таке співвідношення сигнал/шум, яке не дозволить противнику отримати інформацію.

Завдання спеціальних досліджень, як комплексу робіт, дозволяє встановити, чи можливий витік інформації в цьому каналі і зводиться до вимірювання сигналів передавача і перерахунку виміряних значень до величини, яка може надійти на вхід оптимально адаптованого до даного виду інформації приймача потенційного зловмисника [14].

3.3 Методики оцінки захищеності об’єкта

Найважливіший і необхідний напрям робіт із захисту інформації – контроль ефективності захисту інформації. Контроль проводиться силами служби безпеки, керівниками організації та структурних підрозділів, всіма співробітниками організації, допущеними до закритої інформації.

Виділяють три види технічного контролю:

1. Інструментальний.

2. Інструментально-розрахунковий.

3. Розрахунковий.

Інструментальні методи контролю забезпечують найбільш точні результати, так як вони реалізуються за допомогою засобів вимірювальної

техніки в місцях контролю, перш за все на межі контрольованої зони. Для інструментального контролю необхідні високочутливі дорогі вимірювальні прилади. Ця обставина істотно ускладнює реальні можливості проведення контролю.

Найбільші проблеми виникають при інструментальному контролі ПЕМВН, так як частоти побічних випромінювань охоплюють практично весь радіодіапазон. Стандартна контрольно-вимірювальна апаратура не забезпечує проведення досліджень ПЕМВН в необхідному обсязі. Тому для цих цілей використовуються дорогі спеціальні прилади та прилади для фізичних наукових досліджень. Для вимірювань сигналів ПЕМВН застосовуються вимірювальні приймачі, селективні мікровольтметри, аналізатори спектра з технічними характеристиками:

- діапазон частот – десятки Гц – десятки ГГц;
- чутливість – десятки – сотні нВ;
- динамічний діапазон – 100 - 150 дБ;
- вибірковість – одиниці Гц – одиниці МГц;
- точність вимірювання рівня сигналу – 1 - 2 дБ.

Так як багато сигналів ПЕМВН мають імпульсний характер і відповідно до вимог нормативних документів, ці прилади повинні мати пікові та квазіпікові детектори. Дуже корисно для можливості автоматизації вимірювань наявність у вимірювальних приладів програмно-апаратного інтерфейсу з ЕОМ.

Інструментально-розрахунковий технічний контроль дозволяє знизити вимоги до параметрів вимірювальної техніки. Ці методи передбачають проведення вимірювань не на кордоні контрольованої зони, а поблизу можливих джерел сигналів. Біля джерел сигналів рівні випромінювання вищі і, відповідно, вимоги до чутливості вимірювальних приладів нижчі. Рівні же сигналів в місцях проведення контролю розраховуються за відповідними методиками розрахунку. Так як у якості вихідних даних для розрахунку застосовуються результати вимірювань, то точність контролю буде визначатися точністю вимірювань і використаного математичного апарату.

В решті решт, якщо відсутні необхідні для інструментального або інструментально-розрахункового контролю вимірювальні прилади, то здійснюється розрахунковий технічний контроль шляхом проведення розрахунків за апріорними або довідковими вихідними даними. Існуючі методи розрахункового технічного контролю забезпечують допустимі для практики результати при оцінці загроз підслуховування і спостереження.

До останнього методу технічного контролю відноситься графічний метод розрахунку радіуса зони II (R2) технічних засобів ЕОТ.

В основу методу покладена усереднена стандартна функція послаблення електромагнітного поля, що поширюється у вільному просторі (півсфері) над напівпровідною поверхнею [14].

3.4 Визначення функції послаблення ПЕМВН при поширенні в просторі

Технічні засоби обробки інформації вважаємо точковим електричним випромінювачем, оскільки його розміри істотно менші відстані до точки можливого перехоплення інформації. Представимо технічний засіб обробки інформації у вигляді диполя, розміщеного в точці нульового відліку сферичної системи координат, як показано на рис. 3.2.

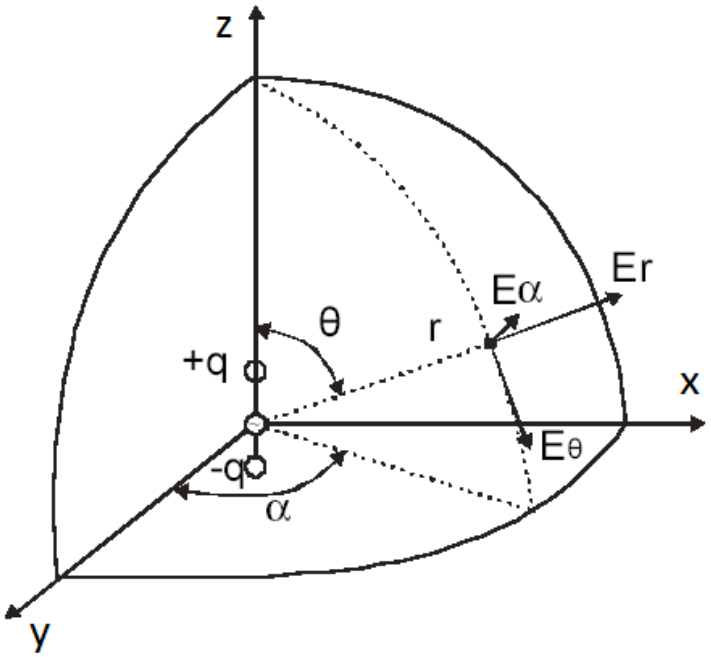


Рисунок 3.2 – Елементарний електричний випромінювач

Математичні вирази для визначення параметрів поля джерел ПЕМВН можна отримати з класичної теорії технічної електродинаміки, використовуючи вираз для векторного потенціалу [4].

Для вирішення рівнянь Максвелла вводяться параметри електромагнітного поля – електричний і магнітний потенціали: A і φ:

$$\varphi = \frac{1}{4\pi\varepsilon_0}\int_V \frac{\rho\left(t-\frac{r}{i}\right)dV}{r}; \qquad A = \frac{\mu_0}{4\pi}\int_V \frac{\delta_i\left(t-\frac{r}{i}\right)dV}{r}, \tag{3.1}$$

де ρ і δ_i – об'ємні площині заряду і струму; r – відстань до точки спостереження.

Для лінійного струму векторний потенціал відповідно дорівнює:

$$A = \frac{\mu_0}{4\pi}\int_e \frac{\delta dl}{r}.$$

З урахуванням формул (3.1):

$$\begin{cases} \bar{E} = -\left(grad\varphi + \dfrac{d\bar{A}}{dt}\right); \\ \bar{H} = \dfrac{1}{\mu_0} rot\bar{A}. \end{cases}$$

Реальні випромінювачі можна розглядати як сукупність елементарних електричних і магнітних випромінювачів (диполів). Розглянемо елементарний електричний випромінювач та особливості електромагнітного поля в безпосередній близькості від джерела.

В полярній системі координат елементарний електричний випромінювач представлений на рис. 3.2. Тоді компоненти електромагнітного поля елементарного електричного випромінювача матимуть такий вигляд [19]:

$$\dot{\bar{E}}_r = \frac{jl\cos\theta}{2\pi\omega\varepsilon_0 r^3}\left(1 + j\alpha r^2\right)e^{-j\omega};$$

$$\dot{\bar{E}}_\theta = \frac{jl\sin\theta}{4\pi\omega\varepsilon_0 r^3}\left(1 + j\alpha r - \alpha^2 r^2\right)e^{-j\omega};$$

$$\dot{\bar{H}}_\alpha = \frac{jl\sin\theta}{4\pi r^2}\left(1 + j\alpha r\right)e^{-j\omega},$$

де $\alpha = \frac{2\pi}{\lambda} = \frac{\omega}{c}$; $j = i\omega\dot{q}$.

В екваторіальній площині (горизонтальна площина) маємо:

$$\begin{cases} \dot{\bar{E}}_\theta = \dot{M}\left(\frac{1}{(\alpha r)^3} + \frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right); \\ \dot{\bar{H}}_\alpha = \frac{\dot{M}}{\rho}\left(\frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right), \end{cases} \tag{3.2}$$

де $\dot{M} = \frac{ql}{4\pi\varepsilon\varepsilon_0}\alpha^3$ – параметр випромінювача; $\rho = \sqrt{\frac{\mu_0}{\varepsilon_0}} = \frac{1}{\varepsilon_0 c}$; $c = \frac{1}{\sqrt{\mu_0\varepsilon_0}}$ – швидкість світла у вакуумі.

При $\alpha r < 1$, тобто $\left(r \le \frac{\lambda}{2\pi}\right)$ – ближня зона випромінювання і напруга електричного поля визначається як:

$$\dot{E}_\theta = \frac{\dot{q}l}{4\pi\varepsilon_0}\frac{1}{r^3},$$

а електричне поле має потенційний характер.

Хвильовий опір в ближній зоні:

$$\frac{E_\theta}{H_\alpha} = \frac{1}{j\alpha r}\rho; \qquad \rho = \sqrt{\frac{\mu_0}{\varepsilon_0}} \approx 377 \text{ Ом}.$$

Враховуючи, що співвідношення компонент поля атмосферних перешкод, визначають межу зони радіоперехоплення $\frac{E_m}{H_m} = \rho$.

Радіус зони перехоплення визначається тільки електричним полем E_θ.

В дальній зоні $\alpha r >> 1$ (хвильова зона):

$$\left|\dot{\bar{E}}_0\right| = \frac{\dot{M}}{\alpha r} = \frac{\dot{q}l\alpha^3}{4\pi\varepsilon\varepsilon_0}\frac{1}{\alpha r} = \frac{\dot{q}l\alpha^2}{4\pi\varepsilon\varepsilon_0}\frac{1}{r}.$$

Так як співвідношення компонент поля маскуючих атмосферних шумів в ефірі також взаємопов’язані тим же хвильовим опором середовища 377 Ом, то розрахункове значення зони радіоперехоплення буде однакове як по магнітній, так і по електричній складовій [4].

Нижче наводяться графіки законів спадання компонент поля для елементарного електричного випромінювача (рис. 3.3).

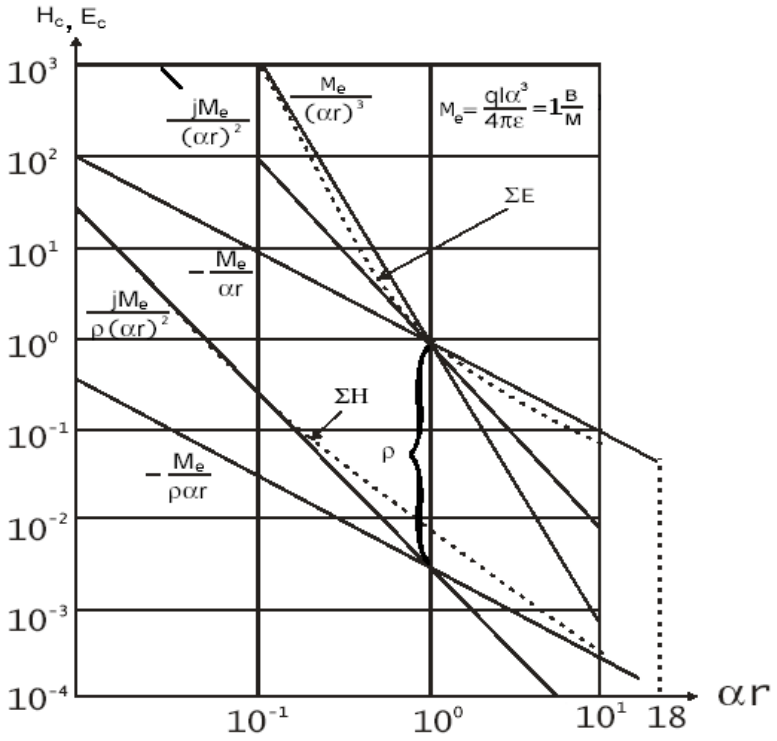


Рисунок 3.3 – Складові поля елементарного електричного випромінювача

З урахуванням аналізу рівняння електромагнітного поля (3.2) та з урахуванням практичних вимірювань для реальних випромінювачів інформаційних сигналів при визначенні граничного радіуса радіоперехоплення використовується дещо інший закон спадання поля. Він відрізняється від закону спадання елементарного електричного випромінювача за рахунок збільшеної квадратичної ділянки від $r = 0{,}16\lambda$ до $r = 3\lambda$ (рис. 3.4).

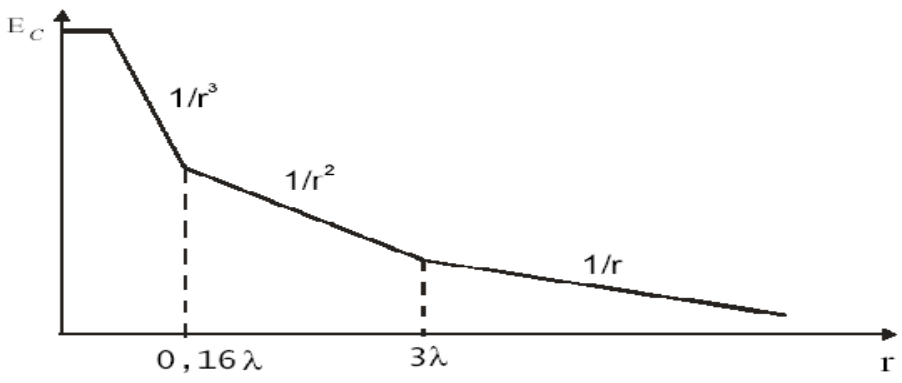


Рисунок 3.4 – Функція спадання електромагнітного поля ненавмисного випромінювача

При цьому ненавмисний електричний випромінювач буде розглядатися як квазіточковий.

Аналітична залежність цих ділянок:

кубічна ділянка $E_{\text{с}} = \frac{M}{\alpha^3}\frac{1}{r^3}$ при $r \le 0{,}16\lambda$;

квадратична ділянка $E_{\text{с}} = \frac{M}{\alpha^2}\frac{1}{r^2}$ при $0{,}16\lambda \ge r \ge 3\lambda$;

лінійна ділянка $E_{\text{с}} = \frac{M}{6\pi\alpha}\frac{1}{r}$ при $r \ge 3\lambda$.

З огляду на те, що при роботі технічних ЗОТ виникають електричні та магнітні випромінювання, причому їх співвідношення між собою, в загальному вигляді, невідомі, необхідно вимілювати поблизу випромінювача електричне і магнітне поле (диполь, рамка) і окремо позаховувати R_2 для E і для H і вибрати з них максимальне значення.

Для реальних випромінювачів електричного поля на частотах до 50 МГц при розрахунку зони радіоперехоплення необхідно використовувати поправочний коефіцієнт $K_{d/h}$, що враховує відміну електричного поля реального випромінювача від елементарного за рахунок кінцевих габаритів випромінювача ($2h$).

В загальному вигляді при вимірюванні поля електричним диполем

$$K_{d/h} = \frac{E_{\text{с}}}{E_{\text{точ}}},$$

де $E_{\text{точ}} = E_{\theta} = \frac{ql}{4\pi\varepsilon_0}\frac{1}{r^3}$ для значення $d = 1$ м при $K = 0{,}46$.

При вимірюванні поля штирової антени для значення $d = 1$ м, $K = 0{,}28$ на частотах 150 МГц і вище, значення цього коефіцієнта наближається до одиниці, тобто випромінювач стає квазіточковим.

3.5 Метод розрахунку радіуса зони *R*2 для засобів ЕОТ

Критерієм захищеності інформації є умова, що на кордоні зони *R2* має виконуватися така умова співвідношення сигнал/шум:

$$\frac{U_{\text{с}}(R)}{U_{\text{ш}}} = \delta .$$

Знаючи закон спадання небезпечного сигналу, що визначено раніше, можна записати:

$$U_{\text{с}}(R) = U_{\text{с}}(d) F(d \to R) .$$

Значення рівня шуму на вході пристрою перехоплення (2-ї і 3-ї категорій об’єктів):

$$U_{\text{ш}} = U_{\text{ш}N} \sqrt{\Delta F_{\text{опт}}} .$$

Отже, для об’єктів 2 і 3 категорії аналітичний вираз для розрахунку зони *R*2 буде виглядати наступним чином:

$$\frac{U_{\text{с}}(d) F(d \to R)}{U_{\text{ш}N} \sqrt{\Delta F_{\text{опт}}}} = \delta .$$

Перепишемо цю формулу таким чином, щоб параметри сигналу були в лівій частині рівняння:

$$\frac{U_{\text{с}}(d)}{\delta \sqrt{\Delta F_{\text{опт}}}} = \frac{U_{\text{ш}N}}{F(d \to R)} .$$

Для визначення зони *R*2 по електричному полю маємо:

$$\frac{E_{\text{с}}(d)}{\delta \sqrt{\Delta F_{\text{опт}}}} = \frac{E_{\text{ш}N}}{F(d \to R)} .$$

Ліва частина рівняння зони являє собою рівень нормованого сигналу, тобто

$$E_{\text{с}N} = \frac{E_{\text{с}}}{\delta \sqrt{\Delta F_{\text{опт}}}} .$$

Праву частину рівняння зони можна побудувати у вигляді єдиної номограми.

Для квазіоптимального приймача рівень небезпечного сигналу на його вході визначається таким чином:

$$E_{\text{с}} = \sqrt{\sum_{1/T} E_{\text{с}i}^2}; \qquad \Delta F_{\text{опт}} = F_T,$$

де $E_{\text{с}i}$ – рівень гармонік тест-сигналу.

Для практичної роботи аналітичний вираз для розрахунку зони $R2$ за допомогою номограми виглядає наступним чином:

$$E_{\text{с}N} = \frac{\sqrt{\sum_{1/T} E_{\text{с}i}^2}}{\delta K_{\text{н}} K_{\text{ф}} K_{d/n} \sqrt{\Delta F}},$$

де $K_{\text{н}}$ – коефіцієнт нормування сигналу з паралельним кодом; $K_{\text{ф}}$ – коефіцієнт форми кодування сигналів; $K_{d/n}$ – коефіцієнт відміни поля від прийнятого в номограмі для різних значень d.

Для обчислення $R2$ необхідно розрахувати за наведеною вище формулою нормоване значення сигналу, а за результатами вимірювання для відповідної частоти визначити за номограмою значення приватної зони. З усіх отриманих приватних зон вибрати максимальну, яка відповідає $R2$.

Для об’єктів ЕОТ 1-ї категорії (оптимальна фільтрація) на кордоні $R2$ має виконуватися наступна нерівність:

$$\sum_i \left(\frac{\Delta i(R)}{\delta} \right)^2 \le 1 \text{ або } \sum_i \left(\frac{E_{\text{с}i} K_0(l \to R)}{E_{\text{ш}} \delta K \sqrt{\Delta F}} \right)^2 \le 1,$$

де $K = \frac{K_{\text{н}} K_{\text{ф}} K_{d/n}}{KD}$; $K_0(l \to R)$ – функція стандартного послаблення поля.

Дане рівняння зони вирішується графоаналітичним методом або на ЕОМ.

3.6 Інструментально-розрахунковий технічний контроль ПЕМВН

Для проведення повного об’єму робіт з дослідження небезпеки ПЕМВН необхідно мати:

- контрольно-вимірювальну апаратуру з відповідним метрологічним забезпеченням;

- висококваліфікований персонал;

- спеціальні методики проведення вимірювань і математичний апарат розрахунку результатів.

Контроль може бути здійснений як інструментальним способом, що полягає у фізичній перевірці неможливості перехоплення ПЕМВН за межами контрольованої зони, так і розрахунково-інструментальний.

В обох випадках тестовий режим повинен задаватися шляхом формування в перевіреній апаратурі сигналу, з одного боку, легко ідентифікованого при прийомі, а з іншого – переводити апаратуру в стан, при якому рівень створюваних нею побічних випромінювань максимальний.

Найбільш просто контроль ЕОТ від витоку через ПЕМВН здійснюється інструментальним способом. При цьому виконується наступна послідовність операцій:

1. Апаратура контролю встановлюється в місцях можливого розташування технічних засобів розвідки.

2. Відключається система автоматичного регулювання підсилення.

3. Виставляється необхідне значення смуги пропускання приймального пристрою ($\Delta f = 6$ кГц – при контролі випромінювань телефонних мереж; $\Delta f = 15,6M$ кГц, де M – число «білих» смуг; $\Delta f = 1/\tau_i$ при контролі випромінювань засобів ЕОТ, де τ_i – тривалість імпульсу в пачці тестового сигналу).

4. Включається тестовий сигнал на апаратурі.

5. Здійснюється пошук випромінювання, модульованого тестовим сигналом, в діапазоні частот від 0,01 до 1000 МГц.

6. При його виявленні приймається рішення про необхідність проведення додаткових заходів щодо захисту інформації.

Недоліком розглянутого способу є відносно високі вимоги до порогової чутливості приймальних пристроїв U_0 (не менше 1 мкВ) і наявності спеціальних комбінованих магнітних і електричних антен [20].

Якщо ці вимоги не виконуються або відсутня можливість проведення досліджень на межі контрольованої зони, можна скористатися розрахунково-вимірювальним способом, який полягає в наступному:

1. Апаратура контролю встановлюється на деякій відстані $R \geq 1$ м від пристрою, що перевіряється.

2. Включається тестовий сигнал.

3. Здійснюється пошук тестового сигналу аналогічно тому, як це робилося у наведеній вище методиці.

4. При виявленні сигналу проводиться вимір його рівня в присутності шумів $U_{с+ш}$ на вході приймача за допомогою вимірювальної радіоконтрольної апаратури.

5. Для всіх частот, на яких були виявлені зміни сигналу, результати вимірювань значення $U_{с+ш}$ заносяться до табл. 3.1.

Таблиця 3.1 – Результати вимірювань

№	Частота сигналу $f_с$, МГц	Рівень сигналу при наявності шумів $U_{с+ш}$, мкВ	Рівень шуму $U_ш$, мкВ	Рівень сигналу $U_с$, мкВ

6. Відключається апаратура контролю, і на всіх частотах, на яких був виявлений тестовий сигнал, вимірюються рівні шумів $U_ш$, їх значення заносяться до табл. 3.1.

Якщо чутливість приймача нижче 10 мкВ, то для визначення рівня $U_с$ доцільно скористатися аналітичним способом, відповідно до якого $U_ш = E_ш h_д$, де $h_д$ – діюча висота антени, а $E_ш$ – шумова напруженість електричного поля. Орієнтовні значення $E_ш$ для великого промислового міста приведені в табл. 3.2 [20].

Таблиця 3.2 – Орієнтовні значення $E_ш$

f, МГц	0,1 - 1	1 - 10	10 - 100	100 - 1000
$E_ш$, мкВ/м	1 - 500	0,8 - 100	0,1 - 10	0,1 - 1

7. За формулою:

$$U_c = \sqrt{U_{с+ш}^2 + U_ш^2}$$

розраховуються значення рівня сигналу $U_с$ на вході приймача контролю, які також заносяться в табл. 3.1.

8. Розрахункова дальність R, на якій можливе перехоплення ПЕМВН, знаходиться зі співвідношення $R=R_к U_с/U_ш$.

9. Якщо розрахункова величина R більше, ніж радіус контрольованої зони $R_{кз}$, необхідно врахувати послаблення напруженості електромагнітного поля штучними або природними перешкодами.

З урахуванням послаблення електромагнітних хвиль можлива дальність перехоплення ПЕМВН буде визначатися значенням $R_0 = R_к/KU_с/U_ш$, де K – послаблення перешкоди або середовища поширення на частоті сигналу.

10. У разі, коли величина R_0 перевищує радіус контрольованої зони $R_{кз}$, необхідно вжити додаткових заходів із захисту інформації від перехоплення.

Слід зазначити, що у випадках: доробки пристроїв ЕОТ, електромагнітного екранування приміщень та активного енергетичного маскування – показником захищеності є співвідношення сигнал/шум, що забезпечується на межі мінімально допустимої зони безпеки. Максимально допустиме співвідношення сигнал/шум розраховується в кожному конкретному випадку за спеціальними методиками. При активному радіотехнічному маскуванні з використанням статистичного методу як показника, що характеризує захищеність, застосовується матриця ймовірностей переходів. У разі ідеальної захищеності ця матриця буде відповідати матриці ймовірностей переходів шумового сигналу, всі елементи якої рівні між собою.

4 ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПЕМВН ВІД ЗАСОБІВ ЕОТ

4.1 Методика оцінки ПЕМВН

1. Мета досліджень – оцінка і підтвердження неможливості витоку небезпечних сигналів за рахунок ПЕМВН від основних технічних засобів і систем ЕОТ [6], встановлених у виділеному приміщенні.

2. Склад досліджуваних пристроїв наведено в табл. 4.1.

Таблиця 4.1 – Склад досліджуваних пристроїв

№	Назва	Тип, модель	Серійний номер
1	АРМ-1		
1.1	Системний блок AST BRAVO	LC 5100	-
1.2	Монітор LG	22MK-600M-W	-
1.3	Клавіатура	SK-2000-RIV	-
1.4	Маніпулятор типу «Миша» Microsoft	2.1 A	-
1.5	Принтер HP LJ5L	C3941A	-
2	Засоби захисту		
2.1	Генератор	«ГШ-1000М»	678
2.2	Генератор	«Соната-РК1»	2386
2.3	Фільтр протизавадний	«ФСП-7»	0014859

3. Методично-нормативне забезпечення та контрольно-вимірювальна апаратура при проведенні спеціальних досліджень.

3.1. Значення небезпечних сигналів вимірювалися і розраховувалися, в першу чергу, від пристроїв з послідовним кодуванням інформації (монітор, накопичувачі на жорсткому та оптичних (CD-R, CD-RW) дисках, принтер, клавіатура). Прилади (вузли, блоки пристроїв) з паралельним кодуванням і розрядністю не оцінювалися.

3.2 Значення співвідношень сигнал/шум (при оцінці ефективності систем активного захисту) вимірювалися і розраховувалися ПЕМВН для пристроїв з послідовним кодуванням інформації (монітор, накопичувачі на жорсткому та оптичних дисках, принтер, клавіатура, інтерфейс E-SATA тощо).

3.3. Досліджувані пристрої комп’ютерної техніки включалися в режимі обробки спеціального тест-сигналу із заздалегідь відомими параметрами переданих даних (тест-програма «Сігурд-тест»). Основні параметри небезпечного сигналу в колах пристроїв виявлялися безпосередніми вимірами в досліджуваних ланцюгах. При дослідженнях відеопідсистеми тактова частота визначалася непрямим методом за кроками частоти гармонік відеосигналу, а тривалість імпульсів так як в режимі вимірювання формувався відеосигнал із співвідношенням тривалості імпульсів і пауз типу «меандр».

3.4. Вимірювання ПЕМВН монітора проводилися при виведенні на екран послідовності чорних і білих елементів зображення (пікселів) в режимі «піксель через піксель».

З метою більш ретельного дослідження частотного діапазону в мегагерцах ПЕМВН від 0 до $1/\tau$ виконані окремі спеціальні дослідження відеопідсистеми в цьому діапазоні частот в тест-режимі «піксель через 7 пікселів», що імітує виведення тексту на монітор.

3.5. Вимірювання ПЕМВН лазерного принтера проводилися в режимі друку чергуванням чорних і білих вертикальних ліній (2 пікселя через 10).

3.6. Оцінка реального загасання проводилася в частотних смугах $1/\tau$. У кожній смузі підсумовувалась оцінка реального загасання мінімум в 5 ... 8 частотних точках, рівномірно розподілених по частоті.

3.7. Дослідження проводилися за електричною та магнітною компонентами електромагнітного поля в усьому встановленому діапазоні частот з поглибленим дослідженням тактових частот небезпечного сигналу.

3.8. Дослідження в мережі електроживлення проводилися в безпосередній близькості від розетки 220 В / 50 Гц, в яку були включені пристрої комп’ютера. Точка розміщення струмового трансформатора на кабелі електроживлення вибиралася за максимумом небезпечного сигналу. Так як система електроживлення не розв’язана гальванічно від зовнішніх споживачів, додатково інструментально оцінювалася ефективність системи пасивного захисту.

3.9. Просторова система зашумлення побудована на базі генератора «ГШ-1000М». Оцінка ефективності захисту (генератор лінійного зашумлення «Соната-РК1») в лініях електроживлення проводилася до частот не вище 300 МГц на підставі того, що потенційна можливість здійснення перехоплення в лінії електроживлення існує в 80 м від об’єкта ЕОТ. Опис та характеристики засобів захисту наведені у дод. Б.

3.10. Пошук сигналів ПЕМВН і можливих паразитних генераторів проводився в діапазоні частот 0,01 ... 1800 МГц.

4. При проведенні спеціальних досліджень використана наступна контрольно-вимірювальна апаратура.

Система «Сігурд» (рис. 4.1):

- аналізатор спектру IFR 2398, зав. № 91200406;

- антена вимірювальна дипольна AI5-0, зав. № 078;

- струмовий трансформатор Rohde & Schwarz 25-300 МГц, зав. № 125/91;

- програмне забезпечення «Сігурд-Інтерфейс», «Сігурд-Тест» та «Сігурд-Дельта».

Рисунок 4.1 – Зовнішній вигляд системи «Сігурд»

5. Аналіз побудови системи електроживлення та заземлення ЕОТ.

5.1. Трансформаторна підстанція розташована в межах контрольованої зони. До неї підключені 2 міських вводи по 10 кВ кожен. Від головного розподільного щита, розташованого в приміщенні «щитової», відходять 4 фідера по 0,4 кВ, до одного з яких підключені зовнішні споживачі, розташовані в навколишньому житловому масиві міста.

5.2. Проведений аналіз показав, що з точки зору можливості витоку інформації з приміщень мережу електроживлення слід розглядати як таку, що має вихід за межі контрольованої зони об’єкта.

5.3. Результати вимірювань та розрахунків наведені у таблицях нижче, а графіки представлені у дод. Г.

5.4. НС від накопичувача на жорсткому диску і від накопичувача на CD-диску не виявлено в ланцюгах живлення та по ефіру до рівня власних шумів тракту вимірювання при смузі пропускання до 1000 Гц. Небезпечний сигнал від відеосистеми, який є визначальним для значень $R2$, $R1$ для всього комплексу технічних засобів. Від клавіатури виявлені сигнали з рівнями на частотах 0,1 ... 8,5 МГц.

5.5. Від лазерного принтера на частотах, кратних тактовій частоті сигналу в лазерному діоді, не виявлені небезпечні сигнали на рівні шумів у смузі пропускання до 300 Гц.

5.6. Небезпечні сигнали від монітору за магнітною компонентою поля за величиною значно менші за електричні компоненти, у зв’язку з чим дані за цими вимірами не наводяться. У табл. 4.4 частоти гармонік небезпечного сигналу згруповані за частотними смугами (тривалість відеоімпульсу при виведенні на екран тесту дорівнювала 15,4 нс, випробувальний відеорежим 800x600 пікселів, 16 біт кольору, частота кадрів 85 Гц). Заміряні значення небезпечного сигналу на відстані d і висоті розміщення h і значення $K_{\text{а}}$ ($K_{\text{підсил}}$) з таблиці калібрування антени (підсилювача) підсумовуються ($U_{\text{сп}}$) і обчислюється нормоване, наведене значення сигналу в смузі $\Sigma E_{\text{с}}$ з урахуванням значень δ для конкретної категорії ЕОТ. Для кожної смуги підсумовування

визначається радіус зони R2 ($R_{\text{пелюстки}}$). Максимальне зі значень *R2* є мінімально необхідним значенням радіусу контрольованої зони для ЕОТ (за умовами 2-й і 3-ї категорій). Для умов 1-ї категорії проводиться розрахунок еквівалентного значення радіуса зони. Ці значення наведені в таблиці для умов категорій об'єкта 1,2,3 (значення є для даного об'єкта довідковими, так як захист визначається засобами активного захисту).

5.7. Оцінка ефективності систем активного захисту для ланцюгів електроживлення і в ефірі (монітор) проводилася шляхом вимірювання спектральної щільності електромагнітного шуму в діапазоні існування ПЕМВН в частотних смугах 50 МГц з подальшим розрахунком значення співвідношення сигнал/шум в цих смугах. За умови, що розраховані значення не перевищують X, X для умов 2-й і 3-ї категорій і 0,00XXX для умов 1-ї категорії. В табл. 6.12 наведені розрахункові дані співвідношень сигнал/шум по смугах підсумовування небезпечного сигналу при роботі систем захисту. Дані інструментального контролю ефективності систем захисту в мережі електроживлення наведено в табл. 6.13 - 6.15.

5.8. Паразитної генерації у вузлах досліджених пристроїв не виявлено.

5.9. Вимірювальні антени розміщувалися відповідно до методичних вказівок. При вимірюванні небезпечних сигналів від монітора антена розміщувалася в точці найбільшого рівня небезпечного сигналу – позаду системного блоку з монітором. Поляризація антени – вертикальна.

4.2 Результати спеціальних досліджень

6. Результати вимірів та розрахунків. Дані вимірювань і розрахунків мінімально необхідного радіусу зони *R*2 наведені в табл. 6.2 - 6.8, оцінки ефективності просторової системи зашумлення в табл. 6.9 - 6.12 і лінійної системи зашумлення в табл. 6.13 - 6.15.

6.1. Результати спеціальних досліджень (монітор в ефірі, розрахунок *R*2).

Розміщення об'єкта та вимірювальної антени наведено на рис. 4.2

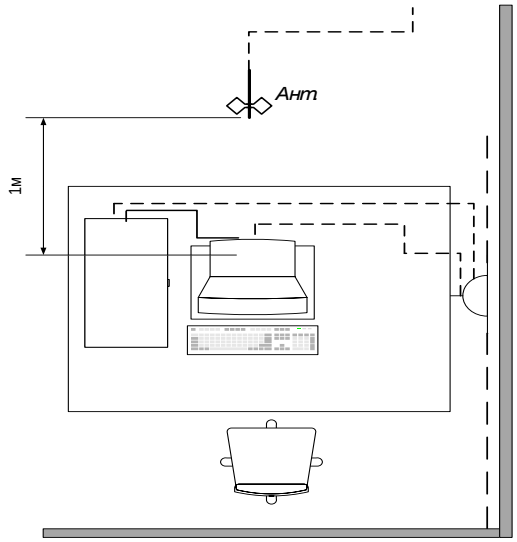


Рисунок 4.2 – Розміщення антени при вимірюваннях

Якщо небезпечний сигнал не виявлено на рівні шумів у вимірювальному тракті, то виконується оцінювальний розрахунок за шумами.

Таблиця 4.2 – Параметри небезпечного сигналу

τ =	$15{,}4\times10^{-9}$ с
d =	1,0 м
δ =	0,1
Kd/h =	0,5
Kc =	1,41
Ft =	24699 кГц
h =	1,0 м

Таблиця 4.3 – Результати вимірювання небезпечного сигналу від монітору

№	F, МГц	U, дБ/мкВ	$U_{шуму}$, дБ/мкВ	RBW, кГц	$K_{ант}$, дБ/мкВ	$K_{підсил}$, дБ/мкВ	$E_{сиг}$, мкВ/м
1	32,458262	37,956	27,267	10	12,863	30,736	44,884741
2	129,785471	33,667	30,933	30	25,839	27,071	40,600649
3	129,832000	36,089	24,578	10	25,840	27,069	55,121009
4	129,881928	34,000	24,956	10	25,841	27,067	43,221748
5	194,702098	28,956	22,756	10	26,834	24,847	34,776231
6	194,750129	33933	20,067	10	26,835	24,846	62,531188
7	194,798554	33,644	20,156	10	26,835	24,844	60,498599
8	227,160178	29,222	19,778	10	27,622	23,789	44,667779
9	227,208209	35,800	21,244	10	27,624	23,788	95,893610
10	227,208209	35,778	21,556	10	27,625	23,786	95,681136
11	259,715107	32,533	21,000	10	28,382	22,831	79,888329

Таблиця 4.4 – Групування результатів в частотні проміжки (пелюстки) $1/\tau$

№	Номер пелюстки	$F_{\text{ц пелюстки}}$, МГц	Номер сигналу в пелюстці	$E_{\text{сиг. пелюстки}}$, мкВ
1	1	32,467532	1	44,884741
2	2	97,402597	2,3	68,459757
3	3	162,337662	4, 5, 6, 7	103,187866
4	4	227,272727	8, 9, 10, 11	163,486452

Таблиця 4.5 – Розрахунок небезпечної зони для об’єктів 1-ї категорії

№	$G_{\text{сиг. пелюстки}}$, мкВ/м	$R_{\text{пелюстки}}$, м	$R_{\text{пелюстки окр}}$, м
1	43,075552	100,879	105
2	65,700318	254,527	255
3	99,028626	393,868	395
4	156,896729	611,657	615

Таблиця 4.6 – Розрахунок небезпечної зони для об’єктів 2-ї категорії

№	$G_{\text{сиг. пелюстки}}$, мкВ/м	γ	$R_{\text{пелюстки}}$, м	$R_{\text{пелюстки окр}}$, м
1	0,112428	0,035739	5,000	5
2	0,262212	0,054649	5,000	5
3	0,616775	0,085283	5,000	5
4	1,206811	0,105323	5,093	10

Таблиця 4.7 – Розрахунок небезпечної зони для об’єктів 3-ї та категорії

№	$G_{\text{сиг. пелюстки}}$, мкВ/м	γ	$R_{\text{пелюстки}}$, м	$R_{\text{пелюстки окр}}$, м
1	0,112428	0,035739	5,000	5
2	0,262212	0,054649	5,000	5
3	0,616775	0,085283	5,000	5
4	1,206811	0,105323	5,093	10

Таблиця 4.8 – Кінцеві результати

Категорія	$R2$, м	$R1$, м	$R1'$, м
1	615	21,291	7,844
2,3	10	5,175	1,907

6.2. Результати спеціальних досліджень (оцінка ефективності систем захисту.

Розміщення вимірювальної антени та антени показані на рис. 4.3.

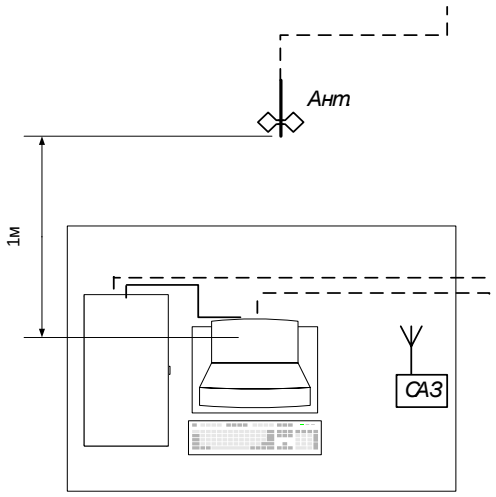


Рисунок 4.3 – Розміщення вимірювальної антени та антени систем активного захисту

Таблиця 4.9 – Параметри небезпечного сигналу

τ =	$15{,}4 \cdot 10^{-9}$ с
d =	1,0 м
δ =	0,1
Kd/h =	0,5
Kc =	1,41
Ft =	24699 кГц
h =	1,0 м

Таблиця 4.10 – Рівні створюваної завади при функціонуванні систем захисту

№ п/п	$F_{саз}$, МГц	$U_{саз}$ дБ/мкВ	$RBW_{саз}$, кГц	$K_{ант}$, дБ/мкВ	$K_{підсил}$, дБ/мкВ	$E_{саз}$, мкВ
1	32,467533	39,567	100	25,863	30,736	18,096
2	97,402597	41,853	100	25,209	28,576	28,000
3	162,337662	48,597	100	26,388	25,844	95,489
4	227,272727	52,123	100	27,625	23,786	209,411
5	292,207792	52,742	100	29,051	21,988	325,914
6	357,142857	47,430	100	29,051	20,406	221,920
7	422,077922	51,604	100	29,442	18,994	423,985
8	487,012987	51,640	100	29,480	17,648	479,119
9	551,948052	42,293	100	25,468	16,641	119,91
10	616,883117	32,849	100	23,552	15,748	35,937
11	681,818182	34,046	100	27,707	14,839	73,892
12	746,753247	32,019	100	29,187	14,067	75,827

Таблиця 4.11 – Рівні небезпечного сигналу від ЕОТ

№ п/п	F, МГц	U, дБ/мкВ	$U_{шума}$, дБ,мкВ	RBW, кГц	$K_{ант}$, дБ/мкВ	$K_{підсил}$, дБ/мкВ	$E_{сиг}$, мкВ
1	32,458	37,956	27,267	10	25,863	30,736	44,885
2	129,785	33,667	30,933	30	25,839	27,071	40,601
3	129,832	36,089	24,578	10	25,840	27,069	55,121
4	129,882	34,000	24,956	10	25,841	27,067	43,222
5	194,702	28,956	22,756	10	26,834	24,847	34,776
6	194,750	33,933	20,067	10	26,835	24,846	62,531
7	194,798	33,644	20,156	10	26,835	24,844	60,499
8	227,160	29,222	19,778	10	27,622	23,789	44,668
9	227,208	35,800	21,244	10	27,624	23,788	95,894
10	227,256	35,778	21,556	10	27,625	23,786	95,681
11	259,715	32,533	21,000	10	28,382	22,831	79,888

Таблиця 4.12 – Групування результатів в частотні проміжки (пелюстки) $1/\tau$

Номер пелюстки	$F_{ц\ пелюстки}$, МГц	Номер сигналу в пелюстці	Номер САЗ в пелюстці	Δ
1	32,467	1	1	0,09735
2	97,402	2, 3	2	0,095961
3	162,337	4, 5, 6, 7	3	0,042457
4	227,272	8, 9, 10, 11	4	0,030461

Система активного захисту в ефірі неефективна для об’єктів 1-ї категорії ($\Delta > \delta$ = 0,00XX) і ефективна для 2-ї, 3-ї, 4-ї категорій ($\Delta < \delta$ = X,X).

6.3. Результати спеціальних досліджень в ланцюгах електроживлення. Небезпечний сигнал вимірювався струмовим трансформатором в 1,5 м від ЕОТ у мережевій вилці (рис. 4.4).

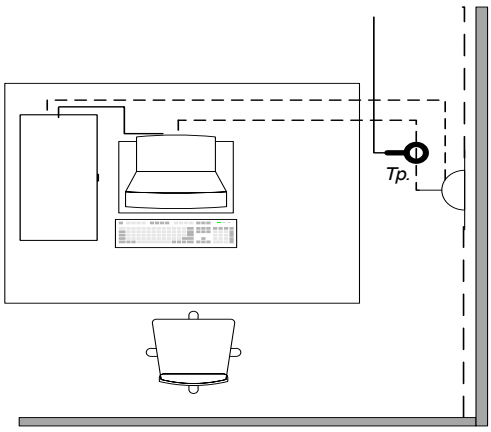


Рисунок 4.4 – Розміщення струмового трансформатора в лінії електроживлення

Таблиця 4.13 – Результати вимірювань в ланцюгах електроживлення при функціонуванні систем захисту

№ п/п	$F_{саз}$, МГц	$U_{саз}$, дБ/мкВ	$RBW_{саз}$, кГц	$K_{ант}$, дБ/мкВ	$K_{підсил}$, дБ/мкВ	$E_{саз}$, мкВ
24	32,468	93,198	100,000	-19,100	30,736	49,091
25	97,403	73,205	100,000	-18,619	28,576	6,659
26	162,338	66,816	100,000	-18,108	25,844	4,636
27	227,273	64,112	100,000	-17,886	23,786	4,414
28	292,208	58,089	100,000	-18,186	21,988	2,622
29	357,143	54,644	100,000	-18,583	20,406	2,021

Таблиця 4.14 – Рівні інформаційного сигналу в мережі електроживлення

№ п/п	F, МГц	U, дБ/мкВ	$U_{шуму}$, дБ,мкВ	RBW, кГц	$K_{ант}$, дБ/мкВ	$K_{підсил}$, дБ/мкВ	$E_{сиг}$, мкВ
12	32,410	45,644	41,000	10	-19,100	30,737	0,605
13	32,459	62,844	37,489	10	-19,100	30,736	4,471
14	32,507	48,644	38,533	10	-19,100	30,735	0,867
15	97,375	41,378	20,000	10	-18,619	28,577	0,512
16	129,834	50,400	22,289	10	-18,407	27,069	1,763
17	129,882	45,889	29,689	10	-18,407	27,067	1,049
18	162,293	47,311	28,178	10	-18,108	25,845	1,471
19	162,340	45,444	21,511	10	-18,108	25,842	1,187
20	162,389	38,111	20,778	10	-18,107	24,846	0,510
21	194,753	46,222	22,822	10	-17,665	23,788	1,533
22	227,209	29,822	19,156	10	-17,886	23,786	0,254
23	227,257	29,444	19,400	10	-17,886	22,831	0,243
24	259,715	36,622	19,156	10	-18,121	21,990	0,607
25	292,126	28,578	20,467	10	-18,185	21,989	0,261
26	292,174	31,800	20,978	10	-18,186	21,170	0,380
27	234,584	30,489	29,356	10	-18,373	21,170	0,337

Таблиця 4.15 – Групування результатів в частотні проміжки (пелюстки) $1/\tau$

Номер пелюстки	$F_{ц\ пелюстки}$, МГц	Номер сигналу в пелюстці	Номер САЗ в пелюстці	Δ
1	32,468	1, 2, 3	1	0,003673
2	97,403	4, 5	2	0,010820
3	162,338	6, 7, 8, 9, 10	3	0,022857
4	227,273	11, 12, 13	4	0,006242
5	292,208	14, 15, 16	5	0,008544

Система захисту в ланцюзі електроживлення неефективна для об’єктів 1-ї категорії ($\Delta > \delta = 0{,}00XX$) і ефективна для 2-ї і 3-ї категорій ($\Delta < \delta = X{,}X$).

Примітка. Заливкою сірим кольором у наведених вище таблицях виділена смуга підсумовування, в якій отримано найбільші значення Δ.

У таблицях результатів розрахунків прийнято такі позначення:

При розрахунку значень *R*2:

F – частота поточного небезпечного сигналу;

U – рівень небезпечного сигналу;

$U_{\text{шуму}}$ – рівень завади на частоті небезпечного сигналу при зупиненому тесті;

$K_{\text{ант}}$ – антенний коефіцієнт (будь-якого антенно-фідерного пристрою, який включає в себе фідер, струмовий трансформатор і т.д.);

$K_{\text{підсил}}$ – коефіцієнт підсилення антенного підсилювача;

$E_{\text{сиг}}$ – значення небезпечного сигналу (з врахуванням завади) в одиницях напруженості поля;

Номер пелюстки – порядковий номер смуги підсумовування небезпечних сигналів;

$F_{\text{ц пелюстки}}$ – центральна частота *i*-ї пелюстки;

Номер сигналу в пелюстці – порядкові номери небезпечних сигналів, які входять в *i*-й пелюсток (смугу підсумовування);

$E_{\text{сиг. пелюстки}}$ – еквівалентне значення небезпечного сигналу в *i*-й пелюстці після підсумовування;

$G_{\text{сиг. пелюстки}}$ – нормоване значення спектральної щільності небезпечного сигналу в *i*-й пелюстці;

γ – значення коефіцієнта для центральної частоти *i*-ї пелюстки;

$R_{\text{пелюстки}}$ – точне розрахункове значення радіусу зони *R*2 для *i*-ї пелюстки;

$R_{\text{пелюстки окр}}$ – округлене (з точністю до 5 м) значення радіусу зони *R*2 для *i*-ї пелюстки.

При розрахунку значень *R*2 в першій пелюстці:

$F_{\text{ц октави}}$ – центральна частота *i*-ї октави;

Номер сигналу – порядкові номери небезпечних сигналів, які входять в *i*-ту октаву (смугу підсумовування);

$E_{\text{сиг. октави}}$ – еквівалентне значення небезпечного сигналу в *i*-й октаві після підсумовування;

$G_{\text{сиг. октави}}$ – нормоване значення спектральної щільності небезпечного сигналу в *i*-й октаві;

γ – значення коефіцієнта для центральної частоти *i*-ї октави;

$R_{\text{октави}}$ – точне розрахункове значення радіусу зони *R*2 для *i*-ї октави;

$R_{\text{октави окр}}$ – округлене (з точністю до 5 м) значення радіусу зони *R*2 для *i*-ї октави;

$R_{(1)}$, $R_{(2)}$ – поточні значення радіусу зон *R*1 і *R*2 в процесі об'єднання;

α, β – допоміжні коефіцієнти об'єднання окремих значень *R*;

$R_{\text{еквів}}$ – еквівалентне значення радіусу зони *R*2 для першої пелюстки.

При розрахунку ефективності систем захисту:

F – частота поточного небезпечного сигналу;

U – рівень небезпечного сигналу;

$U_{\text{шуму}}$ – рівень завади на частоті небезпечного сигналу при зупиненому тесті;

$K_{\text{ант}}$ – антенний коефіцієнт (будь-якого антенно-фідерного пристрою, який включає в себе фідер, струмовий трансформатор і т.д.);

$K_{\text{підсил}}$ – коефіцієнт підсилення антенного підсилювача;

$E_{\text{сиг}}$ – значення небезпечного сигналу (з врахуванням завади) в одиницях напруженості поля;

Номер пелюстки – порядковий номер пелюстки (смуги підсумовування небезпечних сигналів);

$F_{\text{ц пелюстки}}$ – центральна частота *i*-ї пелюстки;

Номер сигналу – порядкові номери небезпечних сигналів, які входять в *i*-й пелюсток (смугу підсумовування);

$E_{\text{сиг. пелюстки}}$ – еквівалентне значення небезпечного сигналу в *i*-й пелюстці після підсумовування;

$F_{\text{САЗ}}$ – частота відповідного шуму систем активного захисту;

$U_{\text{САЗ}}$ – рівень напруги систем активного захисту;

$E_{\text{САЗ}}$ – значення в одиницях напруженості поля рівнів, що створює система активного захисту;

$RBW_{\text{САЗ}}$ – смуга частот приймача при вимірюваннях з системами активного захисту;

RBW – смуга частот приймача при вимірюваннях небезпечного сигналу.

На підставі вищенаведених результатів досліджень, допускається експлуатувати на об’єктах інформатизації відповідних категорій ЕОМ та засоби ЕОТ, за наявності необхідного мінімального радіусу контрольованої зони $R2$, радіусів $R1$ і $R1'$ не менших, ніж наведені в таблицях.

При штатно працюючій системі активного зашумлення вимоги до розмірів зони $R2$ і відстаням $R1$ і $R1'$ не пред’являються. Системи електроживлення та заземлення захищені генератором «Соната-РК1» та фільтром «ФСП-7», а радіоефір в зоні $R2$ – генератором шуму «ГШ-1000М». За умови штатної роботи систем захисту системи електроживлення та заземлення об’єкта є захищеними за умовами 2-й, 3-ї і 4-ї категорій.

В ході проведених спеціальних досліджень ефективності системи захисту на об’єкті інформаційної діяльності за рахунок ПЕМВН обґрунтовано доцільність використання запропонованих ТЗІ.

ВИСНОВКИ

За результатами атестаційної роботи можна зробити наступні висновки:

1. Розглянуто причини утворення технічних каналів витоку через ПЕВМН.

2. Сформовані основні вимоги до системи захисту інформації персонального комп’ютера, на якому оброблюється інформація з обмеженим доступом.

3. Досліджено небезпечний канал витоку інформації, що утворюється за рахунок ПЕМВН, його особливості та фізичну природу виникнення електромагнітних радіовипромінювань від засобів електронно-обчислювальної техніки.

4. Розглянуто основні методики оцінки захищеності інформації від витоку каналами побічних електромагнітних випромінювань та наведень, а також проведені спеціальні вимірювання небезпечних рівнів випромінювань від інтерфейсних ліній персонального комп’ютера.

5. Проведено розрахунок основних критеріїв захищеності інформації, що обробляється засобом електронно-обчислювальної техніки (персональним комп’ютером) і дана оцінка ефективності застосованих засобів захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень.

6. Запропоновані активні і пасивні засоби захисту інформації від витоку каналами ПЕМВН та проведена їх ефективна оцінка.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. НД ТЗІ ТР ЕОТ – 95. «Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок». – Київ, 1995. – 10 с.

2. Галкин А.П. Защита технических каналов связи предприятий и учреждений от несанкционированного доступа к информации: учеб. пособ. / А.П. Галкин, В.С. Эмдин. – СПб.: [Б.И.], 2003. – 100 с.

3. Хорев А.А. Способы и средства защиты информации / А.А. Хорев. – М.: МО РФ, 1996. – 266 с.

4. Хорошко В.А. Методы и средства защиты информации / А.А. Хорошко, А.А. Чекатов. – К.: ПолиграфКонсалтинг, 2003. – 482 с.

5. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». – Київ, 1999. – 35 с.

6. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт зі створення комплексної системи захисту в інформаційно-телекомунікаційній системі». – Київ, 2005. – 22 с.

7. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А.А. Хорев. – М.: Гостехкомиссия РФ, 1998. – 320 с.

8. Маркин А.В. Безопасность излучений и наводок от средств ЭВТ / А.В. Маркин // Зарубежная радиоэлектроника. – 1989. – № 12. – С.102-109.

9. Вартанесян В.А. Радиоэлектронная разведка / В.А. Вартанесян. – М.: Воениздат, 1991. – 270 с.

10. Андрианов В.И. «Шпионские штучки» и устройства для защиты объектов и информации: справ. пособ. / В.И. Андрианов, В.А. Бородин, А.В. Соколов. – СПб: Лань, 1997. – 215 с.

11. Сапожков М.А. Защита трактов радио и проводной связи от помех и шумов / М.А. Сапожков. – М.: Связьиздат, 1959. – 125 с.

12. Галкин А.П. Устранение несанкционированного использования диктофона / А.П. Галкин // Материалы 3-й Международной НТК «Перспективные технологии в средствах передачи информации». – Владимир (РФ): 1999. – С.61-64.

13. Бузов Г.А. Защита от утечки информации по техническим каналам: учеб. пособ. / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Полиграф, 2005. – 416 с.

14. Овсянников В.В. Нужны ли нам защищенные компьютеры? / В.В. Овсянников, Г.Т. Солдатенко // Техника специального назначения. – 2005. – №1. – С.9-11.

15. Вим Ван Эйк. Электромагнитное излучение видеодисплейных модулей: риск перехвата информации / Вим Ван Эйк // Защита информации. Конфидент-Информ. – 2001. – №1. – С.90-93.

16. Wei Chien. Reserch on Anti-Radiation Noise Interference of High Definition Multimedia Interface Circuit Layout of a Laptop / Wei Chien, Yu-Ting Cheng, Chiuan-Fu Hsiao, Kai-Xu Han, Chien-Ching Chiu // Electronics. – 2020. – No 9. – P.2-14.

17. Пепа Ю.В. IP-моніторинг систем перехоплення інформації / Ю.В. Пепа // Тези сьомої НПК «Інформатика, управління та штучний інтелект». – Харків (Україна): 2020. – С.58.

18. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ООО "ТИД ДС", 2002. – 688 с.

19. Стельмашонок. Е.В. Защита информации в компьютерных системах / Е.В. Стельмашонок, И.Н. Васильева. – СПб: СПбГЭУ, 2017. – 163 с.

20. Mario Sajko. Measuring and Evaluating the Effectiveness of Information Security / Mario Sajko // Risk Assessment and Management. – 2014. – No 7. – P.402-411.