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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Білічука Романа Анатолійовича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування засобів зменшення рівня побічних електромагнітних випромінювань при використанні флеш-накопичувача*

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

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Білічуку Роману Анатолійовичу*** **академічної групи** ***125м-22-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

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

на тему ***Обґрунтування засобів зменшення рівня побічних електромагнітних випромінювань при використанні флеш-накопичувача***

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

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.11.2023
Розділ 2	Спеціальна частина	16.11.2023
Розділ 3	Економічна частина	30.11.2023

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Білічук Р.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 104 сторінки, 45 рисунків, 4 таблиці, 4 додатки, 13 посилань.

Мета кваліфікаційної роботи – зменшення рівнів інформативного побічного електромагнітного випромінювання при роботі з флеш-накопичувачами.

Об'єкт дослідження – побічні електромагнітні випромінювання, що виникають при роботі з флеш-накопичувачами.

У спеціальній частині проведений аналіз структури, принципів роботи флеш-накопичувачів і USB-інтерфейсу, сигналів, що надходять з USB-інтерфейсу на флеш-накопичувач і дослідження рівня ПЕМВ. Розроблено порядок проведення досліджень з виявлення та вимірювання рівнів інформативних складових ПЕМВ сигналів. На основі отриманих результатів експериментальних досліджень розроблено рекомендації щодо зменшення рівня побічних електромагнітних випромінювань від флеш-накопичувачів.

В економічному розділі виконано розрахунок витрат на впровадження засобів та заходів інформаційної безпеки на підприємстві.

Наукова новизна роботи полягає у виявленні чинників, що впливають на рівень побічних електромагнітних випромінювань при роботі з флеш-накопичувачами, та розробці рекомендацій щодо зниження рівнів ПЕМВ.

ПОБІЧНЕ ЕЛЕКТРОМАГНІТНЕ ВИПРОМІНЮВАННЯ, ІНФОРМАТИВНИЙ СИГНАЛ, СПЕЦІАЛЬНІ ДОСЛІДЖЕННЯ, ФЛЕШ-НАКОПИЧУВАЧ, АВТОМАТИЗОВАНИЙ ПОШУКОВИЙ КОМПЛЕКС

ABSTRACT

The explanatory note of qualification work consists of: 104 pages, 45 figures, 4 tables, 4 appendices, 13 references.

The purpose of the qualification work is to reduce the level of side electromagnetic radiation when using the flash-drives.

The object of the study is side electromagnetic radiation, which occurs when using the flash-drives.

The special part analyzes structure, the principle of flash storage and USB interface, information-bearing signals going from the USB interface to the flash-drive and the specific research of the SER level. The procedure of the investigation in detecting and testing the levels of tempest information-bearing signals is developed. On the basis of experimental results, the recommendations for reducing the side electromagnetic radiation from flash-drives are made.

In the economic section, the calculation of the cost for implementation of information security at an enterprise is executed.

The scientific novelty of this work lies in identifying the factors that affect the level of side electromagnetic radiation when working with flash-drives, and developing the recommendations for reducing the SER levels.

SIDE ELECTROMAGNETIC RADIATION, INFORMATIVE SIGNAL, SPECIFIC RESEARCH, FLASH-DRIVES, AUTOMATED SEARCH COMPLEX

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПЕМВ - побічні електромагнітні випромінювання;

ТЗ - технічний засіб;

ЕМС - електромагнітна сумісність;

ЗОТ - засіб обчислювальної техніки;

АК - автоматизований комплекс;

ОІД - об'єкт інформаційної діяльності;

ПЗ - програмне забезпечення;

ДТЗС - допоміжні технічні засоби і системи;

КЗ - контрольована зона;

ЗОІ - засоби обробки інформації;

ЕМВ - електромагнітне випромінювання;

ВА - випадкова антена;

ЗВА - зосереджена випадкова антена;

РВА - розподілена випадкова антена;

АС - автоматизована система;

ПЕОМ - персональна електронно-обчислювальна машина

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 9
1.1 Технічні канали витоку інформативних сигналів, що виникають при роботі обчислювальної техніки за рахунок ПЕМВ 9
1.2 Умови існування каналу витоку інформації 13
1.3 Визначення критеріїв захищеності ЗОТ 24
1.4 Характеристики та параметри інформативних сигналів, що підлягають вимірюванню 25
1.5 Принцип побудови флеш-накопичувачів 28
1.6 Висновки. Постановка задачі 34
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 36
2.1 Аналіз фізичного рівня USB 36
2.2 Аналіз сигналів, що надходять через USB-інтерфейс на флеш-накопичувач 40
2.3 Обґрунтування вибору апаратури для проведення експериментальних досліджень 46
2.4 Аналіз параметрів сигналів, що підлягають вимірюванню 54
2.5 Обґрунтування вибору методу виявлення інформативних складових ПЕМВ 57
2.6 Розробка порядку проведення спеціальних досліджень USB флеш-накопичувачів 59
2.7 Дослідження сигналів, що надходять з USB інтерфейсу на флеш-накопичувач 65
2.8 Проведення експериментальних досліджень ПЕМВ від флеш-накопичувачів 69
2.9 Рекомендації щодо мінімізації рівнів ПЕВМ при роботі з USB флеш-накопичувачами 84
2.10 Висновок 85
РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА 86
3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки. .. 86
3.2 Визначення трудомісткості розробки політики безпеки інформації 86
3.3 Розрахунок витрат на створення політики безпеки 87
3.4 Розрахунок (фіксованих) капітальних витрат 89
3.5 Розрахунок поточних (експлуатаційних) витрат 90
3.6 Висновки до розділу 3 95
ВИСНОВКИ 97
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 98

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи 100
ДОДАТОК Б. Перелік документів на оптичному носії..... 101
ДОДАТОК В. Відгук керівника економічного розділу 102
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи 103

ВСТУП

У процесі функціонування технічних засобів (ТЗ) обробки, зберігання та передачі інформації в конструктивних елементах і кабельних з'єднаннях цих пристроїв циркулюють електричні струми інформативних сигналів, до таких технічних засобів відносяться флеш-накопичувачі. Це призводить до формування та випромінювання в навколишній простір електромагнітних полів, рівні яких можуть бути достатніми для їх прийому на відстані від технічного засобу та за допомогою спеціальної апаратури. Можливість прихованого від власника технічного засобу, зокрема флеш-носія, знімання інформації, оброблюваної на пристрої, складність виявлення електромагнітного каналу витоку інформації зумовили високий інтерес до методів і засобів аналізу побічного електромагнітного випромінювання технічних засобів. Особливо при високих темпах зросту використання флеш-накопичувачів при обробці, зберіганні та передачі інформації.

Побічні електромагнітні випромінювання (ПЕМВ) є головною причиною утворення каналів витоку інформації з технічних засобів, зокрема флеш-накопичувачів, і одна з причин існування проблеми їх електромагнітної сумісності (ЕМС). Тому контроль та вимірювання рівнів ПЕМВ є ключовим завданням засобів і систем радіоконтролю і спецдосліджень апаратури.

Порівняльна простота і скритність добування інформації за рахунок перехоплюваних ПЕМВ і наведень, постійне вдосконалення техніки прийому та алгоритмів виділення інформативних сигналів, змушує фахівців проводити спеціальні дослідження технічних засобів для виявлення та інструментального контролю рівня інформативних ПЕМВ.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Технічні канали витоку інформативних сигналів, що виникають при роботі обчислювальної техніки за рахунок ПЕМВ

Під технічним каналом витоку інформації розуміють сукупність джерела інформації, лінії зв'язку (фізичного середовища), по котрій розповсюджується інформаційний сигнал, шуми, що перешкоджають передачі сигналу в лінії зв'язку, та технічних засобів перехоплення інформації.

Проблема витоку інформації через побічні електромагнітні випромінювання (ПЕМВ) технічних засобів вперше звернула на себе увагу фахівців ще на початку XX століття, проте всебічне вивчення ПЕМВ почалося лише наприкінці 1940-х - початку 50-х років. Переважна більшість досліджень носила закритий характер, і тільки з середини 1980-х років стала зростати кількість відкритих публікацій з цієї теми.

Окремі технічні засоби (ТЗ) або група технічних засобів, призначених для обробки конфіденційної інформації, разом з приміщеннями, в яких вони розміщуються, складають об'єкт ЗОТ.

Поряд з ЗОТ в приміщеннях встановлюються технічні засоби і системи, безпосередньо не беруть участь в обробці конфіденційної інформації, але використовуються спільно з ЗОТ і знаходяться в зоні електромагнітного поля, створюваного ними. Такі технічні засоби і системи називаються допоміжними технічними засобами і системами (ДТЗС). До них відносяться: технічні засоби відкритого телефонного, гучномовного зв'язку, системи пожежної та охоронної сигналізації, електрифікації, радіофікації, часофікації, електропобутові прилади та ін.

В якості каналу витоку інформації найбільший інтерес представляють ДТЗС, що мають вихід за межі контрольованої зони (КЗ), тобто зони, в якій виключена поява осіб та транспортних засобів, які не мають постійних або тимчасових перепусток на об'єкт.

Крім з'єднувальних ліній ЗОТ і ДТЗС за межі КЗ можуть виходити дроти і кабелі, що до них не відносяться, але що проходять через приміщення, де встановлені ТЗ, а також металеві труби систем опалення, водопостачання та інші струмопровідні металоконструкції. Такі дроти, кабелі та струмопровідні елементи називаються сторонніми провідниками.

Частотний діапазон побічних електромагнітних випромінювань, супроводжуючих інформативні сигнали, простягається від одиниць кілогерц до гігагерц і вище й визначається тактовою частотою використовуваного засобу обробки інформації (ЗОІ). Так, для стандартного комп'ютерного монітора перехоплення інформації можливий на частотах аж до 50 гармоніки тактової частоти, а рівень випромінювання, що становить в ближній зоні величину до десятків дБ, дозволяє приймати сигнали на віддаленні до декількох сотень метрів.

Крім електромагнітних випромінювань навколо засобів обробки інформації присутні квазистатичні інформаційні електричні й магнітні поля, що викликають наведення на близько розташовані кабелі, телефонні дроти, лінії охоронно-пожежної сигналізації, електромережі і т.п. Інтенсивність полів у діапазоні частот коливається від одиниць кілогерц до десятків мегагерц, в такому випадку прийом сигналів може вестися за межами контрольованої зони (КЗ) при безпосередньому підключенні до цих ліній передач.

Під витоком інформації по каналах побічного електромагнітного випромінювання розуміється можливість доступу до інформації, що обробляється на технічних засобах, здійснюваного шляхом перехоплення і відповідної обробки побічних електромагнітних випромінювань технічних засобів передачі, обробки та зберігання інформації. Канал витоку інформації включає в себе технічний засіб, середу поширення електромагнітних хвиль, систему перехоплення і обробки побічних випромінювань. Канали витоку інформації можуть виникати внаслідок випромінювання інформативних сигналів при роботі технічного засобу і наведення цих сигналів у лініях

зв'язку, ланцюгах живлення і заземлення, інших комунікаціях. ПЕМВ технічних засобів може поширюватися на великі відстані і реєструватися сучасними вимірювальними засобами. Частоти інформаційних складових побічних випромінювань залежать від типу технічного засобу та видів сигналів, що обробляються на ньому, і можуть перекривати діапазон частот від сотень герц до декількох десятків гігагерц.

В даний час технічна література, що стосується забезпечення інформаційної безпеки, практично відсутня. У більшості книг, присвячених проблемі інформаційної безпеки, матеріали про електромагнітні канали витоку інформації носять оглядовий характер. Більшість робіт у галузі дослідження побічного електромагнітного випромінювання технічних засобів проводяться з метою забезпечення державної безпеки, і всі отримані матеріали є секретними.

Для забезпечення інформаційної безпеки технічних засобів необхідно брати до уваги електромагнітну обстановку оточуючого середовища і рівень електромагнітних випромінювань досліджуваних технічних засобів у широкому діапазоні частот. У більшості випадків заходи щодо зниження вразливості радіотехнічного обладнання спираються на сукупність інженерно-технічних досліджень (ІТД), в результаті яких повинні бути отримані обґрунтовані рекомендації для кожного конкретного технічного засобу. Метою ІТД є виявлення та кількісна оцінка ступеня захищеності технічного засобу.

Найбільш часто на практиці застосовують критерій оцінки захищеності у вигляді відношення рівня інформативного сигналу в каналі витоку до рівня нормованої перешкоди. Тобто завдання ІТД полягає у визначенні реального відношення сигнал / шум на виході приймача ПЕМВ в точці його можливого розташування і в порівнянні отриманого значення з нормою. На практиці при оцінці захищеності каналів ЕМІ використовують не реальне відношення сигнал / шум, а відстань від технічного засобу, за межами якого виконується

умова захищеності. В даний час для проведення досліджень ПЕМВ технічних засобів доцільно використовувати такий комплекс апаратури, основу якого складає вимірювальний приймач або аналізатор спектру з набором відповідних вимірювальних антен. Вимірювальні приймачі найбільшою мірою відповідають вимогам, що пред'являються до апаратури для досліджень ПЕМВ. Вони забезпечують високу точність вимірювань при відносно не великих витратах часу. Значна частина вимірювальних приймачів дозволяє спостерігати панораму досліджуваного діапазону частот, аналізувати сигнали на виході детекторів різних типів. Однак ціна вимірювальних приймачів вельми висока. Спектроаналізатори за своїми функціональними можливостями цілком порівнянні з вимірювальними приймачами.

Більше того, на стадії виявлення ПЕМВ вони виявляються більш зручними, ніж приймачі. Для захисту технічних засобів від витоку інформації застосовуються організаційні та технічні заходи. Організаційні заходи спрямовані на те, щоб, не змінюючи рівня ПЕМВ досліджуваного пристрою або рівня електромагнітних шумів шляхом зміни розташування ТЗ домогтися зменшення зони можливого перехоплення інформації. До технічних заходів захисту інформації належать заходи і засоби, що впливають або на рівень ПЕМВ, або на рівень електромагнітних шумів. Наприклад, електромагнітне екранування є ефективним способом захисту інформації. При проведенні ІТД для забезпечення стаціонарності випромінювання технічного засобу і, як наслідок, більш впевненого виявлення інформаційних складових в ПЕМВ ТЗ, на практиці використовують такий режим роботи пристрою, при якому в ньому циклічно виконується набір однакових операцій. Цей режим роботи ТЗ називається тестовим режимом. Наприклад, для окремих блоків персонального комп'ютера використовуються наступні тест-режими: для монітора використовується режим відображення «точка через точку»; для флеш-носіїв використовується чергування запису і читання пакетів даних; для клавіатури - натиснута клавіша. Умови, що пред'являються до якості

вимірювання ПЕМВ ТЗ, вимагають розробки спеціальних програмно-апаратних комплексів, що використовують, поряд з універсальними вимірювачами, спеціалізовані пристрої для виявлення, обробки та реєстрації інформаційних складових ПЕМВ ТЗ. Це визначає актуальність завдання доопрацювання нових методів і алгоритмів ефективного аналізу електромагнітних випромінювань в широкій смузі частот, що враховують характеристики тестових послідовностей і використовуваних універсальних вимірювальних пристроїв.

1.2 Умови існування каналу витоку інформації

Наявність сигналів, що несуть конфіденційні повідомлення, на межі та за межами КЗ створює умови для витоку повідомлень за рахунок перехоплення цих сигналів зловмисником. Середовищем розповсюдження інформативного сигналу може служити навколишній простір (для електромагнітних полів) або провідні ланцюги та комунікації, що виходять за межі КЗ (у тому числі труби опалення та водопостачання). Ефективність каналу витоку визначається такими факторами, як:

- рівень інформативного сигналу від джерела;
- ослаблення та спотворення сигналу в середовищі його поширення;
- технічні характеристики приймального пристрою, що використовується зловмисником.

Чим ближче розташований приймач сигналу до джерела, тим, у загальному випадку, ефективніше працює канал витоку. Системним показником якості каналу витоку є співвідношення сигнал/шум на вході приймача перехоплення, яке визначається співвідношеннями параметрів всіх елементів каналу витоку.

За способом утворення класифікують чотири типи каналів витоку:

- канал електромагнітного випромінювання (ЕМВ), утворений полями, виникаючими при проходженні інформації по ланцюгах ЗОІ;

- канал випадкових антен (ВА), що виникає за рахунок наведених ЕДС в струмопровідних комунікаціях, гальванічно непов'язаних з ЗОІ і мають вихід за межі контрольованої зони (КЗ);

- канал комунікацій що відходять, гальванічно пов'язаних з ЗОІ;

- канал нерівномірного споживання струму (НВТ), що утворюється за рахунок амплітудної модуляції струму спрацьовуванням елементів ЗОІ при обробці інформації.

Канал ПЕМВ характеризується розміром зони ЕМВ - відстанню між ЗОІ і антеною апаратури перехоплення, за межами якої неможливий ефективний прийом внаслідок природного зниження рівня випромінюваного сигналу.

Канал випадкових антен характеризується розмірами їх зони для зосереджених випадкових антен (ЗВА) і розподілених випадкових антен (РВА). До зосереджених випадковим антенам відносяться будь-які технічні засоби, що мають вихід за межі контрольованої зони. До розподілених випадкових антен відносять дроти, кабелі, елементи конструкцій будівлі і т.п. Відстань між ЗОІ і ВА, на якій неможливе ефективне перехоплення, визначає розмір зони ВА.

Канал комунікацій, що відходять характеризується гранично доступним значенням відношення потужностей інформативного сигналу і нормованої перешкоди, при якому неможливий ефективний прийом.

Канал НВТ характеризується гранично допустимим значенням відношення величини зміни струму, що надходить від джерела при обробці інформації, до середньої величини струму споживання. Якщо зазначене відношення не перевищує граничного значення, ефективний прийом по каналу НВТ неможливий. В даний час, з урахуванням практичної відсутності у складі ЗОТ низькошвидкісних пристроїв (діапазон частот цього каналу приймається від 0 до 30 Гц), цей канал не актуальний.

З урахуванням викладеного можна сформулювати критерій захисту захищеності ЗОІ від витоку через ПЕМВ і наведення: ЗОІ вважається захищеним, якщо:

- радіус зони електромагнітних випромінювань не перевищує мінімально допустимої відстані від ЗОІ до кордону КЗ;

- відношення потужностей інформативного сигналу нормованої перешкоди у всіх ВА не перевищує на кордоні КЗ гранично допустиму величину;

- відношення потужностей інформативного сигналу нормованої перешкоди у всіх комунікаціях, що відходять на кордоні КЗ не перевищує гранично допустиму величину;

- відношення величини зміни струму «обробки» до середньої величини струму споживання від електромережі на кордоні КЗ не перевищує гранично допустиму величину.

1.2.1 Електромагнітні поля - основний канал витоку інформаційних сигналів

До електромагнітних каналів витоку інформації належать:

- випромінювання елементів ЗОТ;

- випромінювання на частотах роботи високочастотних генераторів ЗОТ, промодульованих інформаційними сигналами;

- випромінювання на частотах самозбудження ЗОТ.

Зупинимося детальніше на особливостях цього каналу витоку інформації з засобів обчислювальної техніки (діапазон частот 100 Гц ... 1 ГГц). Основні закономірності і властивості електромагнітного поля описуються системою рівняння Максвелла:

$$\begin{cases} rot\overline{H} = \sigma\overline{E} + \varepsilon_0\varepsilon_2 \dfrac{dE}{dt} \\ rot\overline{E} = -\mu_0\mu_2 \dfrac{dH}{dt} \\ div\overline{E} = \dfrac{\rho}{\varepsilon\varepsilon_0} \end{cases}, \qquad (1.1)$$

де $\varepsilon_0 = \dfrac{10^{-9}}{36\pi}(Ф/м)$, $\mu_0 = 4\pi 10^{-7}(Г/м)$.

Для гармонійного сигналу , тобто :

$$\dot{E} = Ee^{\text{iwt}}, \qquad (1.2)$$

$$\dot{H} = He^{iwt}, \qquad (1.3)$$

система рівнянь Максвелла буде мати вигляд:

$$\begin{cases} rot\dot{H} = (\sigma + iw\varepsilon_0)\dot{E} \\ rot\dot{E} = -iw\mu_0 H \\ div\dot{E} = \dfrac{\rho}{\varepsilon_0} \\ div\dot{H} = 0 \end{cases}, \qquad (1.4)$$

де rot E=$\lim \dfrac{\oint_S \overline{A}\,dl}{\Delta S}$. (1.5)

Для вирішення наведених рівнянь Максвелла вводяться додаткові параметри електромагнітного поля - електричний і магнітний запізнілі потенціали: φ и A:

$$\varphi = \frac{1}{4\pi\varepsilon_0}\int_v \frac{\rho\left(t - \dfrac{r}{i}\right)dv}{r}, \qquad (1.6)$$

$$\text{A} = \frac{\mu}{4\pi}\int_v \frac{\delta_i\left(t - \dfrac{r}{i}\right)dv}{r}, \qquad (1.7)$$

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

Для лінійного струму векторний потенціал відповідно дорівнює:

$$A = \frac{\mu_0}{4\pi}\int_e \frac{\delta dl}{r}. \qquad (1.8)$$

З урахуванням введених параметрів A і φ:

$$\begin{cases} \overline{E} = -\left(grad\varphi + \dfrac{d\overline{A}}{dt} \right) \\ \overline{H} = \dfrac{1}{\mu_0} rot\overline{A} \end{cases}, \qquad (1.9)$$

$$grad\varphi = \begin{cases} \dfrac{d\varphi}{dx} \\ \dfrac{d\varphi}{dy} \\ \dfrac{d\varphi}{dz} \end{cases}. \qquad (1.10)$$

Реальні випромінювачі ЗОТ можна розглядати як сукупність елементарних електричних і магнітних випромінювачів (диполів).

1.2.2 Природа виникнення каналу ПЕМВ

Канал ПЕМВ виникає через те, що будь-які автоматизовані системи (АС), побудовані на базі ПЕОМ, в процесі обробки даних створюють в навколишньому просторі електромагнітні поля, що містять інформативні складові, що викликають, у свою чергу, появу наведених сигналів в різних дротах, кабелях, лініях зв'язку, що проходять в безпосередній близькості від ПЕОМ, у тому числі в дротах електроживлення та заземлення. Це також відноситься до програмно-апаратних засобів захисту інформації від несанкціонованого доступу та до систем контролю доступу в приміщення, що мають в своєму складі електронні ідентифікатори.

Рівні ПЕМВ від засобів обчислювальної техніки регламентовані як з точки зору санітарно-гігієнічних норм, так і з точки зору електромагнітної сумісності (ЕМС) як вітчизняними, так і зарубіжними стандартами.

Однак наявність сертифіката з електромагнітної сумісності не є гарантією від перехоплення інформативного сигналу зловмисником, так як для розрізнення сигналу на тлі шумів і його аналізу досить, щоб напруженість поля інформативного сигналу була значно нижче цих значень.

1.2.3 Джерела і класифікація сигналів ПЕМВ

Інформативним ПЕМВ називаються сигнали, що представляють собою ВЧ несучу, модульовану інформацією оброблюваної на ЗОТ, наприклад, передача даних на флеш-накопичувач, дані, котрі обробляються на пристроях введення-виведення і т.д. Неінформативними ПЕМВ називаються сигнали, аналіз яких може дати уявлення тільки про режим роботи ЗОТ і ніяк не відображає характер інформації оброблюваної на ЗОТ.

Інформативного ПЕМВ не мають пристрої, що працюють з інформацією в аналоговому режимі, наприклад, копіювальні апарати, що використовують пряме світлокопіювання.

У ПЕОМ джерелами випромінювання інформативних сигналів є сильнострумові або високовольтні вузли і ланцюги. Прикладом можуть служити відеопідсилювач дисплея, підсилювачі друку в матричному принтері, підсилювачі запису - зчитування сигналів в дисководах. Зазначені вузли є основними джерелами створення інформативної складової електромагнітного поля навколо ПЕОМ, а дані, що циркулюють у цих ланцюгах, представлені у вигляді, найбільш зручному для відновлення.

Характерною особливістю сигналів у випромінюючих ланцюгах ПЕОМ є широкосмуговий спектр, обумовлений імпульсним видом циркулюючих сигналів. Частотний діапазон випромінювання інформативних сигналів лежить в межах від одиниць Гц до декількох ГГц. Причому максимальні амплітуди гармонік спектру електромагнітних сигналів від різних пристроїв ПЕОМ можуть бути зосереджені в різних ділянках зазначеного частотного діапазону.

Електрична або магнітна складова поля поблизу джерела випромінювання (як всередині джерела, так і поза ним) викликає появу напруг між окремими дротами (наприклад, між дротами мережі електроживлення), в результаті чого в них виникає наведений струм. Між корпусом пристрою і землею також існує деякий опір, на якому відбувається падіння напруги, під дією якого корпус пристрою сам стає додатковим джерелом випромінювання в навколишній простір. При цьому наводяться напруги можуть бути симетричними (діючими між проводами) і несиметричними (діючими між проводами і землею).

Частотний діапазон інформативних сигналів, що поширюються по дротах мережі, може становити від десятків Гц до сотень МГц. Тому в області високих частот дроти мережі живлення починають працювати як перевипромінювач антени. У зв'язку з цим мережа живлення може бути додатковим джерелом інформативного сигналу в ланцюгах заземлення ПЕОМ (через нульовий провід). Тому рекомендується напруга живлення підводити до ПЕОМ через мережеві фільтри з обов'язкової фільтрацією в нульовому проводі.

Найбільш небезпечними потенційно-інформативними ПЕМВ ПК є випромінювання, що генеруються ланцюгами, по яким:

- передаються сигнали від контролера клавіатури до порту вводу-виводу на материнській платі;

- передається відеосигнал від відеоадаптера до електродів електронно-променевої трубки монітора;

- відбувається зчитування інформації з магнітних або флеш-носіїв;

- відбувається обмін інформацією з периферійним устаткуванням і т.д.

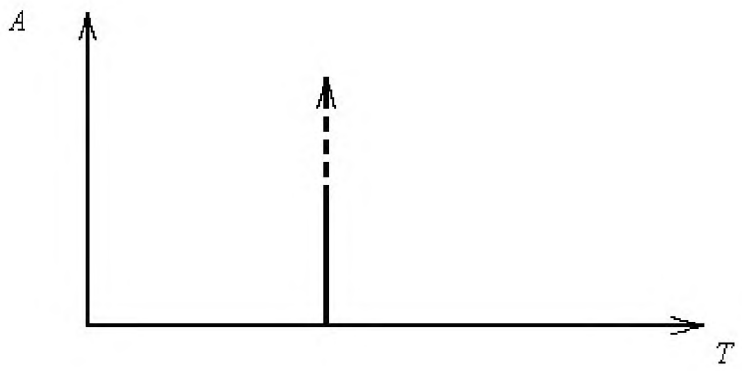
Застосування багаторозрядного паралельного коду (коли для передачі кожного розряду використовується свій електричний ланцюг) у більшості випадків (залежно від розрядності коду, формату представлення інформації) серйозно ускладнює відновлення інформації при перехопленні ПЕМВ. Таким

чином, не всі складові електромагнітного випромінювання ПК є небезпечними з точки зору перехоплення оброблюваної інформації. У той же час, наявність циклічної повторюваності якогось сигналу істотно полегшує його виявлення і виділення на тлі шумів і перешкод. Тому відносно просто вирішується завдання перехоплення інформації, яка циркулює у флеш-накопичувачі, так як в цьому випадку відбувається циклічна передача схожих сигналів в перебігу досить тривалого часу. Це дозволяє підвищити дальність перехоплення і зменшити ймовірність помилки при відновленні інформації.

Інформативні сигнали можуть поширюватися також за рахунок електромагнітного зв'язку джерела випромінювання з проводами і кабелями, що проходять поблизу ПЕОМ (телефонні лінії, лінії охоронної та пожежної сигналізації та ін.).

1.2.4 Спектри імпульсних сигналів

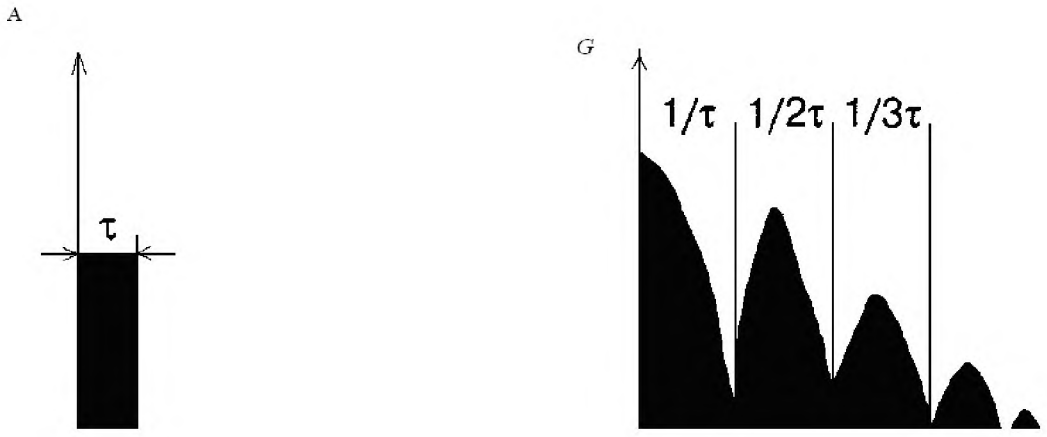
На рис. 1.1 а) приведений простий одиночний імпульсний сигнал, так звана «дельта-функція». Такий сигнал характеризується нескінченно малою тривалістю і нескінченної амплітудою, а площа такого імпульсу завжди дорівнює 1. Спектр такого сигналу наведено на рис 1.1 б). Спектр такого сигналу суцільний (без урахування властивостей випадкових антен в конкретному технічному засобі), нескінченний за частотою і його огинає плоска.



а)

б)

Рисунок 1.1 - Дельта-функція а) та її спектр б)

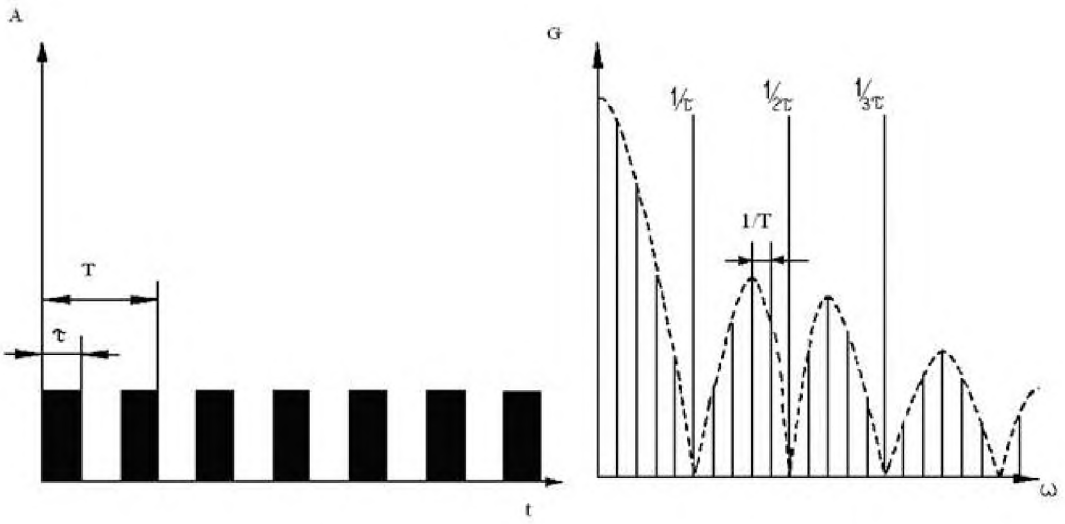


а) б)

Рисунок 1.2 - Одноразовий імпульс кінцевої тривалості а) та його спектр б)

У реальності таких імпульсів не буває. На рис. 1.2, а) наведено одиночний імпульс кінцевої тривалості. Огинаюча спектра стала нерівномірною (рис. 1.2, б)

На малюнку огинаюча представлена за абсолютною величиною, насправді кожний парний виток спрямований у другий квадрант. Для наближення моделі до реальних сигналах розглянемо нескінченну послідовність імпульсів кінцевої тривалості. Цей сигнал і його спектр наведено на рис. 1.3.



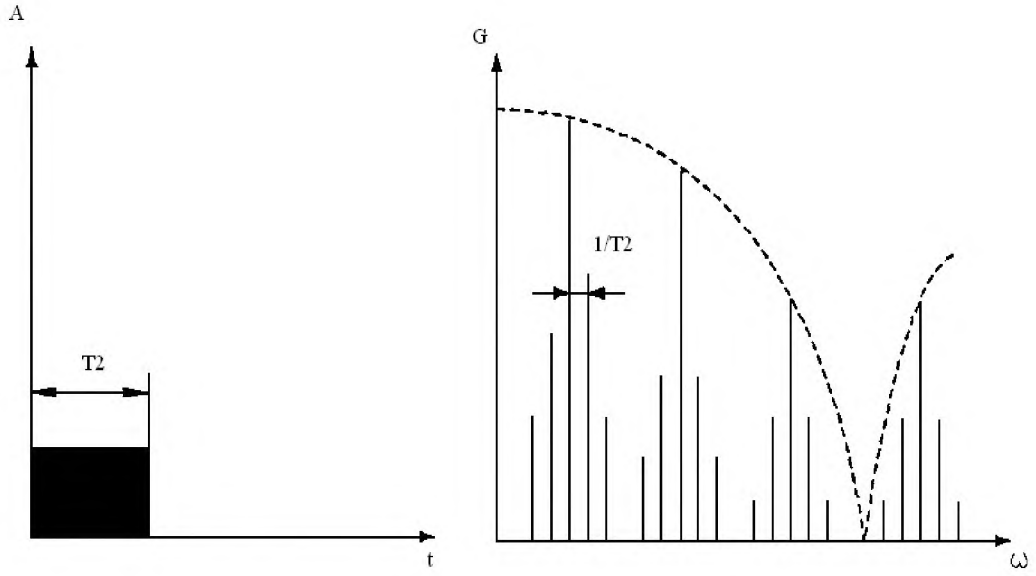
а) б)

Рисунок 1.3 - Спектр нескінченної послідовності імпульсів

Таким чином, спектр послідовності імпульсів становиться «лінійчатим», зберігаючи огинаючу одиночного імпульсу. Причому крок гармонік за частотою обернений періоду проходження імпульсів. А амплітуда гармонійних складових виросла. Саме цей ефект і дозволяє різко поліпшити співвідношення сигнал / шум при вимірюванні сигналів ПЕМВ.

Всі наведені вище спектри ілюструють гранично ідеалізовану картину. Реальні спектри ПЕМВ при збігу частот, мають абсолютно випадкові розподіли амплітуд. Реальне випромінювання є суперпозиція великого числа випромінювачів (випадкових антен), у кожного з яких своя амплітудно-частотна характеристика зі своїми піками і провалами, резонансами і т.ін.

У реальних пристроях імпульсні послідовності не бувають нескінченними. Практично без винятків будь-яке пересилання, обробка виконується «пакетами». Тому найбільш реальною моделлю сигналу в ланцюгах ПЕОМ буде послідовність таких пакетів, в яких довжина пакета істотно більше тривалості одного імпульсу. Така модель і її спектр представлені на рис. 1.4



а) б)

Рисунок 1.4 - Спектр послідовності пакетів імпульсів

Як видно на рисунку біля кожної спектральної складової, зумовленої самими імпульсами, з'явилися бічні складові, обумовлені частотою проходження пакетів.

1.2.5 Характеристика середовища поширення сигналів

У середовищі поширення повідомлень завжди присутні різні перешкоди (будь-який вплив на сигнал, що перешкоджає правильному прийому повідомлення) так чи інакше маскують сигнал. Перешкоди поділяються на адитивні і мультиплікативні. Адитивні завади характеризуються тим, що суміш сигналу s(t) і перешкоди n(t) на вході приймача являють собою їх суму:

$$x(t)=s(t)+n(t). \qquad (1.11)$$

У більшості випадків можна вважати, що перешкода являє собою білий шум, який як узагальнений процес не має жодних розподілів ймовірності, але після проходження через фільтр він завжди перетворюється на гауссівський процес. Такий шум характеризується односторонньою спектральною

щільністю потужності N_o (що має розмірність енергії) і кореляційної функцією, що представляє собою дельта-функцію $\delta(t-\tau_0)$. При зверненні до двосторонніх спектральних щільностей процесів, визначених для позитивних і негативних значень кругової частоти (від $-\infty$ до $+\infty$), спектральна щільність потужності білого шуму приймається рівною $0,5N_0$.

Характерним прикладом адитивних перешкод є:

- атмосферні перешкоди, зумовлені електричними процесами в атмосфері, і, перш за все грозовими розрядами;

- космічні перешкоди, викликані радіовипромінюванням Сонця та інших небесних тіл;

- внутрішні шуми радіоприймача, зумовлені хаотичним рухом носіїв заряду в самому приймачі;

- індустріальні перешкоди, обумовлені роботою електричних пристроїв і агрегатів;

- перешкоди від сторонніх радіостанцій.

Атмосферні перешкоди - це той вид перешкод, який завжди присутній у навколишньому просторі, тому, при визначенні дальності поширення повідомлень по каналу ПЕМВ, необхідно враховувати не тільки природне загасання сигналів, але і спотворення, що вносяться цими перешкодами.

Таким чином, усі ці фактори необхідно брати до уваги при побудові системи захисту, опираючись на критерії захищеності ЗОТ.

1.3 Визначення критеріїв захищеності ЗОТ

Критерієм оцінки захищеності об'єкта обчислювальної техніки є умова: якщо для влаштування ЗОТ відношення сигнал/шум (Δ) на виході приймального пристрою перехоплення секретної інформації не перевищує гранично допустимого значення δ у всіх можливих каналах витоку, тобто

$$\delta \geq \Delta = \frac{U_{с.пик}}{U_{ш.эфф}}, \qquad (1.12)$$

де $U_{с.пік}$ - пікове значення сигналу , $U_{ш.эфф}$ - значення рівня шуму

то пристрій захищений від витоку. Об'єкт вважається захищеним в цілому, якщо захищений кожний пристрій.

Виміряне співвідношення небезпечний сигнал / перешкода (Δ) - відношення амплітуди імпульсного сигналу до середньоквадратичної напруги перешкоди на виході приймального пристрою.

Для об'єктів категорії 1 - це оптимальний приймач імпульсних сигналів з повністю відомими параметрами на прийомі, що забезпечує мінімальну ймовірність помилки. Для об'єктів категорії 2 і 3 - перестроюваний узгоджений фільтр з оптимальною смугою пропускання.

Δ f, лежить в межах:

$$f_T \prec \Delta f \prec \frac{1}{\tau}, \qquad (1.13)$$

де f_T – тактова частота сигналу, τ- тривалість імпульсу.

1.4 Характеристики та параметри інформативних сигналів, що підлягають вимірюванню

Під сигналом s (t) розуміють зміну в часі одного з параметрів фізичного процесу. Детермінованим називається сигнал, який точно визначений в будь-який момент часу (наприклад, заданий в аналітичному вигляді). Детерміновані сигнали можуть бути періодичними і неперіодичними. Періодичним називається сигнал, для якого виконується умова s (t) = s (t + Kt), де к - будь-яке ціле число, Т - період, який є кінцевим відрізком часу. Приклад періодичного сигналу - гармонійне коливання. Будь-який складний періодичний сигнал може бути представлений у вигляді суми гармонійних коливань з частотами, кратними основній частоті

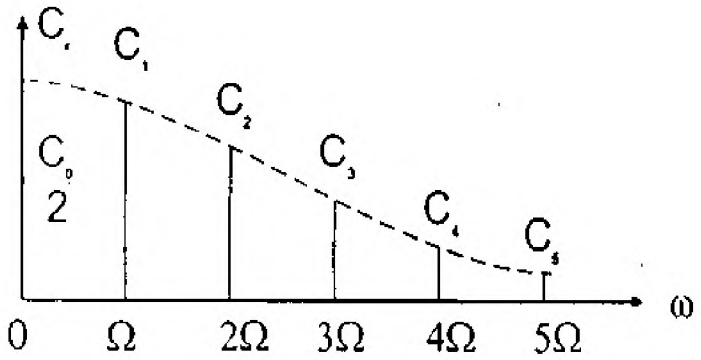
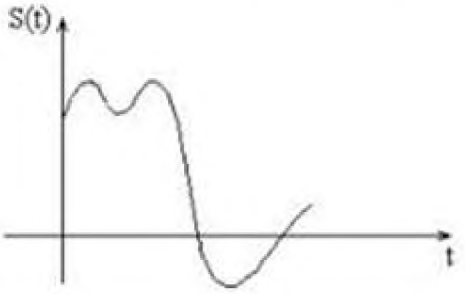


Рисунок 1.5 - Спектр періодичної функції

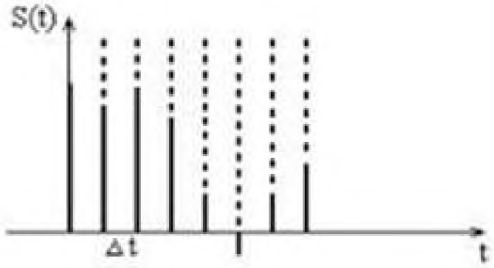
Неперіодичний сигнал, як правило, обмежений у часі. Випадковим сигналом називають функцію часу, значення якої заздалегідь невідоме і може бути передбачене лише з деякою ймовірністю. В якості основних характеристик випадкових сигналів приймають:

а) закон розподілу ймовірності (відносний час перебування величини сигналу в певному інтервалі);

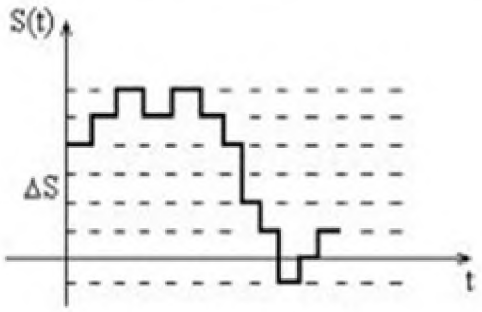
б) спектральний розподіл потужності сигналу.



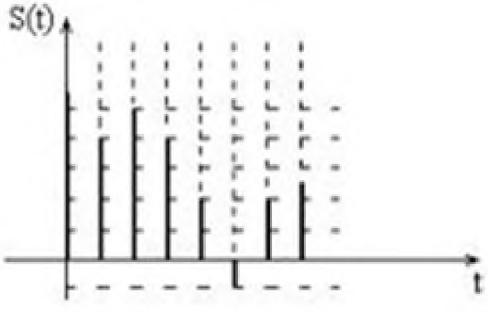
а) безперервний



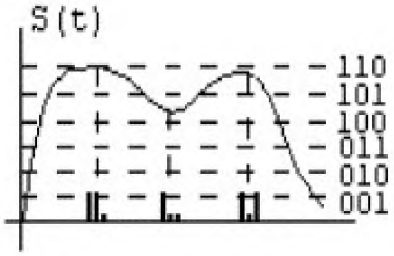
б) дискретний



в) квантований



г) дискретно-квантований



д) цифровий сигнал

Рисунок 1.6 - Форми детермінованих сигналів

Цифровий сигнал представляє з себе комбінацію вузьких імпульсів однакової амплітуди, що виражають в двійковому вигляді дискретні відліки сигналу.

У радіотехніці в якості базисних функцій розкладання Фур'є використовують переважно тригонометричні функції.

Спектр періодичного сигналу є дискретним і представляє набір гармонійних коливань, у сумі становить вихідний сигнал. Однією з переваг розкладання сигналу в спектр є наступне: сигнал, проходячи по ланцюгу, зазнає змін (посилення, затримка, детектування, зміна фази, обмеження і т.д.) Струми і напруги в ланцюзі під дією сигналу описуються диференціальними рівняннями, відповідними елементам ланцюга і способу їх з'єднання. Лінійні ланцюги описуються лінійними диференціальними рівняннями, причому для лінійних ланцюгів вірний принцип суперпозиції, згідно з яким дія на систему складного сигналу, що складається з суми простих сигналів, дорівнює сумі дій від кожного складового сигналу окремо. Це дозволяє при відомій реакції системи на який-небудь простий сигнал, наприклад, на синусоїдальне коливання з певною частотою, визначити реакцію системи на будь-який складний сигнал, розклавши його в ряд по синусоїдальним коливанням.

Описані типи сигналів виникають при роботі різних технічних засобів , наприклад: жорстких дисків, моніторів, принтерів, а також флеш-накопичувачів. Флеш-накопичувачі набули широкого застосування відносно

недавно. У зв'язку з цим відсутня достатня кількість матеріалів та літератури у відкритому доступі щодо досліджень рівнів ПЕМВ при роботі з флеш-накопичувачами та рекомендацій щодо їх зниження. Тому постає необхідність проведення спеціальних досліджень по виявленню ПЕМВ при роботі з флеш-накопичувачами. Для вирішення даного питання для початку необхідно проаналізувати структуру та принципи побудови флеш-накопичувачів.

1.5 Принцип побудови флеш-накопичувачів

Флеш-пам'ять - різновид напівпровідникової технології електрично перепрограмованої пам'яті (EEPROM). Це ж слово використовується в електронній схемотехніці для позначення технологічно закінчених рішень постійних запам'ятовуючих пристроїв у вигляді мікросхем на базі цієї напівпровідникової технології. У побуті це словосполучення закріпилося за широким класом твердотільних пристроїв зберігання інформації. Завдяки компактності, дешевизні, механічної міцності, великому обсягу, швидкості роботи і низькому енергоспоживанню, флеш-пам'ять широко використовується в цифрових портативних пристроях і носіях інформації. Серйозним недоліком даної технології є обмежений термін експлуатації носіїв, а також чутливість до електростатичного розряду.

В основі будь-якої флеш-пам'яті лежить кристал кремнію, на якому сформовані польові транзистори. У такого транзистора є два ізольованих затвора: керуючий (control) і плаваючий (floating). Останній здатний утримувати електрони, тобто заряд. У комірці, як і у будь-якого польового транзистора, є стік і джерело (рис. 1.7). У процесі запису на керуючий затвор подається позитивна напруга і частина електронів, що рухаються від стоку до витоку, відхиляється до плаваючого затвору. Деякі з електронів долають шар ізолятора і проникають (дифундують) у плаваючий затвор. У ньому вони можуть залишатися протягом багатьох років. Концентрація електронів в області плаваючого затвора визначає одне з двох стійких станів транзистора -

комірки пам'яті. У першому, початковому, стані кількість електронів на плаваючому затворі мала, а порогова напруга відкриття транзистора невисока (логічна одиниця). Коли на плаваючий затвор занесено достатню кількість електронів, транзистор виявляється в другому стійкому стані. Напруга відкриття його різко збільшується, що відповідає логічному нулю.

При зчитуванні вимірюється порогова напруга, яку потрібно подати на стік для відкриття транзистора. Для видалення інформації на керуючий затвор короткочасно подається негативна напруга, і електрони з плаваючого затвора дифундують назад на витік. Транзистор знову переходить у стан логічної одиниці і залишається в ньому, поки не буде проведений черговий запис.

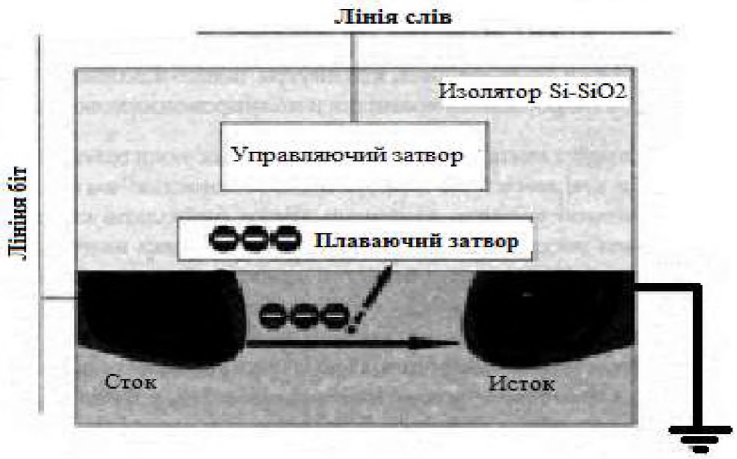


Рисунок 1.7 - Комірка флеш-пам'яті

Примітно, що у флеш-пам'яті один транзистор зберігає один біт інформації - він і є коміркою. Весь процес «запам'ятовування» заснований на дифузії електронів в напівпровіднику. Звідси випливають два не надто оптимістичних виводу. Час зберігання заряду дуже великий і вимірюється роками, але все ж обмежений. Закони термодинаміки і дифузії свідчать, що концентрація електронів у різних областях рано чи пізно вирівняється. З тієї ж причини обмежена кількість циклів запису-перезапису: від ста тисяч до декількох мільйонів. З часом неминуче відбувається деградація самого матеріалу і p-n-p переходів.

1.5.1 Компоненти USB флеш-накопичувача

Незважаючи на різноманітність корпусів, всі флеш-диски USB влаштовані однаково. Якщо половинки корпусу з'єднані засувками, вони зазвичай легко роз'єднуються. Водонепроникні корпуси доводиться розкривати руйнівними методами, наприклад, розрізати. На платі всередині USB флеш-накопичувача обов'язково присутні дві мікросхеми: чіп пам'яті і контролер. На обох нанесене заводське маркування. Іноді на платі розміщується два чіпи флеш-пам'яті, які працюють в парі. Обв'язка мікросхем складається з декількох резисторів і діодів, стабілізатора живлення і кварцового резонатора. Стабілізатори все частіше вбудовуються безпосередньо в контролер і кількість навісних елементів скорочується до мінімуму. Крім того, на платі можуть перебувати світлодіодний індикатор і мініатюрний перемикач для захисту від запису. Роз'єм USB припаяний безпосередньо до плати. Місця пайки контактів в багатьох моделях є досить вразливими, оскільки на них припадає механічне навантаження при підключенні і відключенні пристрою.

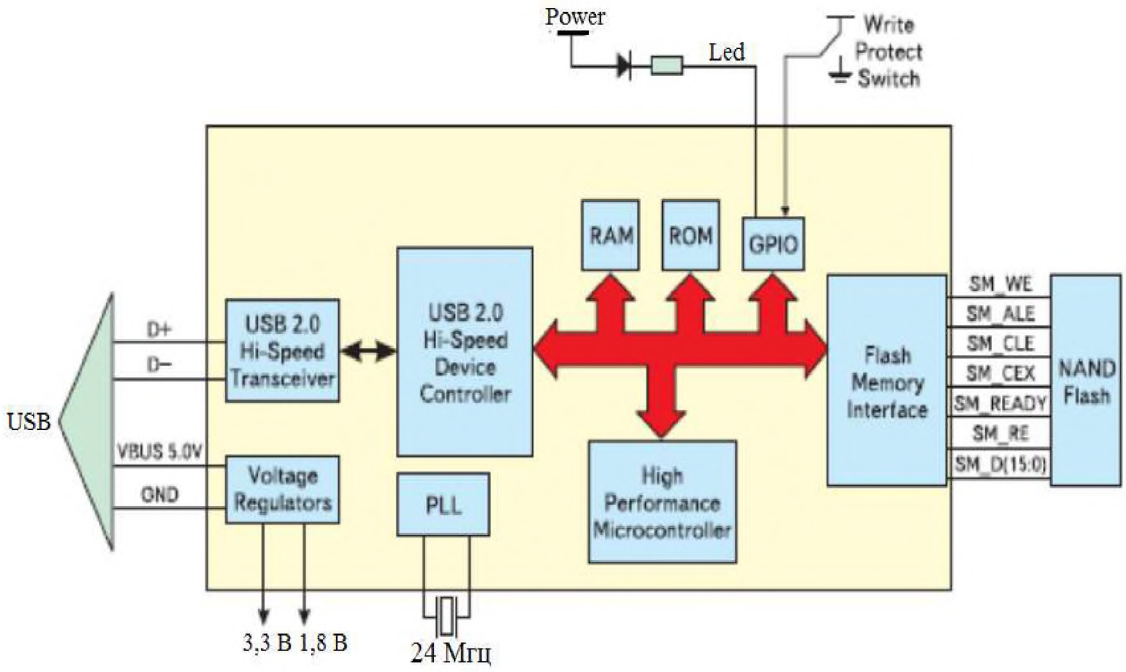


Рисунок 1.8 - Структурна схема контролера USB флеш-накопичувача

Як видно зі структури контролера, до його складу входять блоки для підтримки інтерфейсу USB і роботи з флеш-пам'яттю. Протокол інтерфейсу

USB і флеш-пам'яті підтримується вбудованим мікроконтролером High Performance Microcontroller, який використовує для своєї роботи вбудовану постійну пам'ять програм ROM і оперативну пам'ять RAM. Підтримка інтерфейсу USB здійснюється за допомогою блоку високошвидкісного приймача-USB2.0 Hi-Speed Transceiver і пристрої керування USB2.0 Hi-Speed Device Controller. Внутрішній синтезатор частот PLL забезпечує необхідну синхронізацію роботи всіх внутрішніх пристроїв за допомогою зовнішнього кварцового резонатора на 24 МГц. Блок GPIO забезпечує зовнішнє управління і індикацію режиму роботи контролера. Зв'язок контролера з флеш-пам'яттю здійснюється через інтерфейс пам'яті Flash Memory Interface. Вбудований регулятор напруги Voltage Regulators формує з вхідної напруги 5 В, що надходить від інтерфейсу USB, необхідні для роботи ядра контролера і зовнішніх мікросхем пам'яті напруги живлення 3,3 і 1,8 В. Контролер випускається в сучасному малогабаритному 48-вивідному корпусі типу QFN розміром всього 77 мм.

1.5.2 Структура флеш-пам'яті з архітектурою NOR

Схема логічного елемента (NOR - Not OR - у булевій математиці позначає заперечення «АБО»), наведена на малюнку.

За допомогою неї здійснюється перетворення вхідних напруг у вихідні, відповідні «0» і «1». Вони необхідні, тому що для читання / запису даних в комірці пам'яті використовуються різні напруги.

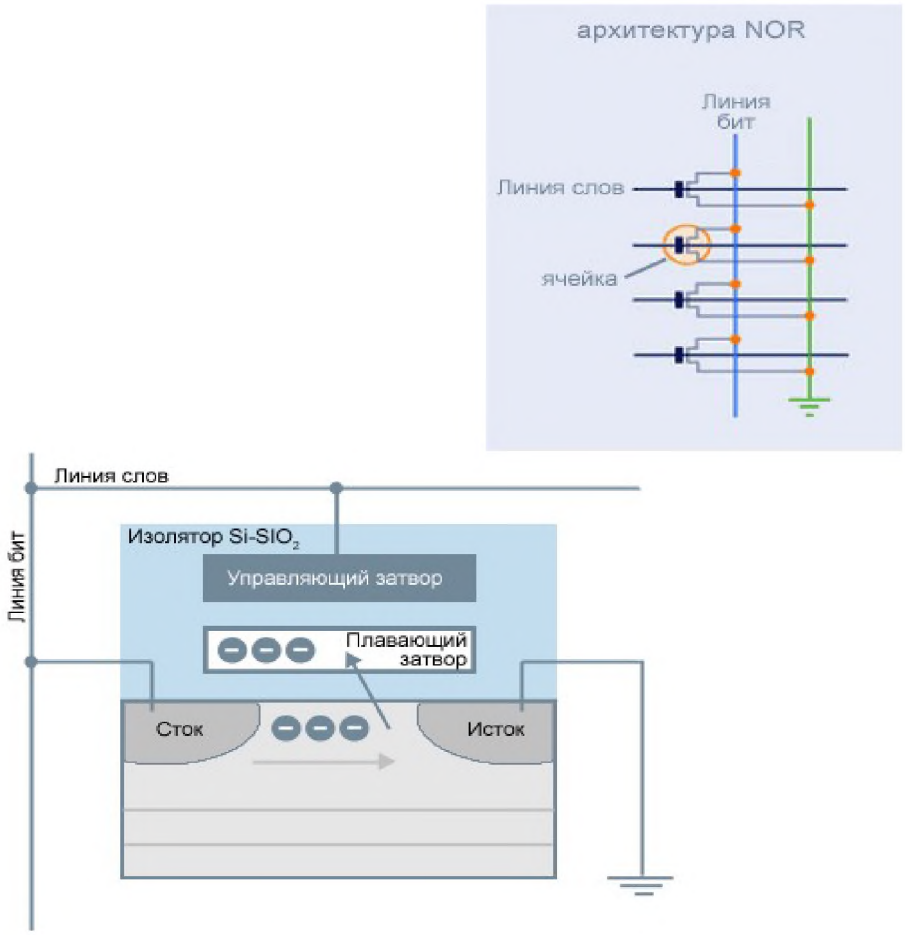


Рисунок 1.9 - Схема архітектури NOR

Дана схема характерна для більшості флеш-чіпів і представляє з себе транзистор з двома ізольованими затворами: керуючим (control) і плаваючим (floating). Важливою особливістю останнього є здатність утримувати електрони, тобто заряд. Також в комірці є так звані «стік» і «витік». При програмуванні між ними, внаслідок впливу позитивного поля на керуючому затворі, створюється канал - потік електронів. Деякі з електронів, завдяки наявності більшої енергії, долають шар ізолятора і потрапляють на плаваючий затвор. На ньому вони можуть зберігатися протягом декількох років. Певний діапазон кількості електронів (заряду) на плаваючому затворі відповідає логічній одиниці, а все, що більше його, - нулю. При читанні ці стани розпізнаються шляхом вимірювання порогової напруги транзистора. Для стирання інформації на керуючий затвор подається висока негативна напруга,

і електрони з плаваючого затвора переходять (туннелують) на джерело. У технологіях різних виробників цей принцип роботи може відрізнятися за способом подачі струму і читання даних з осередку. У структурі флеш-пам'яті для зберігання 1 біта інформації задіюється тільки один елемент (транзистор), в той час як в енергозалежних типах пам'яті для цього потрібно кілька транзисторів і конденсатор. Це дозволяє істотно зменшити розміри мікросхем, спростити технологічний процес, а, отже, і знизити собівартість. Але і один біт далеко не межа: Intel вже випускає пам'ять StrataFlash, кожен осередок якої може зберігати по 2 біти інформації. Крім того, існують пробні зразки, з 4-х і навіть 9-й бітними осередками. У такій пам'яті використовуються технологія багаторівневих осередків. Вони мають звичайну структуру, а відмінність полягає в тому, що заряд їх ділиться на кілька рівнів, кожному з яких у відповідність ставиться певна комбінація біт. Теоретично прочитати / записати можна і більше 4-х біт, однак, на практиці виникають проблеми з усуненням шумів і з поступовою витоком електронів при тривалому зберіганні. З недоліків, зокрема, у флеш-пам'яті з архітектурою NOR варто відзначити погану масштабованість: не можна зменшувати площу чіпів шляхом зменшення розмірів транзисторів. Ця ситуація пов'язана зі способом організації матриці осередків: у NOR архітектурі до кожного транзистору треба підвести індивідуальний контакт. Набагато краще в цьому плані проявляють себе флеш-пам'ять з архітектурою NAND.

1.5.3 Структура флеш-пам'яті з архітектурою NAND

NAND - Not AND - у булевій математиці позначає заперечення «І». Відрізняється така пам'ять від попередньої логічною схемою.

Пристрій і принцип роботи осередків аналогічний NOR. Істотною відмінністю даних архітектур є - розміщення осередків та їх контактів. На відміну від вищеописаного випадку, тут є контактна матриця, в перетинах рядків і стовпців якій розташовуються транзистори. Це порівняно з пасивною

матрицею в дисплеях. (а NOR - з активною TFT). У випадку з пам'яттю така організація дещо краще - площа мікросхеми можна значно зменшити за рахунок розмірів комірок. Недоліки полягають у більш низькою порівняно з NOR швидкості роботи в операціях побайтового довільного доступу.

1.6 Висновки. Постановка задачі

Аналіз технічного каналу витоку інформації показав, що побічні електромагнітні випромінювання (ПЕМВ) є головною причиною утворення каналів витоку інформації технічних засобів, зокрема флеш-накопичувачів, і однією з причин існування проблеми їх електромагнітної сумісності (ЕМС). Тому контроль та вимірювання рівнів ПЕМВ є ключовим завданням засобів і систем радіоконтролю і спецдосліджень апаратури. Також відсутні відкриті джерела з рекомендаціями по зниженню рівнів ПЕМВ при роботі з флеш-накопичувачами.

Виходячи з цього необхідно провести дослідження чинників, які можуть впливати на рівні ПЕМВ при роботі з флеш-накопичувачами. На основі аналізу отриманих даних розробити рекомендації щодо їх зменшення з метою зниження ймовірності витоку інформації через ПЕМВ.

В зв'язку з цим необхідно виконати наступні задачі :

- провести аналіз принципів дії, режимів роботи, структури флеш-накопичувачів, особливостей кодування та передачі даних через USB інтерфейс;
- обґрунтувати вибір апаратури з виявлення та вимірювання рівнів ПЕМВ для проведення експериментальних досліджень;
- розробити порядок проведення експериментальних досліджень рівнів ПЕМВ при роботі з флеш-накопичувачами;

- згідно з розробленого порядку провести дослідження впливу визначених чинників на рівні ПЕМВ, що виникають при роботі з флеш-накопичувачами;
- провести аналіз отриманих результатів та розробити рекомендації щодо зниження рівня ПЕМВ під час обробки інформації з обмеженим доступом при використанні флеш-накопичувачів.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

Перед початком проведення експериментальних досліджень виявлення ПЕВМ від флеш-накопичувачів необхідно провести аналіз структури та елементів USB-інтерфейсу, принципів кодування та синхронізації даних, які передаються через USB-інтерфейс, а також проаналізувати типи сигналів, що генеруються у USB-інтерфейсі та передаються на флеш-накопичувач.

2.1 Аналіз фізичного рівня USB

Фізичний рівень USB 1.1 складається з двох драйверів і фізичного середовища (кабелю) між ними. Драйвери фізичного рівня не симетричні, тобто мають різну структуру. Фізичне середовище одноточкове і одностороннє (напівдуплекс).

Існує два типи драйвера: Downstream (передаючий вниз) - цей драйвер завжди ведучий, тобто тільки він визначає хто, коли і скільки буде передавати даних в лінію зв'язку. Драйвери цього типу завжди генерують інформаційний сигнал у напрямку від хоста. У мережі ці драйвери встановлені на хості або передаючий вниз порт хаба. Структура драйвера представлена на рис. 2.1 Upstream (передаючий вгору) - це драйвер завжди ведений. Він завжди генерує інформаційний сигнал у напрямку хоста. Час і порядок його роботи визначає ведучий драйвер (Downstream).

Ці драйвера встановлюються в пристроях і передаючих вгору портах хаба. Драйвер Upstream може бути одного з двох видів:

- upstreeam Full Speed - для роботи на швидкості 12 Mb/s;
- upstream Low Speed - для роботи на швидкості 1,5 Mb/s.

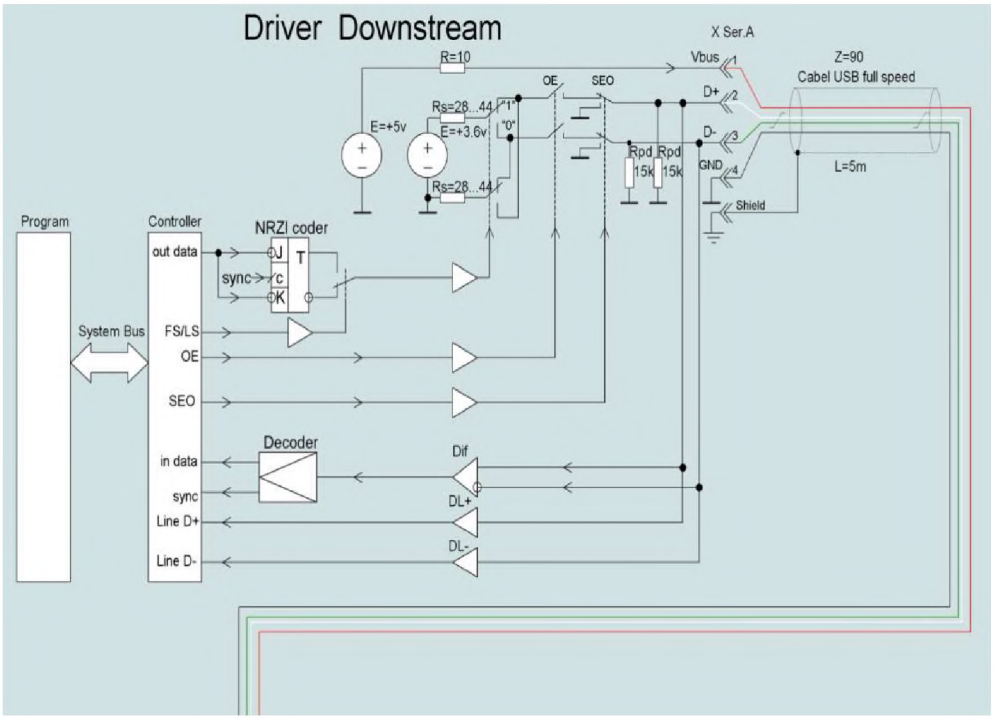


Рисунок 2.1 - Структура драйвера Downstream

Так як драйвери несиметричні, зв'язок у фізичному рівні USB 1.1 можливий тільки між драйверами різного типу, тобто тільки між Downstream і Upstream. Відповідно несиметричний кабель для підключення, з боку Downstream він має роз'єм серії A, а з боку Upstream роз'єм серії B. Драйвера і кабелі RS232 і RS485 симетричні, тому ПК можна з'єднувати між собою через COM порти. З'єднати два ПК через USB-порти неможливо. Цей факт звичайно, погіршує універсальність порту, але дозволяє спростити апаратну частину, так як односторонні драйвери апаратно більш прості. Крім того, одностороння реалізація спрощує програмний рівень, так як паралельні процеси в ПК важко реалізувати. Структура драйвера Full Speed представлена на рисунку 2.2, драйвера Low Speed на рисунку 2.3.

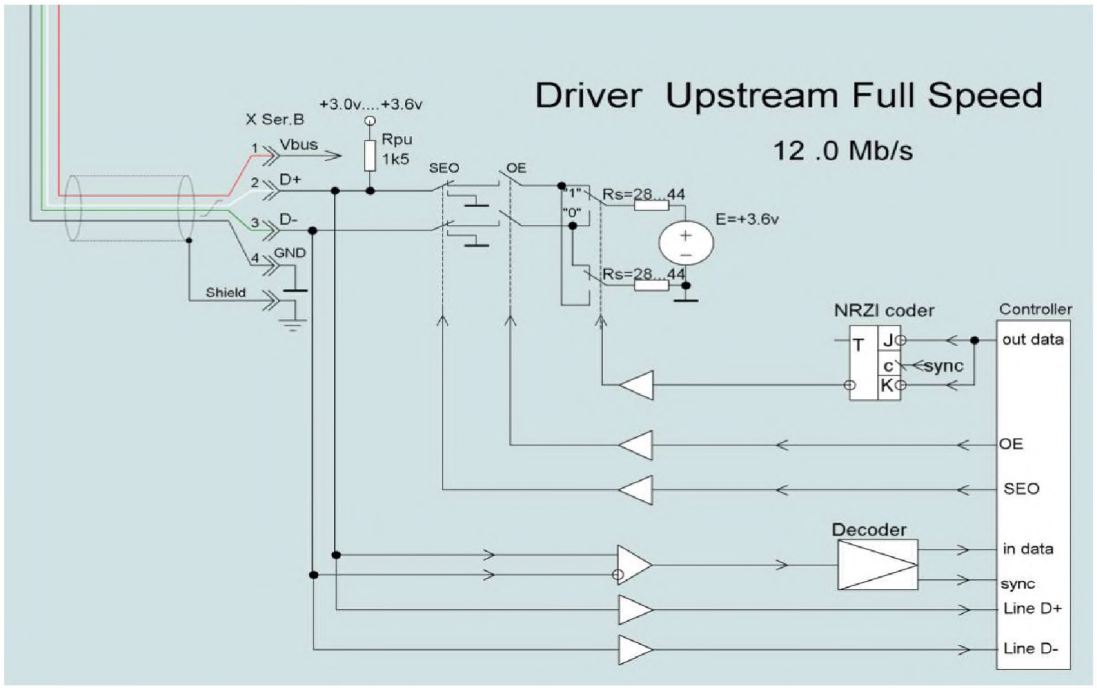


Рисунок 2.2 - Структура драйвера Upstream Full Speed

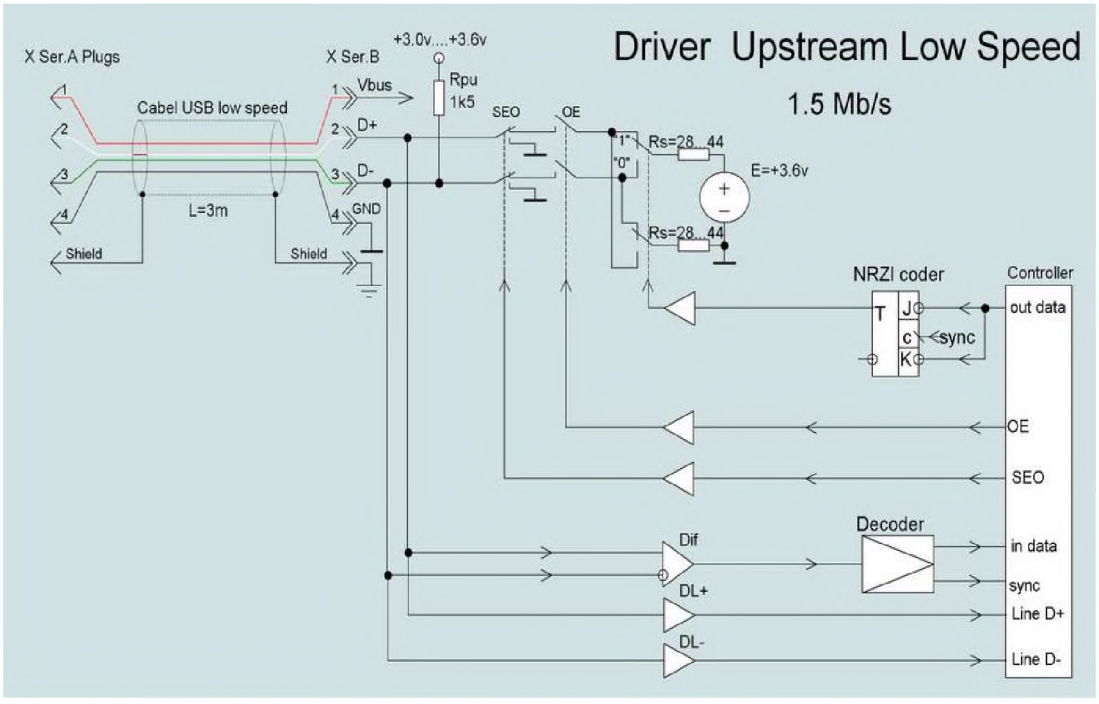


Рисунок 2.3 - Структура драйвера Upstream Low Speed

2.1.1 Аналіз структури драйверів USB-інтерфейсу

Як видно з рис. 2.3 драйвери USB складаються з: контролера, кодера, декодера, генератора, диференціального та лінійних приймачів, підтягаючих резисторів і джерела живлення.

Контролер драйвера

Контролер з'єднує генеруючу і приймальну частину драйвера через системну шину з програмним рівнем хоста, концентратора або пристрою. Оскільки весь переданий пакет може бути сформований програмним рівнем, то апаратна реалізації контролера не складна.

Кодер NRZI

Пакет кодується методом NRZI за допомогою JK-тригера. Алгоритм NRZI кодування досить простий, при передачі нуля генератор повинен змінити полярність сигнальної лінії на протилежну, при передачі одиниці залишити полярність сигналу колишньої (тобто нічого не змінювати). Кодери для Full Speed і Low Speed відрізняються вихідним сигналом (протилежні).

NRZI кодування дозволяє скоротити число сінхробітов, котрі вставляються в пакет даних.

Декодер

Перетворює NRZI закодовані дані до початкового вигляду і виділяє синхросигнал із прийнятих даних.

Генератор

Генератор передає в лінію зв'язку диференціальні нулі й одиниці.

Коли генератор не передає дані, він відключений від лінії зв'язку сигналом OE і не впливає на її роботу.

Генератор може замикати лінію зв'язку на загальний провід сигналом SEO. Це використовується для скидання шини.

Параметри генератора:

EPC генератора: +3,6 В.

Внутрішній опір: 56 .. 88 Ом.

Макс. допустиме пряме лінійне напруга: +4,6 В.

Макс. допустима зворотна лінійна напруга: -1,0 В.

Генератор повинен статично тримати параметри лінійної напруги на виході:

VOL = не більше +0.3 В при навантаженні 1,5 кОм підключеної до +3,6 В для низ. лінійного сигналу (0);

VOH = не менше +2.8 В при навантаженні 15 кОм підключеної до GND для вис. лінійного сигналу (1).

Наростання фронту лінійного сигналу, має бути в межах: 4ns .. 20нс (FS), 75нс .. 300нс (LS).

Тривалість лінійного сигналу високого рівня при передачі біта повинна бути не менше: 60нс.

Перетин лінійних сигналів D + і D-(Vd + = Vd-) має бути в діапазоні: VCRS = 1,3 В ... 2,0 В.

Нагрузочна ємність виходу: CL = 50 пФ (FS), 50 пФ .. 150 пФ (LS Upstream), 200 пФ .. 600 пФ (LS Downstream).

2.2 Аналіз сигналів, що надходять через USB-інтерфейс на флеш-накопичувач

2.2.1 Принципи кодування та синхронізації даних , які передаються через USB-інтерфейс

Бінарні дані передаються через інтерфейс USB кодуються методом NRZI.

Метод NRZI (Non Return to Zero Invert) полягає в зміні полярності сигналу при кодуванні "0".

При передачі "1" полярність сигналу залишається колишньою.

NRZI кодовані сигнали Low Speed пристроїв протилежні сигналам Full Speed пристроїв USB. Принцип роботи даного методу кодування представлений на рисунку 2.4.

Кодування використовується для збільшення інформаційної ємності сигналу, за рахунок зменшення кількості вбудованих синхробітів.

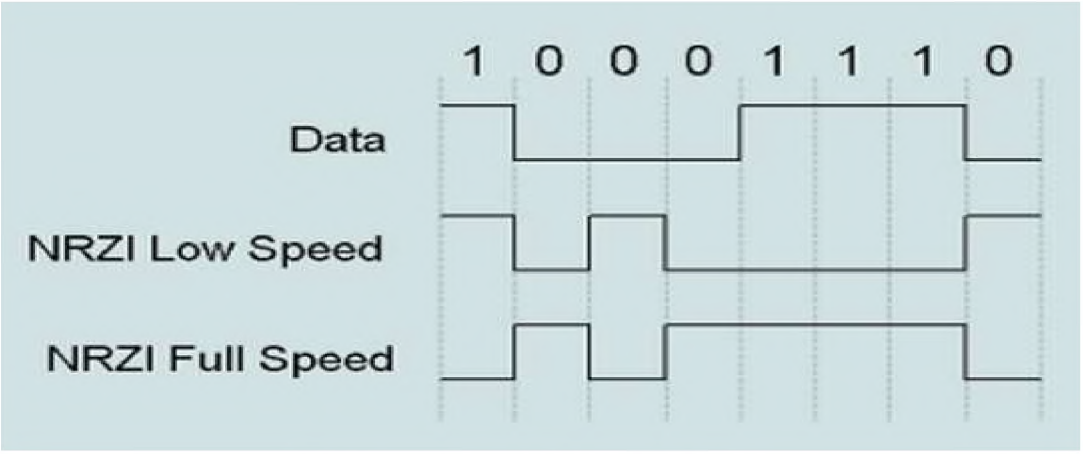


Рисунок 2.4 - NRZI кодування.

Синхронізація даних здійснюється від кожного перехідного фронту сигналу.

Так як кожен "0" біт даних змінює полярність сигналу при NRZI кодуванні на протилежний, то кожен "0" біт створює перехідною фронт сигналу, відносно якого синхронізується приймач даних.

Три методу синхронізації пакету даних в USB:

1 SOP (Start-of-Packet) Перехід зі стану Idle в стан K.

У початку кожного пакета вставляється байт 80h, який має 7 нулів і одну одиницю. Сім фронтів йдуть підряд дозволяють надійно синхронізувати приймач з початком пакету даних.

2 "0" біт даних.

Кожен "0" біт даних додатково синхронізує приймач. В результаті NRZI кодування, всі дані містять "0" біт не потребують додаткового синхробітах.

3 Stuffed Bit-вставляється синхробіт.

Якщо в пакеті даних з'являються поспіль шість "1", то щоб не втратити синхронізацію приймача вставляють "0", який вважається синхробітом. Тобто, "0" після шести "1" не є бітом даних та програмним рівнем ігнорується.

Рахунок одиниць починається з поля SYNC, тобто з одиниці наявної в цьому полі. Синхробіти не прив'язані до байтів, вони враховуються у всій бітової послідовності пакета. Вставка біта здійснюється завжди, без винятку.

Якщо за правилами потрібно вставка біта, нульовий біт буде вставлений, навіть якщо це - останній біт, тобто біт перед сигналом кінець-пакета (EOP).

Недоліки синхронізації з NRZI:

1 В пакеті з'являються байти завдовжки в 9 біт.

2 Кожний Stuff біт затримує залишок пакету на час рівний інтервалу біта. Тому різні пакети передаються з різним часом затримки.

3 Пакети стають плаваючої довжини.

З рис. 2.5 видно, що початкове положення Idle для FS і LS мають різний знак, тому перший біт синхробайта повинен змінити початкове положення на протилежне, інакше ми б втратили значення першого біта. Таким чином видно, що кодування NRZI для FS і LS різняться.

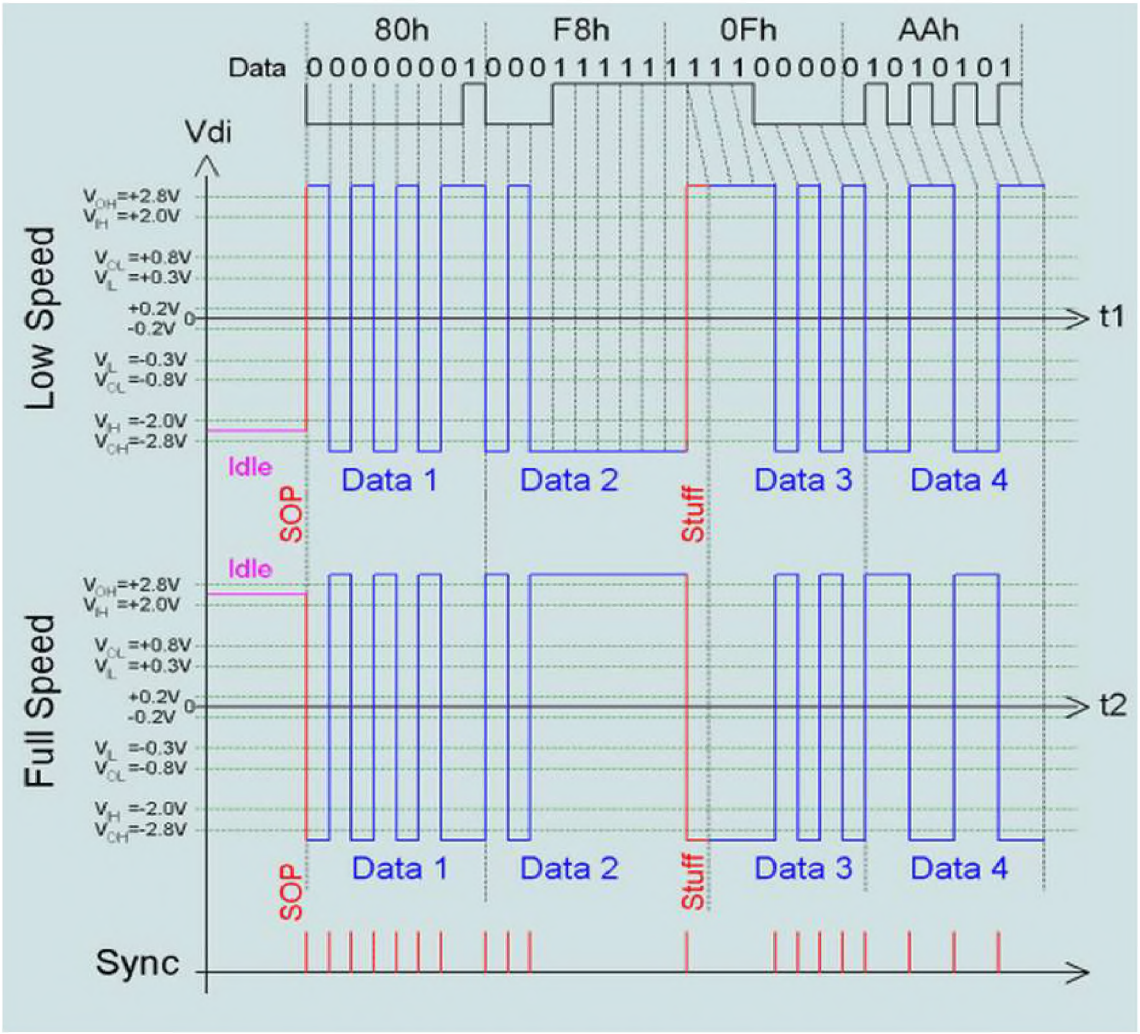


Рисунок 2.5 - Синхронізація пакету даних USB

2.2.2 Сигнали, що генеруються у USB-інтерфейсі

1 D+D- = 00

SE0 (Single-ended 0) - стан лінії "однополярний нуль". Це стан коли обидві лінії закорочені генератором драйвера за сигналом SE0 (див. рис. 2.3) або коли до шини не підключений Upstream драйвер. Цей стан використовується для генерації сигналів: EOP, Disconnect, Reset

2 EOP (End-of-Packet) - сигнал кінець пакету. Цей сигнал подається в лінію зв'язку в кінці кожного пакету даних. Він служить для розділення пакетів даних в часі. Після стану SE0, який триває протягом двох бітових інтервалів 160нс .. 175нс (Full Speed) або 1,25 мкс .. 1,50 мкс (Low Speed) передається сигнал протягом 1 біта. Після чого може бути передано новий пакет або шина перейде у стан Idle.

3 Disconnect-сигнал від'єднання Upstream від Downstream порту, визначається на Downstream. Цей сигнал фіксується на Downstream порту, коли Upstream драйвер подав сигнал SE0 або був фізично від'єднаний від шини USB. При фізичному від'єднанні низький рівень лінійних сигналів забезпечують підтягує резистори драйвера Downstream RPD = 15кОм.

4 Reset - сигнал скидання шини. Це сигнал генерується після сигналу Disconnect, воно ініціалізує перезапуск опитування пристроїв USB.

5 D+D- = 01/10.

6 Idle - вільний (незайнятий) стан лінії зв'язку. Це стан коли до порту Downstream підключено пристрій та обміну даними не проводиться.

За допомогою цього стану генеруються сигнали: Connect, Suspend.

Connect - сигнал з'єднання пристрою з Downstream портом. Цей сигнал повідомляє Downstream порту, що до нього підключено пристрій.

7 Suspend - сигнал призупинення обміну даних по шині. Цей сигнал повідомляє пристрою, що обмін даних з ним призупинено. Відновлення роботи здійснюється виставленням сигналу Resume.

8 Диференційний "1" - стан високого рівня сигналу на лінії зв'язку.

9 Диференційний "0"-стан низького рівня сигналу на лінії зв'язку.

За допомогою цих станів генеруються сигнали: J, K, Resume, SOP

J - сигнал J (Jump), повернення лінії зв'язку до рівня вихідного стану (Idle)

Сигнал визначається:

Low Speed: стан диференційний "0"

Full Speed: стан диференційний "1"

K - сигнал K (Kill), скидання вихідного (Idle) рівня стану лінії зв'язку.

Пристрій може перебувати в режимі припиненого обміну даними (Suspend), вихід з цього режиму здійснюється подачею сигналу Resume, після якого обмін даними поновлюється.

SOP - сигнал (Start of Packet) початок пакету.

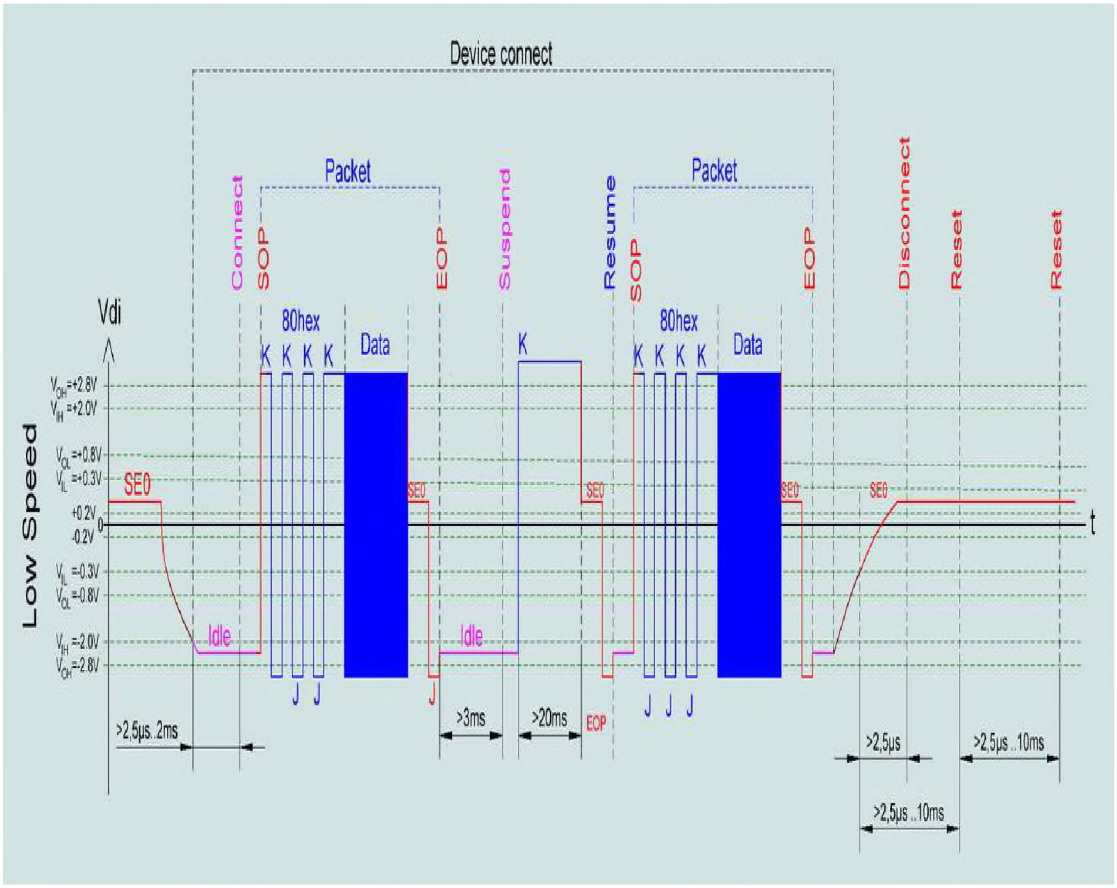


Рисунок 2.6 - Сигнали та стани лінії зв'язку

2.2.3 Аналіз передачі даних пакетами від USB-інтерфейсу до флеш-накопичувача

Передача даних від USB інтерфейсу до флеш-накопичувача здійснюється пакетами. Початок пакета визначається за сигналом SOP (Start of Packet), це перехід зі стану Idle в стан K. Далі йде байт синхронізації SYNC (80hex), який після NRZI кодування має вигляд KJKJKJKK. Останніх два біти SYNC-KK є маркерами початку блоку даних.

Блок даних складається з полів різної довжини, сумарна довжина блоку даних повинна бути кратна 8 бітам.

Байти передаються у порядку черги, починаючи з молодшого біта і закінчуючи старшим бітом. Структура передачі даних пакетами представлена на рис. 2.7, 2.8.

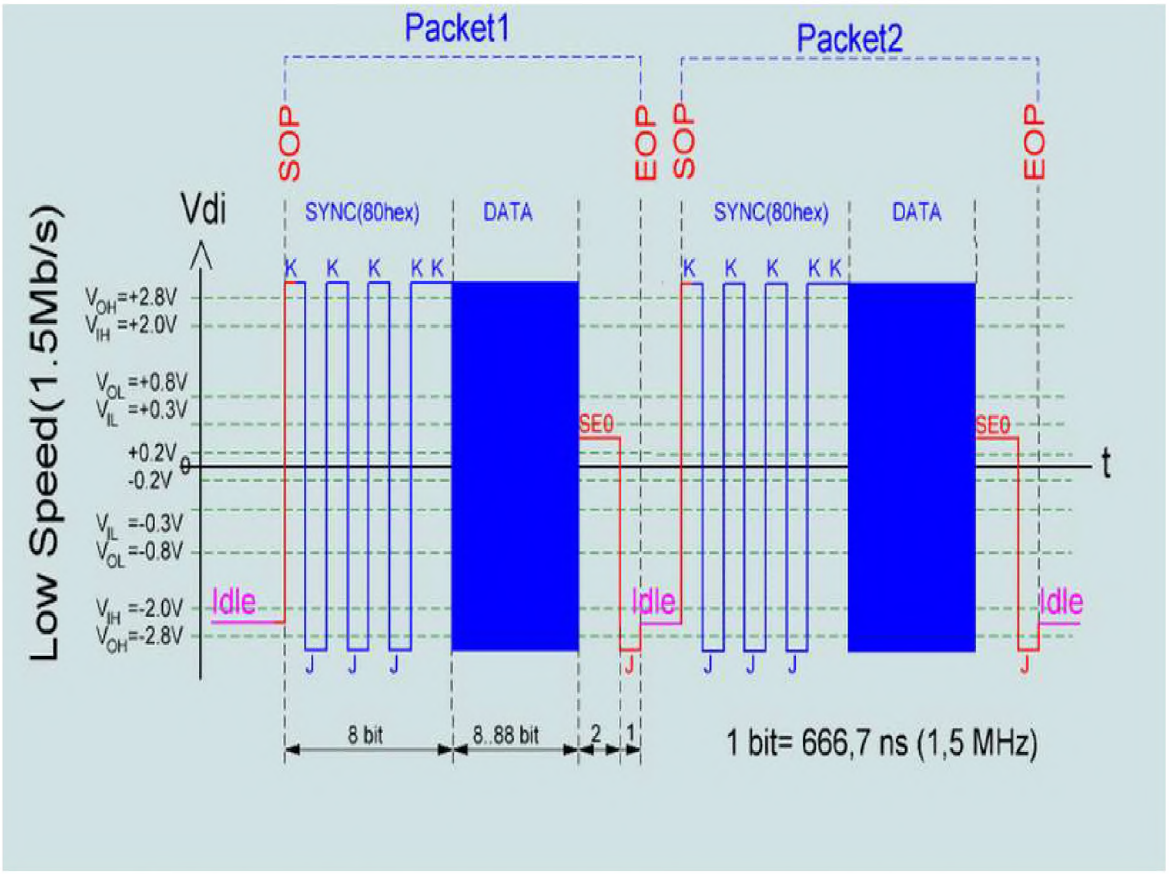


Рисунок 2.7 - Схема пакета Low Speed USB (1.5 Mb/s)

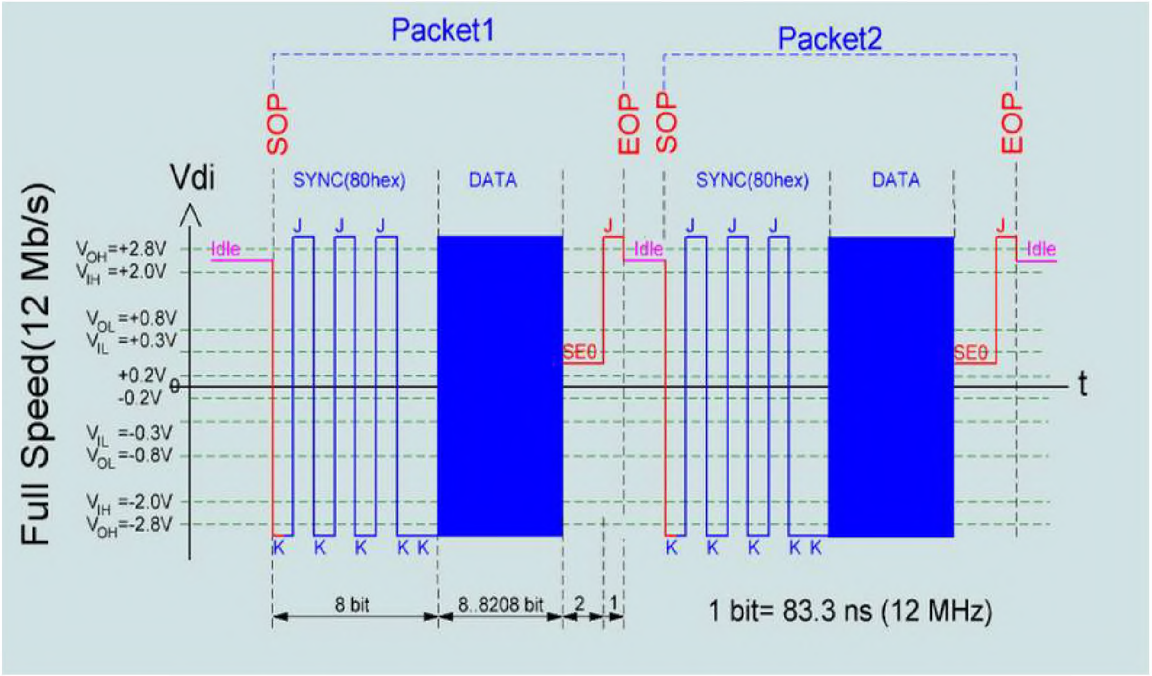


Рисунок 2.8 - Схема пакета Full Speed USB (12 Mb/s)

Закінчується пакет сигналом EOP (End of Packet) тривалістю 3 біти, який є тимчасовим роздільником пакетів.

Після аналізу структури, типів сигналів USB-інтерфейсу, принципів передачі, кодування даних, необхідно обрати обладнання, яке необхідно використовувати для проведення експериментальних досліджень по виявленню ПЕВМ. До такого обладнання відносяться автоматизовані пошукові комплекси.

2.3 Обґрунтування вибору апаратури для проведення експериментальних досліджень

Порівняна скритність добування інформації за рахунок перехоплення інформативних ПЕМВН, постійне вдосконалення техніки перехоплення і алгоритмів виділення інформативних сигналів змушує фахівців проводити спеціальні дослідження технічних засобів для виявлення та інструментального контролю інформативних ПЕМВ.

Необхідність виділення ПЕМВ на тлі сторонніх сигналів завад пред'являють жорсткі вимоги по частотній вибірковості апаратури та

динамічному діапазону рівнів аналізованих сигналів. До такої апаратури належать скануючі приймачі.

2.3.1 Скануючі приймачі

За габаритними показниками і функціональним можливостям скануючі приймачі можна умовно розділити на переносні і транспортовані. До переносних відносяться малогабаритні апарати масою більше 350 г, які мають автономні джерела живлення. Ці прилади в діапазоні частот 100 (500) Гц ... 1300 (1900) Мгц здійснюють прийом сигналів з амплітудною (AM), вузькосмугової (NFM) або широкосмугової (WFM) частотної модуляцією. Деякі зразки реєструють сигнали односмуговою AM (SSB), що передаються на частотах верхньої бічної смуги (USB) або нижньої бічної смуги (LSB), а також радіотелеграфні посилки (CW). При прийомі з відношенням сигнал / шум 10 дБ/мкВ чутливість сканерів складає 0,35 ... 1мкВ для NFM і 1 ... 6 мкВ для WFM. При кроці перебудови від 50 ... 500 Гц до 50 ... 1000 кГц швидкість сканування досягає 20 .. .30 каналів в секунду.

Відомості про частоту сигналів фіксуються в пристроях пам'яті ємністю від 100 до 1000 незалежних каналів. Окремі апарати управляються ПЕОМ.

Транспортовані приймачі, що відрізняються габаритами і масою, яка досягає 8 ... 20 кг, володіють значно більшими можливостями, майже всі зразки керуються від ПЕОМ.

Для скануючого приймача характерні високі реальна чутливість і вибірковість, використання методів, що забезпечують стійкість і надійність в умовах впливу сильних імпульсних, флуктуаційних і зосереджених по спектру завад.

Скануючий приймач відноситься до першої групи цифрових радіоприймальних пристроїв. Типи радіоприймальних пристроїв наведені у таблиці 2.1

Таблиця 2.1 – Типи радіоприймальних пристроїв

Тип пристрою	Наявність преселектора	Ширина смуги пропускання	Відображення спектрів	Наявність калібрування	Наявність демодулятора	Вимірювання параметрів сигналів
Скануючий радіоприймач	Так	Визначається смугами сигналів, для прийому яких призначений приймач (від сотень Гц до сотень кГц)	Зазвичай немає	Ні	Так	Ні
Селективний мікровольтметр	Так	Настроюється (від сотень Гц до сотень кГц)	Зазвичай немає	Так	Бажано	Так
Аналізатор спектру	Зазвичай немає	Зазвичай настроюється	Так	Так	Бажано	Так
Панорамний радіоприймач	Так	Широка. Зазвичай від сотень кГц до десятків МГц	Так	Ні	Так	Так
Панорамний радіоприймач	Так	Настроюється (від десятків Гц до десятків МГц)	Так	Так	Так	Так

Необхідною умовою отримання достовірних результатів спеціальних досліджень є застосування спеціальної вимірювальної апаратури, що забезпечує високу точність і повторюваність результатів вимірювань з плином часу і в різних умовах її експлуатації. До такої апаратури відносять автоматизовані комплекси. Сучасний вимірювальний комплекс неможливий без включення до його складу ПЕОМ, що забезпечує недосяжний іншими шляхами рівень продуктивності і сервісних можливостей апаратури.

2.3.2 Автоматизовані пошукові комплекси

Жорстким вимогам щодо чутливості та частотної вибірковості, які пред'являються до апаратури при дослідженнях ПЕОМ, відповідає досить вузьке коло вимірювальних приладів. В даний час для проведення дослідження ПЕМВ допустимо використовувати тільки такого комплексу апаратури, основу якого складає вимірювальний приймач або аналізатор спектру з набором відповідних вимірювальних антен.

Незважаючи на спільність принципів роботи, з усього розмаїття РПУ, що використовуються в даний час для вирішення завдань радіомоніторингу, можна виділити кілька характерних видів, наведених у табл. 2.2.

Пошукові вимірювальні комплекси останнім часом набувають особливої важливості у зв'язку з необхідністю вимірювання та аналізу небезпечних сигналів від засобів обчислювальної техніки (ЗОТ). Пов'язано це, перш за все, з тим, що ефірні і дротяні сигнали від ЗОТ носять специфічний характер. Імпульсні і не строгоперіодичні сигнали від ЗОТ з крутими фронтами і квазівипадковою змінною тривалістю утворюють широкосмугові шумоподібні та структуровані спектри випромінювань, а характерні для ЗОТ пачки імпульсів з неперіодичною прогальністю між пачками при паузах у межах 0,5-12 секунд утворюють спектри ПЕМВ з максимумами спектральної щільності в частотних діапазонах слабо корельованих з частотами, що утворюють спектри окремих імпульсів входять до пачки, а це ускладнює прогноз визначення небезпечних ділянок частотного діапазону, в якому поява небезпечних сигналів видається найбільш імовірним. Безсумнівні переваги автоматизованих комплексів (АК) в порівнянні з іншими способами і засобами виявлення і вимірювання ПЕМВН. До цих переваг відносяться, перш за все:

– оперативність процедур виявлення і вимірювання небезпечних сигналів;

– знижена ймовірність "пропуску" небезпечних сигналів, особливо при радіомоніторингу об'єктів інформаційної діяльності (ОІД);

– висока ергономічність (продуктивність) проведення пошуково-вимірювальних заходів, процедур обробки та документування отриманої при вимірах інформації.

Актуальним залишається питання оцінки достовірності отриманих результатів при пошукових і вимірювальних роботах, особливо при визначенні характеристик і рівнів небезпечних сигналів у межах частотної панорами безлічі сигналів і шумів, а також надійної повторюваності проведених вимірювань незалежно від різних факторів. До таких факторів належать:

- необхідність застосування декількох режимів вимірювань (крок перебудови за частотою, ширина частотної смуги перегляду, смуга пропускання вхідних каскадів вимірювача або смуга пропускання детектора, час вимірювання в точці і т.п.), що саме по собі вимагає оперативності у зміні цих режимів при пошукових роботах по поточних контекстним ознаками;

- поточна радіообстановка на ОІД на якому функціонує ЗОТ;

- кліматичні чинники, що впливають на вимірювально-пошукову апаратуру, дестабілізуючи її характеристики;

- фактор стабільності параметрів вимірювальних трактів залежно від часу;

- фактор відповідності програмного забезпечення (ПО) АК нормативно-методичній базі;

- фактор сумісності особливостей вимірюваних сигналів з характеристиками вхідних фільтрів, детекторів вимірників, способу детектування і часу вимірювання в точці.

Важливим напрямком діяльності автоматизованих пошукових комплексів є: постійний або періодичний контроль завантаження радіодіапазону, виявлення та аналіз нових випромінювань, оцінка їх небезпеки для установи, виявлення потенційних і спеціально організованих радіоканалів витоку інформації.

Кожне з цих завдань багатоетапне, вирішується в умовах складної електромагнітної обстановки як на об'єктах, так і на виїзді, і вимагає широкої номенклатури спеціальних технічних засобів. Автоматизовані пошукові комплекси забезпечують:

– виявлення за мінімальний інтервал часу пристроїв активного знімання акустичної інформації та визначення їхнього місця розташування;

– панорамний аналіз широкого діапазону частот у реальному масштабі часу в умовах складної електромагнітної обстановки, оцінку параметрів випромінювань, адаптацію до навколишнього радіообстановки, виявлення та аналіз її змін;

– протоколювання (реєстрацію) протягом тривалого часу амплітудно-частотно-часового завантаження досліджуваного діапазону з прив'язкою до реального часу;

– статистичний аналіз зареєстрованих даних завантаження діапазону з можливістю протоколювання інтегральних показників по кожному радіоканалу (джерелу), порівняння з базами даних і виявлення кореляційних частотно-часових взаємозв'язків між радіоканалами.

Для вирішення перерахованих завдань останнім часом все частіше використовуються автоматизовані програмно-апаратні комплекси ближньої радіорозвідки, які дозволяють автоматизувати вельми трудомісткі операції з виявлення, ідентифікації локалізації джерел несанкціонованого радіовипромінювання. У простому випадку такий комплекс може складатися з стандартного скануючого приймача, керованого ПЕОМ, що працює під управлінням спеціального ПЗ. Більш складні системи також побудовані на базі керуючої ПЕОМ, скануючого приймача і різних додаткових блоків.

Перевагами таких комплексів є порівняно невисока вартість, модульна організація апаратної частини, що допускає просту модернізацію (заміна окремих функціональних блоків). Мала вага і порівняно невеликі габарити в поєднанні з універсальним живленням (220В, 12В) і вбудованими

акумуляторними батареями дозволяють експлуатувати комплекси як в стаціонарних, так і при умовах, коли комплекс необхідно багаторазово переносити. Початковим етапом функціонування автоматизованого програмно-апаратного комплексу є адаптація до навколишньої електромагнітної обстановки. На даному етапі автоматично формується так званий «файл зразку», в який заноситься амплітудно-частотне завантаження робочого діапазону поза контрольованого приміщення. Виконання даної операції дозволить згодом значно прискорити виявлення і аналіз «невідомих» сигналів в контрольованому приміщенні. У таблиці 2.2 представлені найпоширеніші комплекси та їх характеристики.

Таблиця 2.2 – Характеристики автоматизованих пошукових комплексів

Хар-ки\АК	"НАВІГАТОР"	"АСТРА-В"	"АКОР-ПК"	"ТИКОС-18"
Базовий прилад	Аналізатор спектра E4411B	Аналізатор спектра E4402B та аналогічні	РПУ AR-5000	РПУ AR-5000
Діапазон частот панорами	9 кГц - 1 ГГц (базовий варіант)	до 26 ГГц	10 Гц - 1 ГГц	100 кГц-2,6 ГГц
Шкала вікон перегляду (смуг пропуску.)	1;3;10;30;100; 300 кГц; 1;3 МГц	1;3;10;30;100; 1000 Гц;1;3;10; 30;100;300; 1000 кГц; 1;3;5 МГц.	44 кГц и 3;6;15;30;110; 220 кГц	12,5 и 200 кГц на виході 2 ПЧ приймача при кроці перебудови 8 Мгц.
Точність вимірювання рівня ПЕМВ	±2% + точність калібрування антен	±2% + точність калібрування антен	±2 дБ + точність калібрування антен	-

Сучасні технології пошуку та вимірювання ПЕМВ реалізовані в таких комплексах, як "АКОР-ПК", RS-1100 і RS-1200 (комплекс для пошуку закладних пристроїв), "АСТРА-В", "НАВІГАТОР". Кожний з цих автоматизованих комплексів має свої особливості та переваги у вирішенні специфічних задач: пошук закладних, вимірювання рівня ПЕМВ від ЗОТ, моніторинг ефіру і т.і.

Цифровий вимірювач побічних електромагнітних випромінювань реалізований на основі автоматизованого вимірювача АКОР-1ПК і являє собою аналізатор спектру і високочутливий селективний вимірювальний приймач для частотного діапазону від 10 Гц до 1000 МГц. Після аналізу автоматизованих пошукових комплексів, для проведення експериментальних досліджень був обраний саме цей комплекс. АКОР-2ПК має всі необхідні технічні характеристики і задовольняє вимогам для проведення досліджень у пошуку та вимірюванню ПЕВМ. Комплекс є розробкою Українського науково-технічного центру "КВАНТ" і є сертифікованим на території України.

Рисунок 2.9 - Зовнішній вигляд комплексу АКОР-2ПК

2.4 Аналіз параметрів сигналів, що підлягають вимірюванню

Формулювання завдання перехоплення в методичних документах однозначне - розпізнавання одного двійкового розряду. При цьому противнику доступна для здійснення цього завдання енергія ПЕМВ в усьому встановленому діапазоні частот (10 Гц - 1000 МГц).

Звідси виходить, що і реєстрації (вимірюванню) підлягають всі частотні складові сигналу ПЕМІ в цьому діапазоні, що мають ознаки інформативності. Відповідно до методичних документів такими вважаються такі складові ПЕМВ, амплітуда яких зазнає змін при зміні переданої інформації. У класичному випадку - при переході від «0» до «1» або навпаки. Ця зміна, як правило, пов'язана не з реальною зміною енергії ПЕМВ, а з перерозподілом її по спектру. Енергія випромінювання, в загальному випадку, не залежить від

полярності інформаційного імпульсу або напрямку переходу потенціалу (чим і кодується «0» або «1» в ланцюгах цифрових пристроїв). Розглядаючи вузькосмуговий засіб вимірювання як еквівалентний LC ланцюг можна визначити його постійну часу як величину, зворотню смузі пропускання.

$$\tau = \frac{1}{F_{пр}}, \tag{2.1}$$

де $F_{пр}$ – смуга пропускання засобу вимірювання в Гц.

За час, більший 3-5τ, перехідний процес на виході такого ланцюга вважається кінцевим. Таким чином, якщо послідовність інформаційних імпульсів з постійною тактовою частотою проходження неперервна протягом такого або більшого проміжку часу, послідовність може вважатися нескінченною. Отримане за цієї умови значення амплітуди буде істинним піковим значенням.

Ця залежність підтверджується у всіх випадках. Так, наприклад, у випадку дослідження USB інтерфейсу ПЕОМ та тест-режиму у вигляді послідовності імпульсів з шпаруватістю 2 (тобто меандру) при смузі пропускання засоби вимірювання близько 10 кГц (найбільш часто застосовувана) необхідна тривалість безперервного пакета не менше:

$$T \geq 5\tau = 5 \cdot \frac{1}{1 \cdot 10^4} = 5 \cdot 10^{-4} c, \tag{2.2}$$

тобто не менше 500 мкс.

Формування тест-сигналу (тест-режиму) не у вигляді безперервної послідовності, а, як правило, у вигляді послідовності досить протяжних пакетів імпульсів, призводить до появи бічних частот. Спектр сигналу ПЕМВ набуває вигляду:

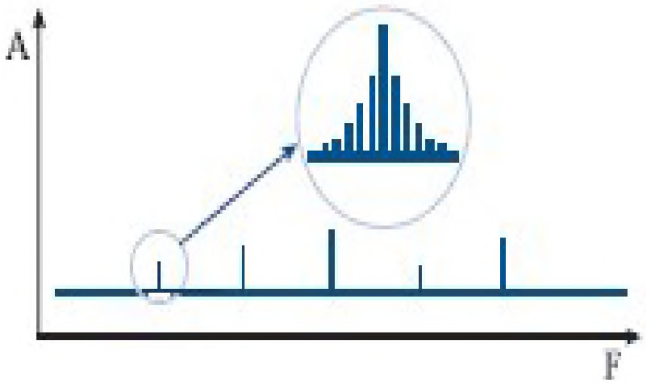


Рисунок 2.10 - Типовий спектр ПЕМВ

Всі складові такого спектру є інформативними і повинні бути виміряні. Це можливо виконати двома способами:

- вимірювання досить широкої смуги пропускання засобу;

- вимірювання, щоб одночасно виміряти енергію не тільки основної частоти (гармоніки), кратній тактовій частоті, але і всі її бічні складові (частоти);

- роздільним виміром кожної складової спектру, включаючи бічні частоти.

У даному випадку також необхідно встановити практичні обмеження.

Враховуючи, що в установленому методі розрахунку, проводиться підсумовування квадратів складових спектру, має сенс враховувати лише ті бічні частоти, амплітуда яких не більше, ніж на 13-16 дБ менше від центральних частот. Вимірюючи USB-інтерфейс ПЕОМ зазвичай для вимірів за першим варіантом необхідна смуга пропускання 100-500 кГц. Але в цьому випадку вірогідна значна помилка за рахунок завданих, неінформативних сигналів, що потрапляють в таку широку смугу пропускання.

Таким чином, оптимальним є уважне і акуратне вимірювання кожної складової окремо.

2.5 Обґрунтування вибору методу виявлення інформативних складових ПЕМВ

Існує принципова різниця між виявленням побічного електромагнітного випромінювання в цілому і пошуком інформативних складових ПЕМВ.

Вирішити перше завдання з цілком прийнятною якістю можна на основі простого порівняння усереднених спектрів. Для цього необхідно в контрольованому діапазоні частот провести усереднення спостережуваних спектральних оцінок спочатку при вимкненому тестовому обладнанні, а потім повторити накопичення спектральних даних, включивши обладнання, що перевіряється, і встановивши активний (тестовий) режим. Виявити ж інформативні складові ПЕМВ подібним чином важко, особливо якщо тестування проводиться в недостатньо екранованому від зовнішніх ЕМП

приміщенні. Справа в тому, що накопичення даних займає досить великий інтервал часу, протягом якого «зовнішня» радіообстановка майже напевно буде змінюватися. Це породжує проблему відділення змін, викликаних зміною режиму роботи тестованого обладнання, від змін, породжуваних зовнішніми причинами.

Кореляційні методи, що успішно використовуються для виявлення слабких електромагнітних випромінювань складної форми, застосувати до пошуку інформативних складових ПЕМВ вельми проблематично. Це пов'язано з тим, що в якості еталонних сигналів повинні використовуватися власні сигнали тестованої апаратури, які відомі лише приблизно та мають низьку інтенсивність і можуть істотно змінюватися від одного примірника апаратури до іншого.

Дослідження інформативності сигналів ПЕМВ істотно спрощується, якщо є можливість у ході тестування багаторазово змінювати поточний режим роботи апаратури, що перевіряється. При такому підході критерієм інформативності служить виявлення взаємозв'язку між режимом роботи тестованого пристрою і спостережуваним розподілом потужності спектральних складових по частотах. Конкретні методи виявлення такого

взаємозв'язку залежать від характеристик комплексу радіомоніторингу, використовуваного для тестування. Для апаратури з низькою спектральною роздільною здатністю можлива робота з двоетапним алгоритмом, розглянутим нижче. Перший етап служить для виявлення всіх ПЕМВ обладнання, що перевіряється, він базується на порівнянні накопичених спектрів, спочатку в досліджуваному діапазоні частот проводять усереднення спостережних спектральних оцінок при пасивному режимі роботи обладнання, що перевіряється. Потім накопичення спектрів повторюють, переключивши обладнання, що перевіряється, у тестовий режим. У результаті зіставлення отриманих даних вдається виділити сукупність частот, що складають ПЕМВ та підлягають перевірці на інформативність. Зазначимо, що для запобігання пропусків слабких складових ПЕМВ на цьому етапі слід
вважати значущими навіть малі (одиниці децибел) відхилення інтенсивностей відліків спектру. Разом з тим використання подібного низького порогу виявлення неминуче призводить до істотного зростання кількості частот, що заносяться до списку перевірки на інформативність.

Метою другого етапу є перевірка інформативності всіх підозрілих частот. Ця перевірка може здійснюватися оператором «на слух» з використанням того чи іншого набору демодуляторів або автоматично за рахунок почергової вузькосмугової обробки внесених до списку складових ПЕМВ. Критерієм інформативності служить виявлення взаємозв'язку між режимом роботи тестованого пристрою і спостережуваним розподілом потужності спектральних складових. Результативність другого етапу залежить від набору демодуляторів, застосовуваних при вузькосмуговій обробці, причому визначити заздалегідь, який саме демодулятор виявиться ефективним для виявлення інформативності, вельми проблематично.

Для підвищення достовірності бажано використовувати всі наявні демодулятори і впродовж багатьох циклів перевіряти наявність або відсутність взаємозв'язку між режимом роботи тестованого пристрою і

спостережуваним розподілом потужності по частотах на виході кожного з демодуляторів.

Описана двоетапна процедура працездатна і забезпечує надійне виявлення інформативних ПЕМВ, проте вона має низьку швидкодію. Більш того, необхідні великі витрати часу на обробку отриманих результатів ,які можуть змінюватися, так що навіть за наявності швидкодіючої апаратури перевірка конкретного пристрою може тривати кілька днів. Однак для апаратури радіомоніторингу з низькою спектральною роздільною здатністю. Подібна методика виявляється, практично, єдиною можливою. Надалі ця методика буде називатися TOP-алгоритмом (тестування і виявлення роздільне) і буде використовуватися для проведення досліджень ПЕМВ флеш-накопичувачів.

2.6 Розробка порядку проведення спеціальних досліджень USB флеш-накопичувачів

Згідно з методикою наведеною в розділі (2.5.) виявлення небезпечних сигналів із загальної сукупності сигналів і вимірювання їх рівня проводиться при спеціально організованих тестових режимах USB флеш-накопичувачів, при яких тривалість і амплітуда інформаційних імпульсів залишаються тими ж, що і в робочому режимі, але використовується періодична імпульсна послідовність у вигляді пачок.

Циклічне повторення одних і тих же «пакетів» інформації дозволяє за рахунок накопичення енергії ПЕМВ у вхідних ланцюгах вузькосмугових засобів вимірювання (приймачі, спектроаналізатори і т.д.) значно простіше виявляти і вимірювати значення «небезпечних» сигналів на тлі шумів і завад.

Виявлення сигналу здійснюється з усіх боків флеш-накопичувача. Вимірювання сигналу проводиться в піковому (квазіпіковому) режимі у напрямі максимального випромінювання, де виявлено небезпечний сигнал. Для виявлення тест-сигналів і виявлення їх із загальної сукупності прийнятих

сигналів використовуються такі ознаки, як збіг частот виявлених гармонік і інтервалів між ними з розрахунковими значеннями, період і тривалість пачок, зміна форми сигналу на виході приймача при зміні параметрів тест-сигналу.

Вимірювання рівнів ПЕМВ проводиться лише після того, як підтверджено, що прийнятий саме тест-сигнал.

При проведенні вимірювань необхідно:

– вивчити технічний опис і принципові схеми ТЗ;

– вивчити можливі режими роботи ТЗ;

– підготувати вимірювальну апаратуру до роботи.

Вимірювання параметрів побічних електромагнітних випромінювань флеш-накопичувача здійснюється в усіх режимах його роботи. Заземлення і електроживлення повинні виконуватися відповідно до правил експлуатації даного ТЗ. Перед початком вимірювань флеш-накопичувач перевіряється на працездатність у відповідності з інструкцією по експлуатації.

Рекомендовані вимоги до приміщення, в якому проводяться спеціальні дослідження:

– приміщення, в якому проводиться вимірювання параметрів поля небезпечного сигналу, повинно мати розміри кімнати не менше 6 х 6 м (36 м^2);

– поблизу вимірюваного технічного засобу (ближче 2,5м), яке встановлюється в середині кімнати, не повинно бути громіздких металевих предметів (сейфів, шаф тощо), які можуть спотворювати картину ПЕМІ;

– настил підлоги приміщення може бути як дерев'яним (паркет), так і металевим;

– закони спадання поля в атестованому приміщенні мають відповідати стандартної функції ослаблення поля в межах 2 ... 2,5 м від ТЗ в напрямку установки вимірювальної антени.

Флеш-накопичувач встановлюється на поворотній тумбі, висотою 0,8 ... 1,0 м, живлення на системний блок ПК подається через фільтр типу ФП, загасанням не менше 40 .. .60 дБ. Для виключення впливу завад від мережі

електроживлення при вимірах необхідно застосовувати ноутбук, який працюватиме автономно від акумуляторної батареї.

Порядок проведення експериментальних досліджень

Для проведення досліджень необхідно дотримуватися всіх технічних вимог та проводити виміри згідно з наведеними нижче пунктами:

1 Обирається приміщення площею не менше 36 $м^2$ з дерев'яним покриттям підлоги, у якому немає металевих шаф, сейфів та інших предметів, які можуть спотворити показання виміру ПЕМВ в приміщенні.

2 Для проведення вимірювань необхідно застосовувати таке обладнання: осцилограф С1-93, персональний комп'ютер, два ноутбуки, автоматизований комплекс АКОР-2ПК та кільцевий струмознімач, широкосмугові активні антени SA-2A, SA-1, широкосмугову, дипольну вимірювальну антену «AI 5-0», якими комплектується комплекс АКОР-2ПК.

3 Обладнання необхідно встановити в центрі приміщення, а досліджувані флеш-накопичувачі встановити на поворотну тумбу висотою 1 м.

4 Знеструмити всі електричні і радіоприлади, які не застосовуються при проведені вимірювань.

5 Підібрати необхідні флеш-накопичувачі, які будуть досліджуватися і вивчити їх параметри.

6 Підготувати вимірювальне устаткування до роботи: включити автоматизований комплекс АКОР-2ПК на 30-40 хвилин прогріватися. Схема, склад та принципи роботи комплексу АКОР-2ПК наведенні у додатку В. Запустити необхідне програмне забезпечення, яке йде у комплекті з комплексом АКОР-2ПК.

7 На допоміжному комп'ютері запустити програму TestPC версії 2.05 для створення тестового сигналу (інтерфейс даної програми зображений на рис 2.11). Дана програма не цілком призначена для тестування флеш-накопичувачів , а є універсальною для різних технічних засобів. Аналогів даної програми у відкритому доступі не існує, тому є вимушена необхідність

використовувати тестовий сигнал, призначений для тестування жорстких дисків, для флеш-накопичувачів. Програма є сертифікованою і йде в комплекті з автоматизованим комплексом АКОР-2ПК. Тест-сигнал для дослідження флеш-накопичувача являє собою постійний посил пакетів даних різного типу на флеш-накопичувач. Такий посил пакетів створює сигнал інформативного випромінювання максимальної амплітуди із заданою частотою повторень, для максимально ефективного виявлення ПЕМВ флеш-накопичувачів.

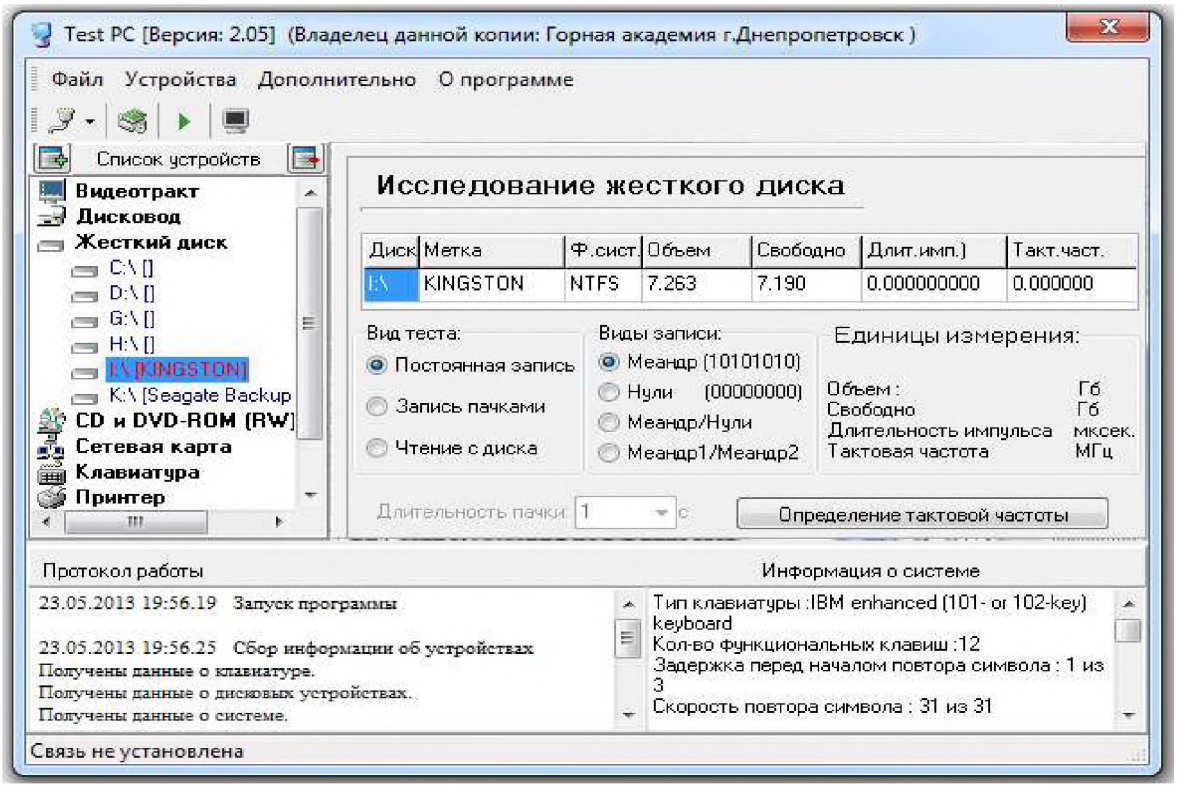


Рисунок 2.11 - Інтерфейс тестової програми "Test PC"

8 Розмістити досліджуваний флеш-накопичувач на поворотній тумбі і підключити його до допоміжного ПК.

9 Для вимірювання характеристик тестових сигналів, що надходять на флеш-накопичувач, необхідно до контактів USB інтерфейсу підключити осцилограф С1-93 за допомогою струмознімача, згідно зі схемою зображеної на рис. 2.12

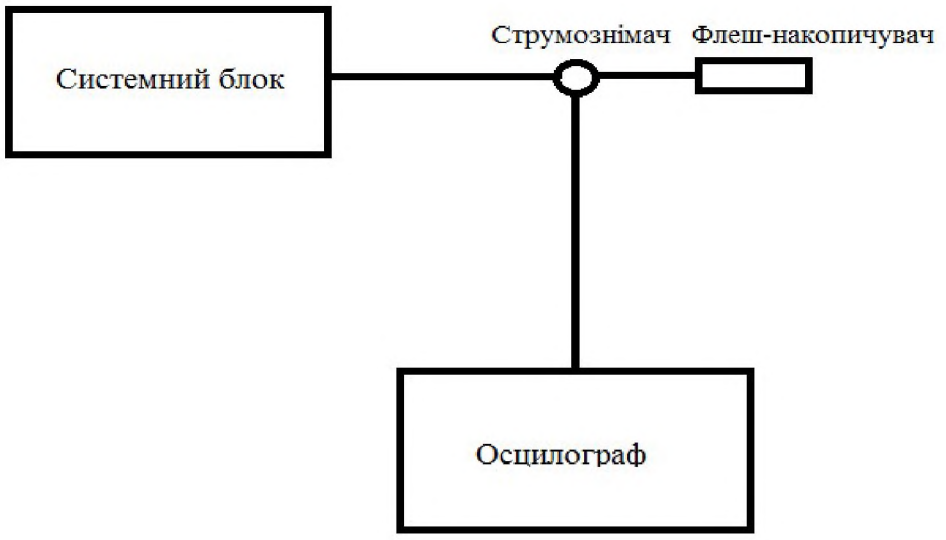


Рисунок 2.12 - Схема підключення осцилографа до флеш-накопичувача

10 Для пошуку та вимірювання ПЕМВ від флеш-накопичувачів, в інтерфейсі програмного забезпечення АКОР-2ПК необхідно вибрати модуль "майстер дослідження ПЕМВН". Усі наступні етапи вимірювань проводяться за допомогою даного модуля:

а) створюється список пристроїв, котрі підлягають дослідженню;

б) проводиться вибір способу пошуку ПЕМВ;

в) задається тип антени, яка буде використовуватися;

г) задаються параметри сканування (діапазон частот, смуга пропускання);

д) проводиться вимірювання фонової панорами. Сканування фону проводиться в середньому 5 разів, поки не буде встановлено, що всі сторонні частоти виявлені і відфільтровані для подальшого проведення вимірювань.

11 Для виявлення ПЕМІ від флеш-накопичувача до автоматизованого комплексу АКОР-2ПК в роз'єм ANT 2.1 підключається широкосмугова активна антена SA-2A з коефіцієнтом посилення 12 - 16 дБ, яка застосовується для прийому сигналів у ближній зоні. Схема підключення антени зображена на рис. 2.13. Після сканування фонової панорами, проводиться виявлення частот ПЕМІ від флеш-накопичувачів. Отриманий список частот

ідентифікується на наявність небезпечних сигналів згідно з методом ТОР (розділ 2.7)

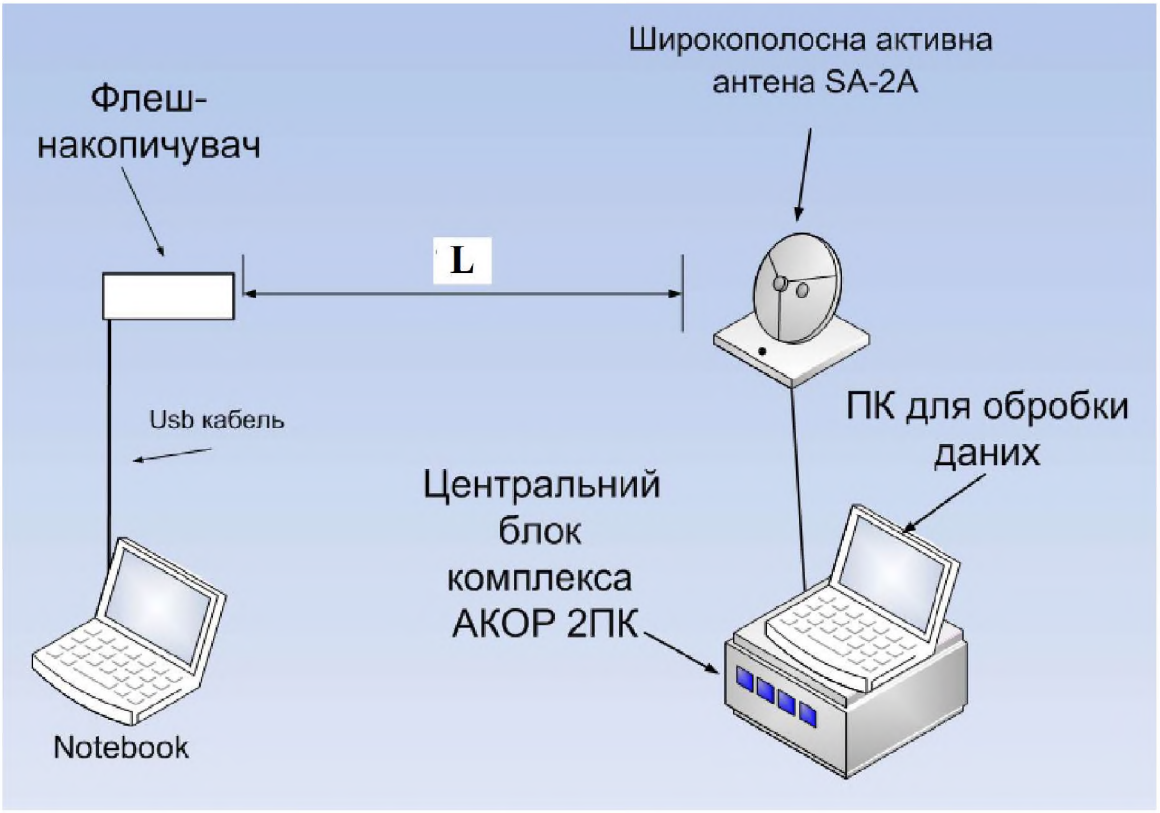


Рисунок 2.13 - Схема підключення широкополосної активної антени SA-2A

12 Для вимірювання рівня сигналу небезпечних частот до автоматизованого комплексу АКОР-2ПК в роз'єм ANT 1.1 підключається широкосмугова, дипольна вимірювальна антена «AI5-0» з робочим діапазоном частот 0,009 - 2000МГц, на відстані 1 м. від досліджуваного флеш-накопичувача, як представлено на рис. 2.14. Кожна частота в сформованому списку небезпечних частот вимірюється автоматично із заданою кількістю повторів вимірювання. Для більш точних результатів вимірювань необхідно встановити кількість повторів сканування рівня сигналу на рівні 5.

13 Отримані результати вимірювань заносяться до таблиць протоколів вимірювань і зберігаються.

14 Після проведення всіх необхідних вимірювань, необхідно закрити все програмне забезпечення, відключити досліджувані флеш-накопичувачі і допоміжне обладнання, після чого вимкнути автоматизований комплекс АКОР-2ПК.

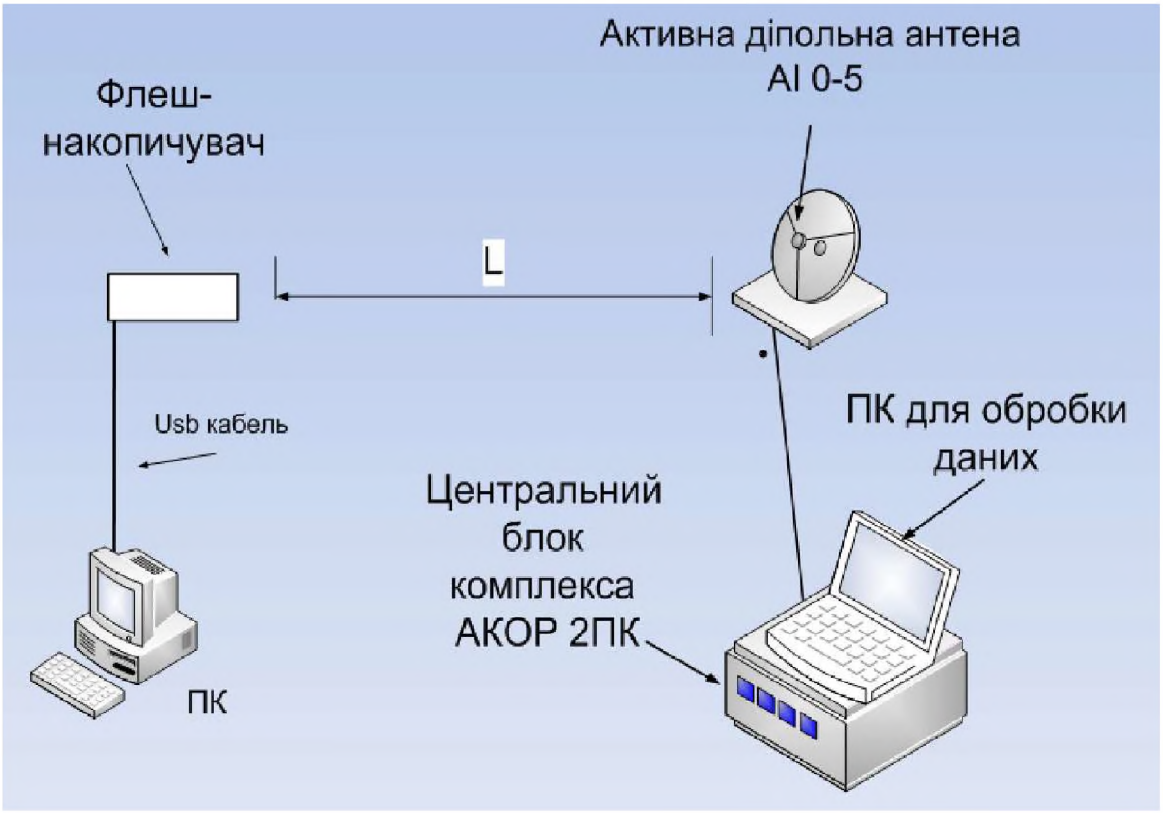


Рисунок 2.14 - Схема підключення активної дипольної антени AI-05

2.7 Дослідження сигналів, що надходять з USB інтерфейсу на флеш-накопичувач

Дослідження проводилися згідно порядку, описаному в розділі 2.6. Для вимірювання характеристик тестових сигналів, що надходять на флеш-накопичувач, до контактів USB-інтерфейсу був підключений осцилограф С1-93 за допомогою струмознімача (рис. 2.15) При вимірах осцилографом на досліджуваний флеш-накопичувач подавалися пакети інформації, що містили тестові сигнали типу "Меандр" і "нулі ". Параметри отриманих сигналів вимірювалися з використанням часових характеристик розгортки сигналу і положень перемикача вхідного дільника осцилографа С1-93. Результати вимірювань представлені на рис. 2.16 і 2.17.

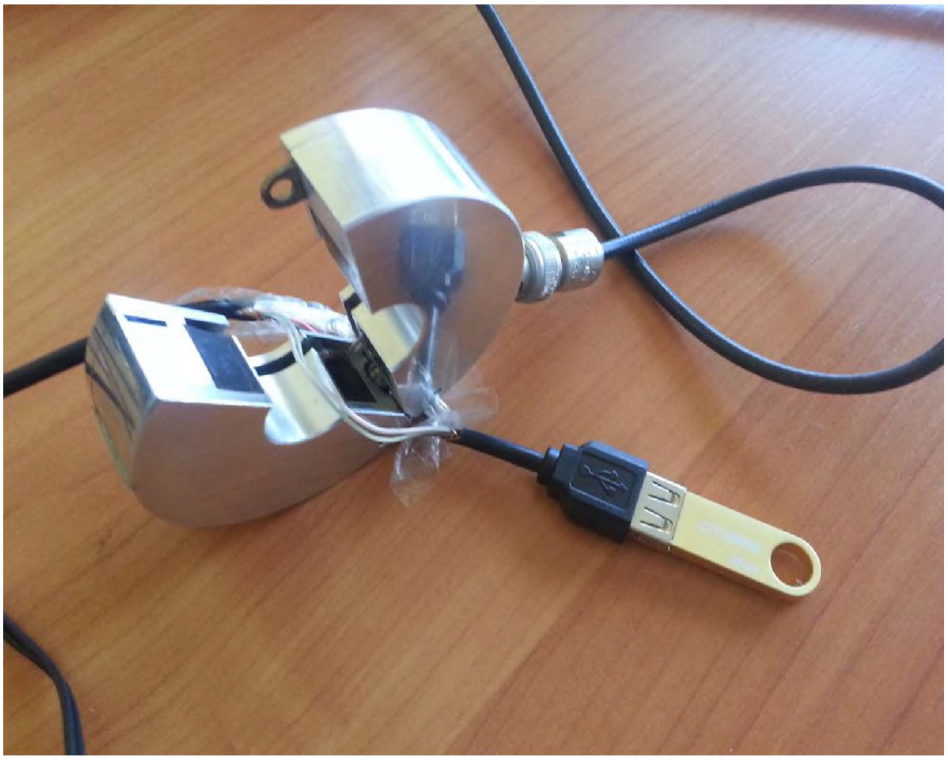


Рисунок 2.15 - Підключення струмознімача до USB-інтерфейсу

Осцилограма сигналів при надходженні на флеш-накопичувач тестового сигналу "Меандр" (101010) зображена на рис. 2.16.

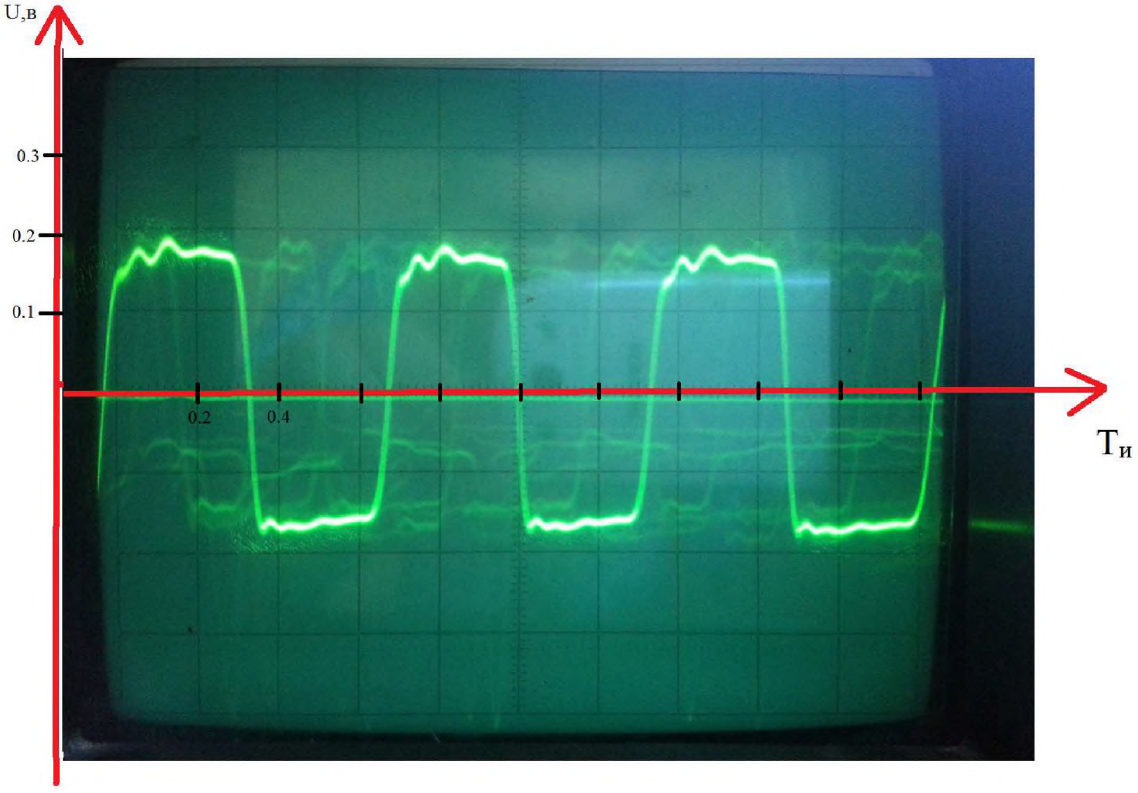


Рисунок 2.16 - Осцилограма тестового сигналу "Меандр"

При проведенні вимірювань перемикачі осцилографа були встановленні на наступні значення:

Положення вхідного дільника 0,01 В/діл.

Розгортка 0,2 мкс/діл.

На осцилограмі видно структуру імпульсу, викиди переднього фронту і невеликі викиди заднього фронту. За отриманою осцилограмою можна визначити тривалість імпульсу - τ_u, $T_и$ - період проходження імпульсів і амплітуду - U:

τ_u=3,3·0,2=0,66 (мкс),

$T_и$=1,4·0.2=0,28 (мкс),

U= 0,017 В.

Осцилограма сигналів при надходженні на флеш-накопичувач тестового сигналу "Нулі" (000000) зображена на рис. 2.17.

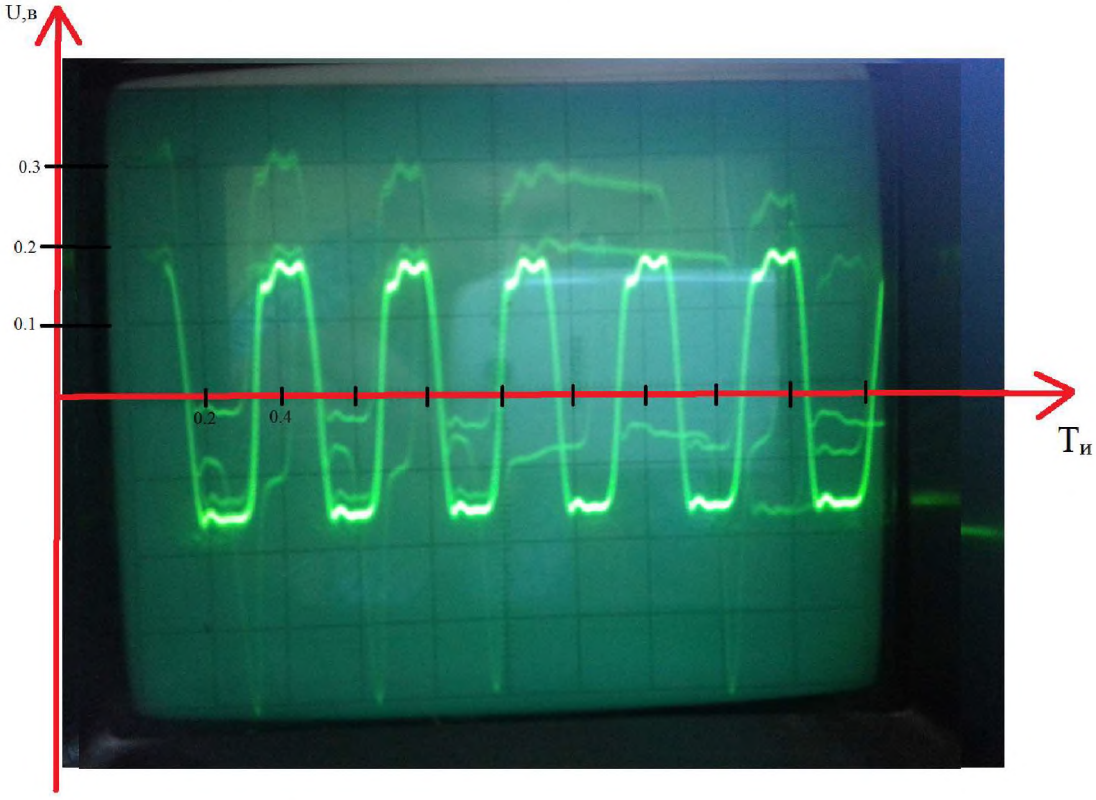


Рисунок 2.17 - Осцилограма тестового сигналу "нулі"

При проведенні вимірювань перемикачі осцилографа були встановленні на наступні значення:

Положення вхідного дільника 0,01 В/діл.

Розгортка 0.2 мкс/діл.

$\tau_и$=1,8·0,2=0,36 (мкс),

$T_и$=1·0,2=0,2 (мкс),

U= 0,018 В.

На осцилограмі чітко проглядається структура сигналу. Дані кодуються методом NRZI. Таким чином, при передачі нуля генератор змінює полярність сигнальної лінії на протилежну, при передачі одиниці полярність сигналу залишається попередньою. Порівнюючи отримані осцилограми можна спостерігати зміну полярності тестового сигналу "Нулі" (000000) у двічі частіше, ніж тестового сигналу "Меандр" (101010), що відповідає методу кодування NRZI.

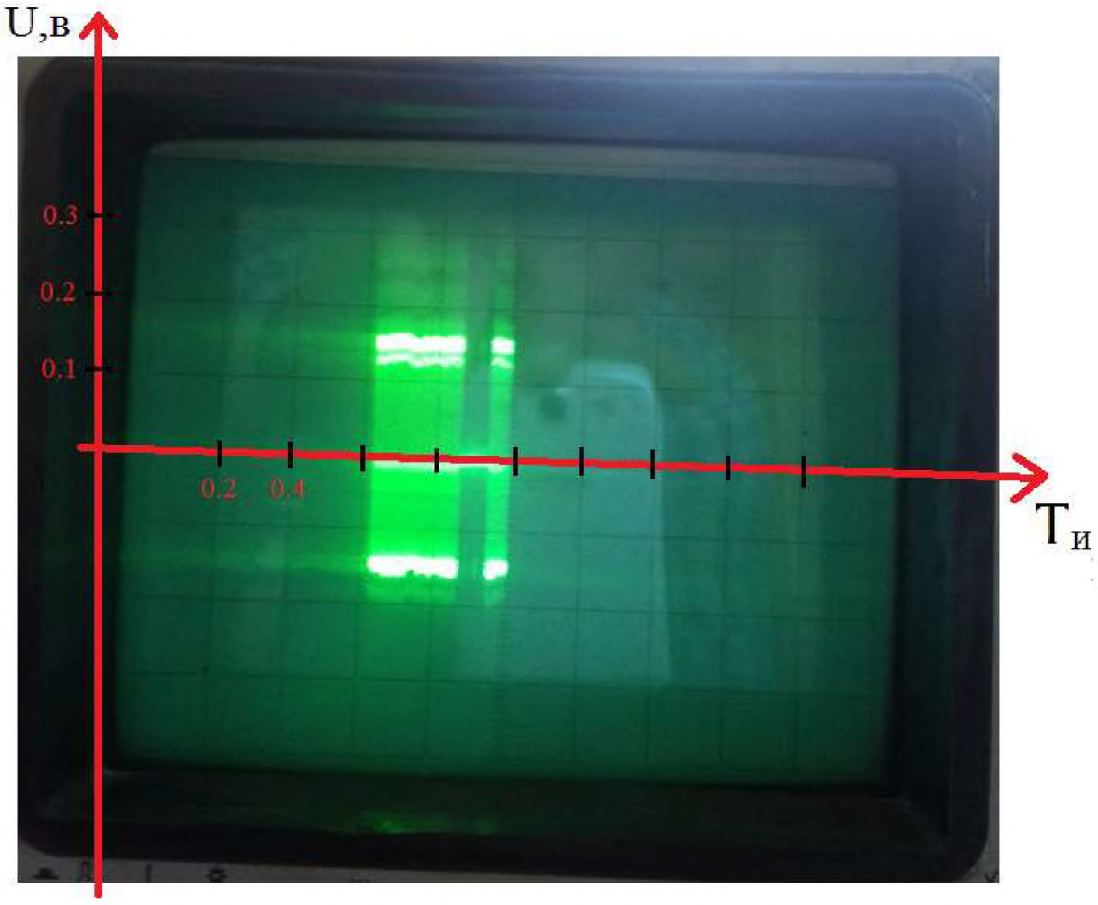


Рисунок 2.18 - Осцилограма пакету даних

При проведенні вимірювань перемикачі осцилографа були встановленні на наступні значення:

Положення вхідного ділителя 0,01 В/діл.

Розгортка 0.2 мкс/діл.

$T_и$=1,2·0,2=0,24 (мкс).

U= 0,018 В.

На даній осцилограмі видно структуру передачі даних пакетами, яка відповідає схемі, що приведена на рис. 2.7. Таким чином можна зробити висновок о наявності інформативної складової у сигналах, які передаються з USB інтерфейсу на флеш-накопичувач.

2.8 Проведення експериментальних досліджень ПЕМВ від флеш-накопичувачів

Дослідження проводилися за п.11-12 порядку, що описаний у п.2.6.

Для досліджень були обрані наступні види usb флеш-накопичувачів. Для проведення вимірювань по оцінці рівнів ПЕМВ при роботі флеш-накопичувачів були встановлені такі чинники, що впливають на рівень ПЕМ випромінювання:

- тип контролера флеш-накопичувача;
- кількість мікросхем пам'яті;
- тип застосовуваної файлової системи на флеш-накопичувачі;
- версія USB інтерфейсу;
- тип USB кабелю, що використовується при роботі з флеш-накопичувачем;
- тип матеріалу з якого виготовлений корпус флеш-накопичувача.

Отримані результати вимірювань залежності ПЕМВ від перерахованих вище факторів приведені в розділі 2.8.

Пошук ПЕМВ від флеш-накопичувачів виконувався згідно з алгоритмом, пункти 10,11.

Таблиця 2.3 Характеристики флеш-накопичувачів, що досліджувались

Модель	Kingston DTGE9	Kingston DT101G2	Transcend JetFlash T3K	Transcend JetFlash V85	EasyDisk ED722	Transcend JetFlash 770
Живлення, В	5	5	5			
Ємність, Гб	16/8	16/8	8			
Інтерфейс USB	2.0	2.0	2.0	2.0	2.0	2.0
Тип корпусу	мет.	пласт.	пласт.	мет.	резин.	пласт.
Номінальний струм, мА	125	100	125	125	15	125
Струм в режимі роботи	130	120	130	30	36	30
Тактова частота, Мгц	11.2	9.9	29	28	12	49
Розміри, мм	39,00 x 12,35 x 4,55	39,00 x 12,35 x 4,55	60 x 18.59 x 8.7	49.5 x 15.8 x 7.4	67 x 21 x 8	69.6 x 20.9 x 8.9

а) Список пристроїв, що досліджувалися був складений за таблицею 2.3;

б) Пошук ПЕМВ проводився за електричною складовою поля;

в) Застосовувалася антена SA-2A ;

г) Сканування проводилося в діапазоні від 1 до 300 МГц, смуга пропускання 500 кГц);

д) сканування фонової панорами проводилося не менше 5 разів. зразок сканування фонової панорами приведений на рис. 2.19

Після сканування панорами був проведений пошук частот ПЕМВ. Отримані частоти ідентифікувалися на наявність інформативної складової згідно з методом, описаним в розділі 2.7. Пошук ПЕМВ та ідентифікація небезпечних частот проводилися для кожного флеш-накопичувача. Результат ідентифікації небезпечних частот одного з досліджуваних флеш-накопичувачів представлений на рис. 2.20.

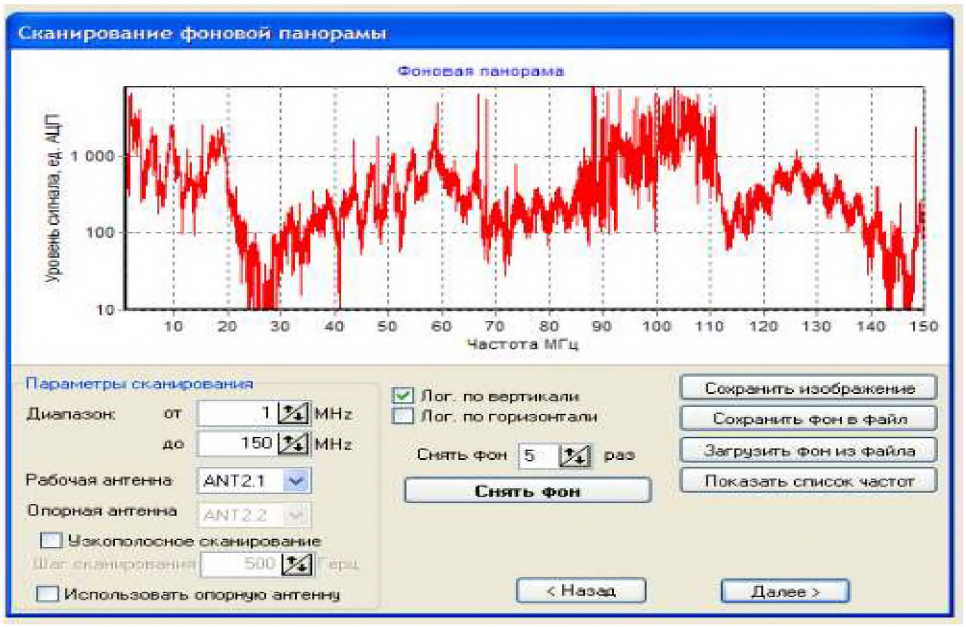


Рисунок 2.19 - Інтерфейсне вікно з прикладом сканування фонової панорами

З виявлених небезпечних частот формувалась таблиця для подальшого вимірювання рівнів сигналу ПЕМВ цих частот. Для отримання більш точних результатів вимірювань, сканування кожної небезпечної частоти повторювалося не менше 5 разів. Вимірювання рівня сигналу, а так само список небезпечних частот представлені на рис. 2.20 і 2.21.

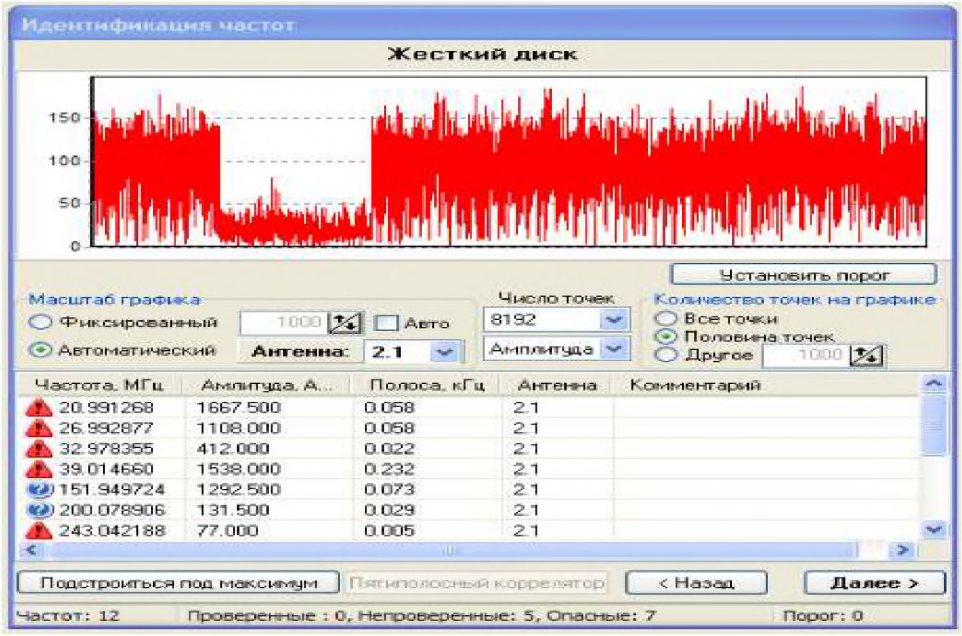


Рисунок 2.20 - Інтерфейсне вікно з прикладом ідентифікації небезпечних частот

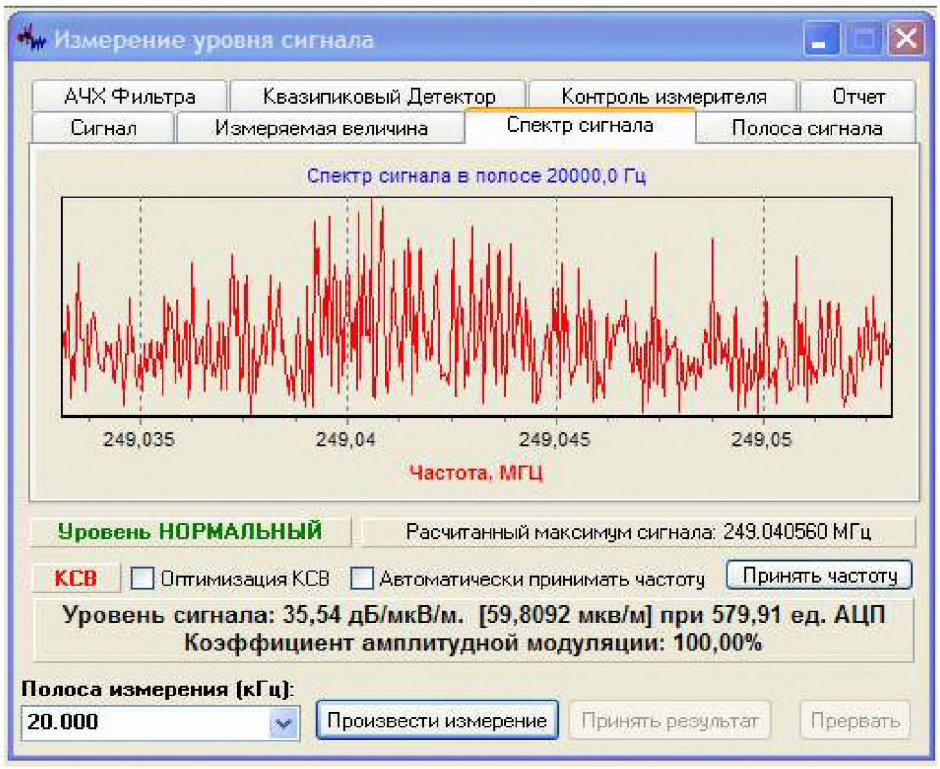


Рисунок 2.21 - Інтерфейсне вікно з прикладом вимірювання рівня сигналу небезпечної частоти

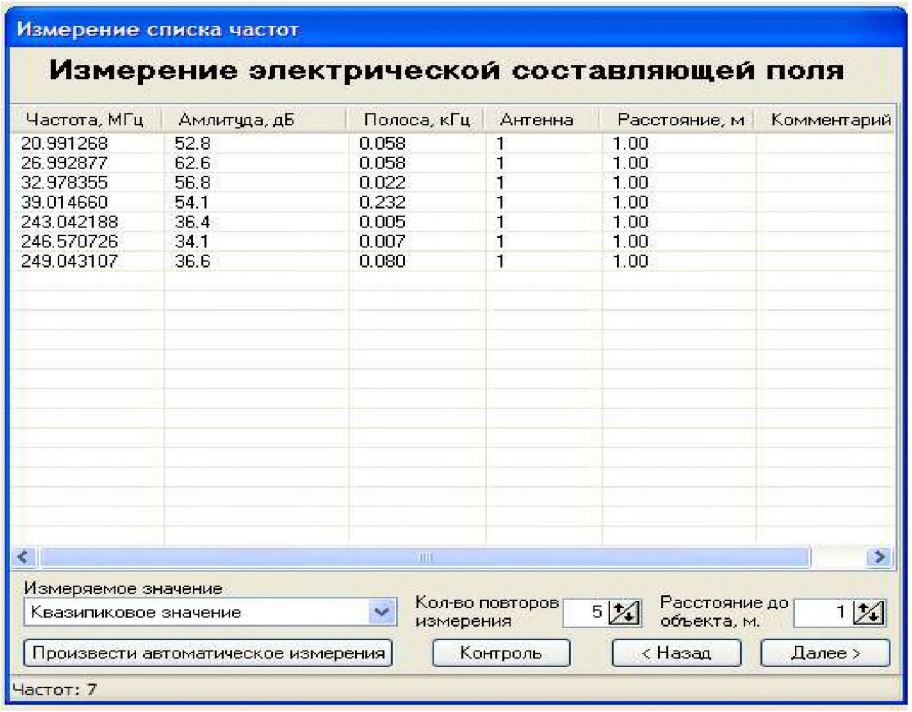


Рисунок 2.22 - Список небезпечних частот, які підлягають вимірюванню

Для проведення вимірювань рівнів ПЕМВ при роботі з флеш-накопичувачами, були встановлені такі чинники, що впливають на рівень побічного електромагнітного випромінювання :

- тип контролера флеш-накопичувача. Для проведення досліджень були обрані флеш-накопичувачі двох найпоширеніших виробників: Kingston (Тип контролерів PHISON PS2251-61-5) і Transcend (Тип контролерів ALCOR AU6980);

- кількість мікросхем пам'яті;

- файлова система, що використовується на флеш-накопичувачі. Найпоширеніші з них: Fat32, NTFS і exFat;

- тип протокольного рівня при роботі флеш-накопичувача: USB 1.1, 2.0, 3.0;

- тип USB-кабелю, що використовується при роботі з флеш-накопичувачем: екранований кабель та екранований кабель з феритовими кільцями;

- тип матеріалу, з якого виготовлений корпус флеш-накопичувача: метал, пластик.

1 Проведення дослідження залежності рівня ПЕМВ від типу контролера флеш-накопичувача

При проведенні досліджень застосовувалися флеш-накопичувачі двох найпоширеніших виробників: Kingston (тип контролерів PHISON PS2251-61-5) і Transcend (тип контролерів ALCOR AU6980). Вимірювання рівня ПЕМВ флеш-накопичувачів з різними типами контролерів проводилися в рівних умовах:

- з флеш-накопичувачів були зняті корпуси;
- встановлена однакова файлова система;
- застосовувався USB кабель 2.0 з феритовими кільцями;

За отриманими результатами побудовані графіки (рис. 2.23 і рис. 2.24).

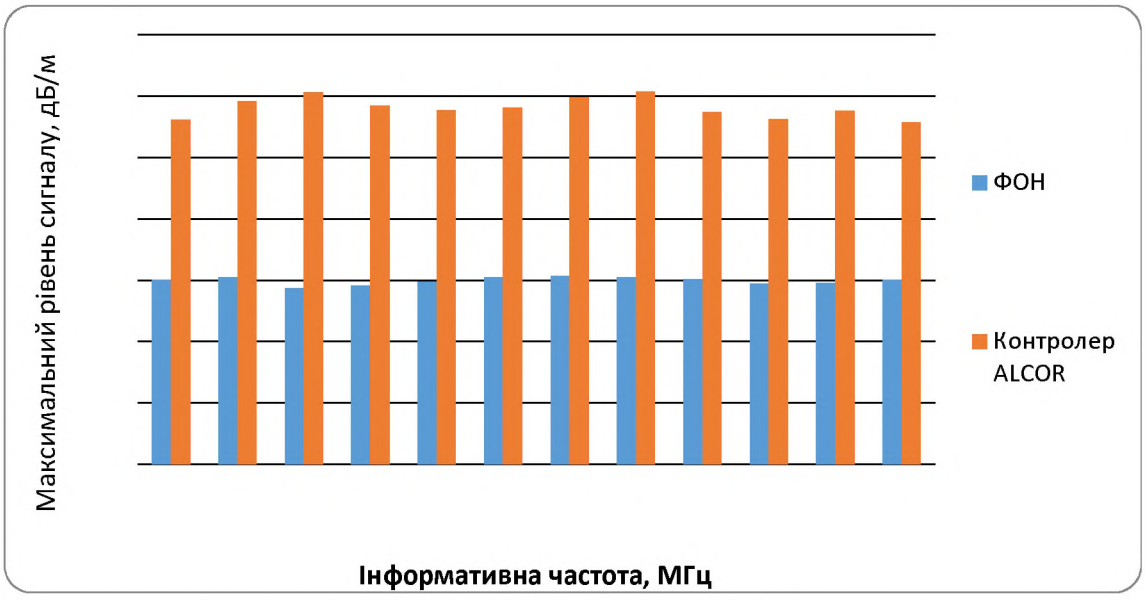


Рисунок 2.23 - Рівні ПЕМВ флеш-накопичувача з контролером типу ALCOR

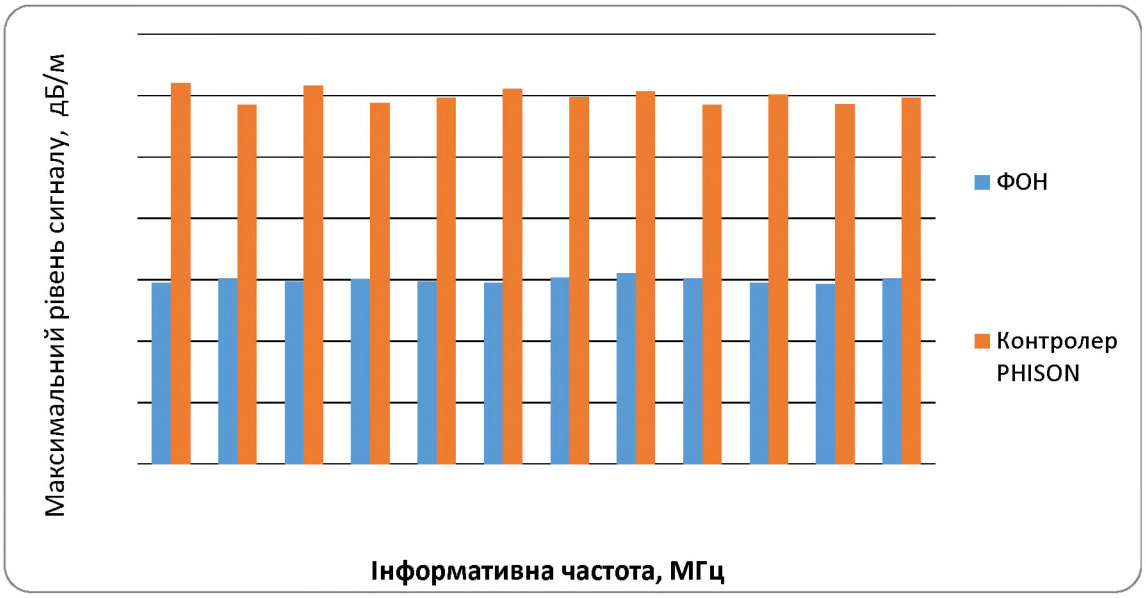


Рисунок 2.24 - Рівні ПЕМВ флеш-накопичувача з контролером типу PHISON

Враховуючи мінімальні відмінності отриманих результатів і роблячи поправку на конструктивні особливості вимірюваних флеш-накопичувачів, можна зробити висновок про те, що тип контролера несуттєво впливає на рівень ПЕМВ від флеш-накопичувачів.

2 Залежність рівнів ПЕМВ від типу файлової системи USB флеш-накопичувача

Наступним етапом проведення вимірювань було дослідження залежності рівнів ПЕМВ від різних файлових систем USB флеш-накопичувачів марки Kingston DTGE9 і Transcend JetFlash 770. Виміри проводилися з використанням екранованого кабелю USB-інтерфейсу з феритовими кільцями. За отриманими результатами побудовані графіки (рис. 2.24, 2.25).

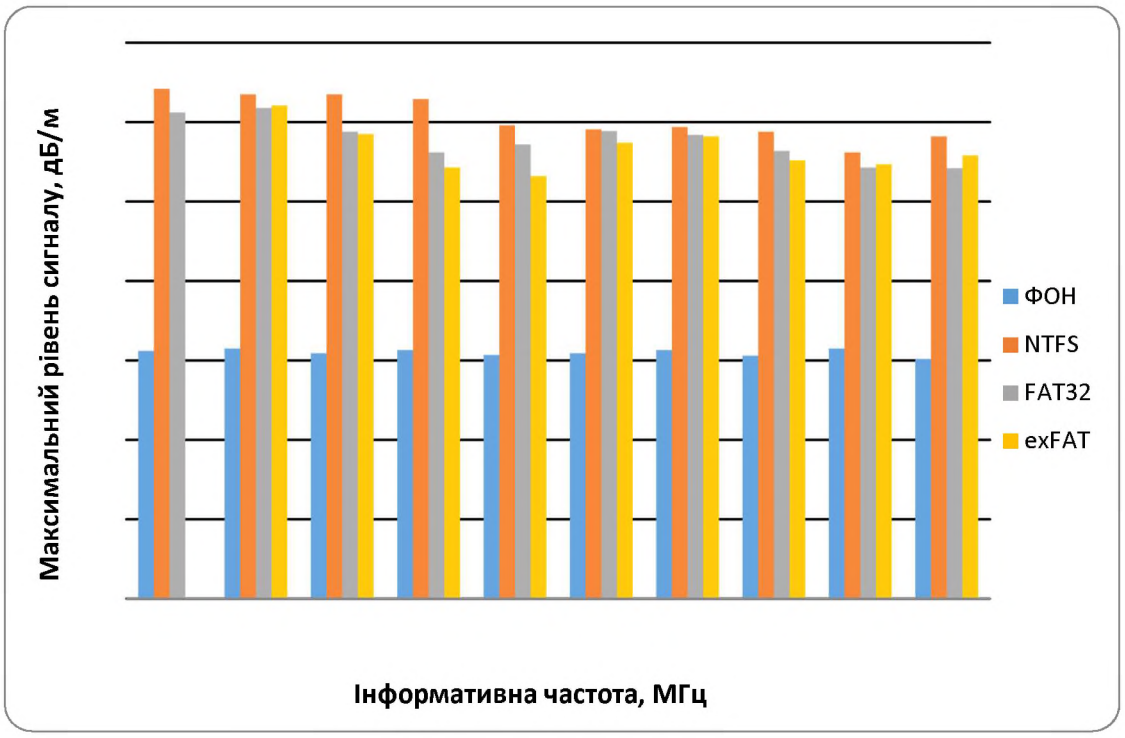


Рисунок 2.24 - Рівні ПЕМВ USB-Flash 2.0 при застосуванні різних файлових систем

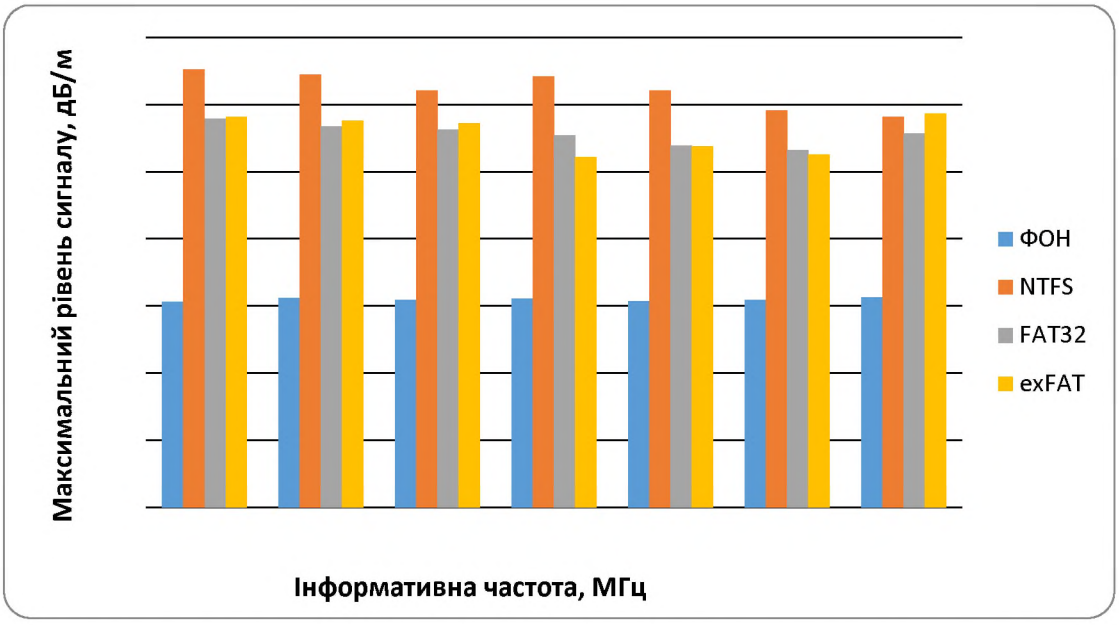


Рисунок 2.25 - Рівні ПЕМВ USB-Flash 3.0 при застосуванні різних файлових систем

У ході вимірювань було встановлено, що випромінювання флеш-накопичувачів, які працювали на файловій системі NTFS вище, ніж при роботі на файлових системах FAT32 або exFAT. Це обумовлено тим, що файлова система NTFS має більш високу частоту роботи з даними, на відміну від інших досліджуваних файлових систем. Так само було виявлено, що кількість небезпечних частот при роботі на файловій системі FAT32 значно зменшувалася.

3 Залежність рівнів ПЕМВ від типу протокольного рівня інтерфейсів USB 1.1, 2.0, 3.0. при роботі флеш-накопичувача

На даному етапі вимірювань проводилися дослідження залежності рівня ПЕМВ від типу використовуваного протокольного рівня USB при роботі флеш-накопичувача. Для вимірювань використовувався флеш-накопичувач моделі Transcend JetFlash 770. Перемикання рівня USB здійснювалося за допомогою BIOS. За отриманими результатами побудовані графіки (рис. 2.26-2.29).

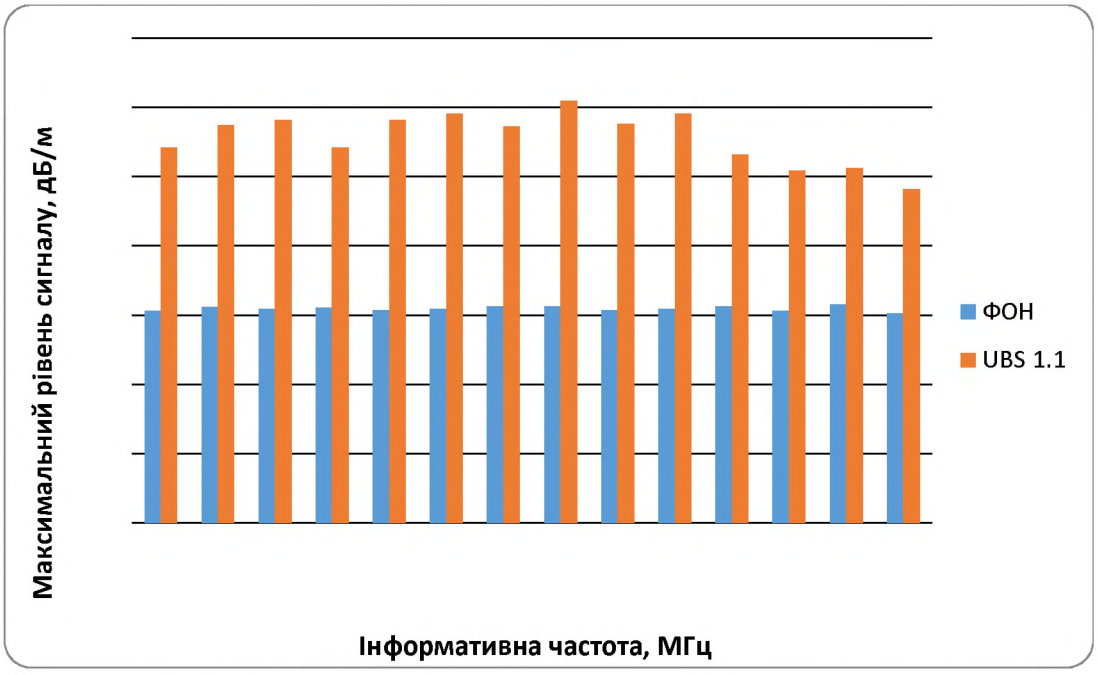


Рисунок 2.26 - Рівні ПЕМВ при роботі флеш-накопичувача на протокольному рівні USB 1.1

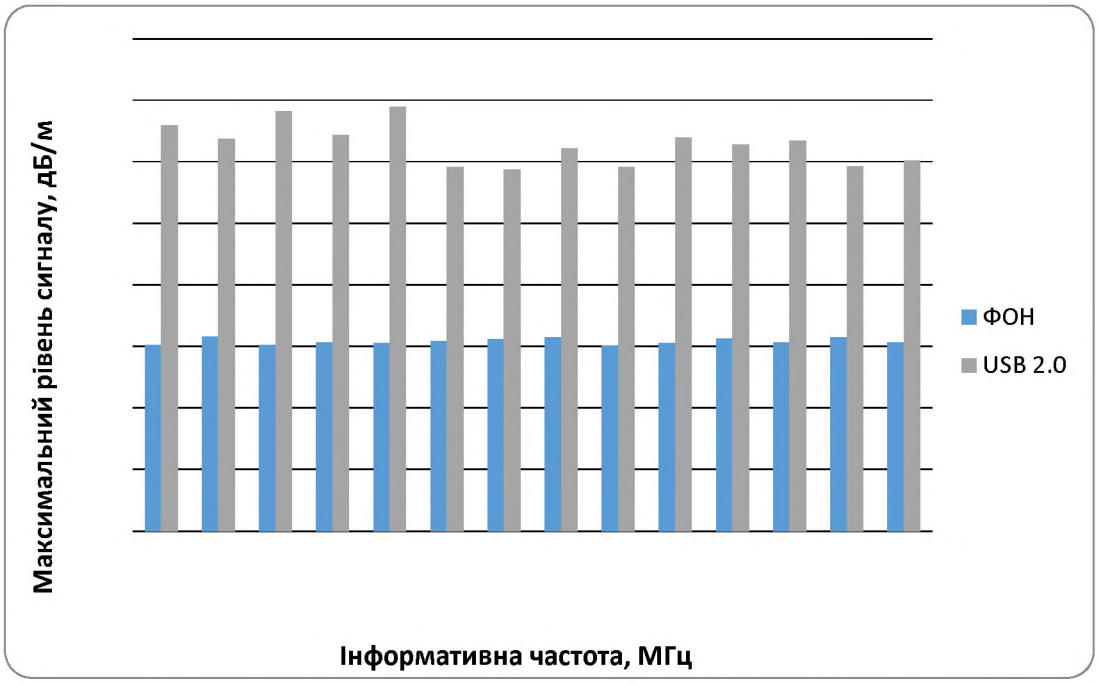


Рисунок 2.27 - Рівні ПЕМВ при роботі флеш-накопичувача на протокольному рівні USB 2.0

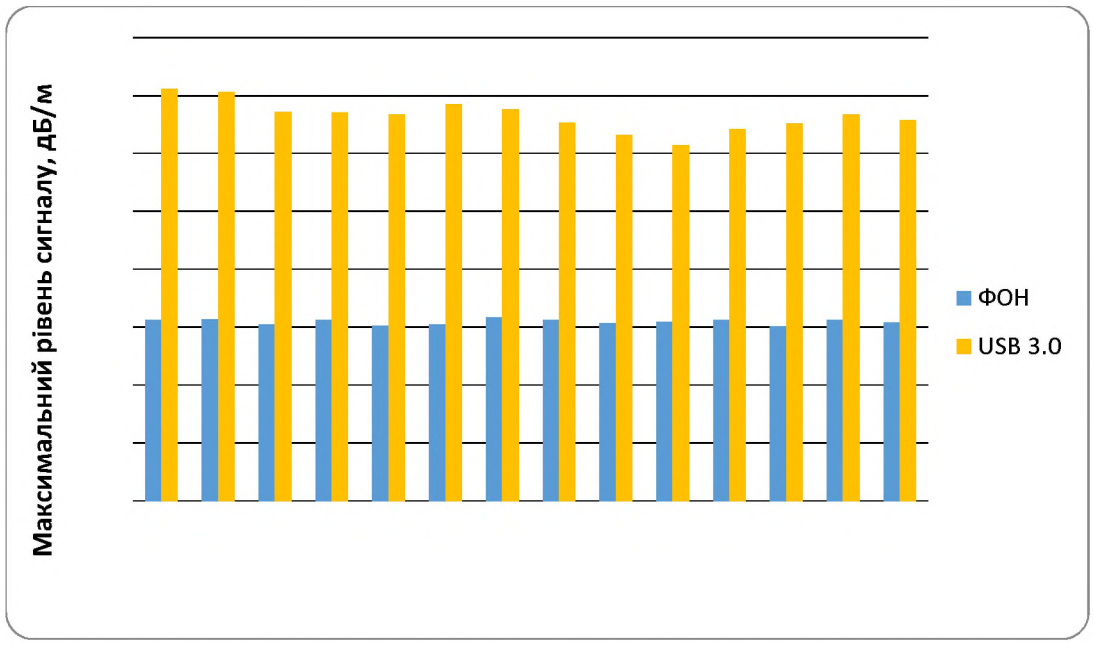


Рисунок 2.28 - Рівні ПЕМВ при роботі флеш-накопичувача на протокольному рівні USB 3.0

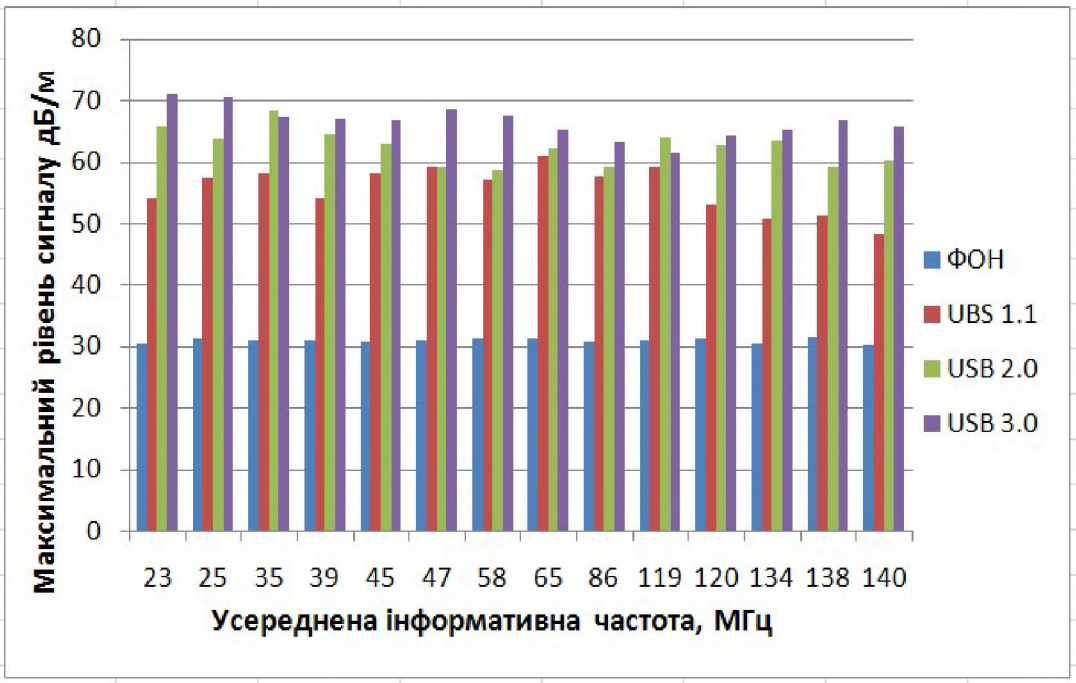


Рисунок 2.29 - Рівні ПЕМВ при роботі флеш-накопичувача на протокольному рівні USB 1.1, 2.0, 3.0

Проаналізувавши отримані дані, можна зробити висновок про те, що із застосуванням більш високого рівня протоколу інтерфейсу, а отже підвищенням частоти обміну даних, зростає рівень інформативних випромінювань в області ВЧ до 200 МГц. Також випромінювання виявляються і на частоті 300 і більше МГц.

4 Залежність рівнів ПЕМВ від типу інтерфейсного кабелю USB

На даному етапі вимірювань проводилися дослідження залежності рівня ПЕМВ від типу кабелю USB, що використовувався для підключення флеш-накопичувача до ЗОТ. Для дослідження були обрані найбільш поширені види кабелю: стандартний, екранований, екранований з феритовими кільцями, довжиною 1.8 м. За отриманими результатами побудовані графіки (рис. 2.30, 2.31).

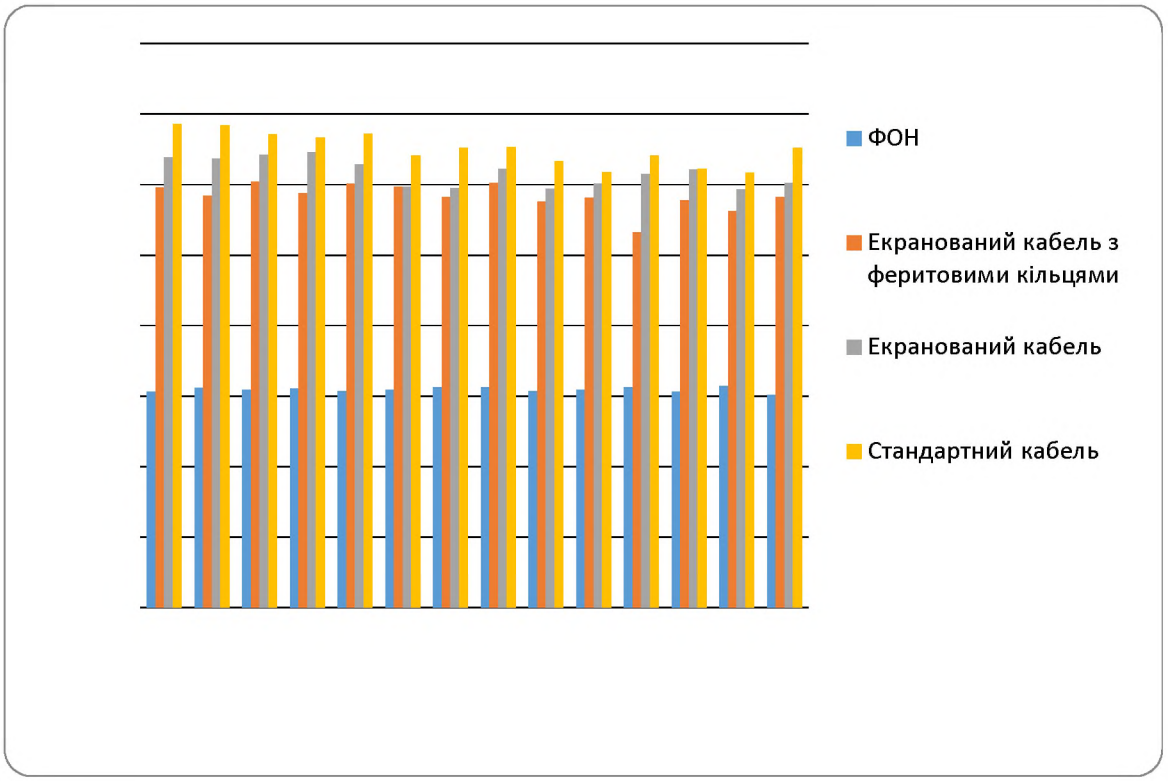


Рисунок 2.30 - Залежність рівнів ПЕМВ від типу інтерфейсного кабелю USB (Режим USB 2.0)

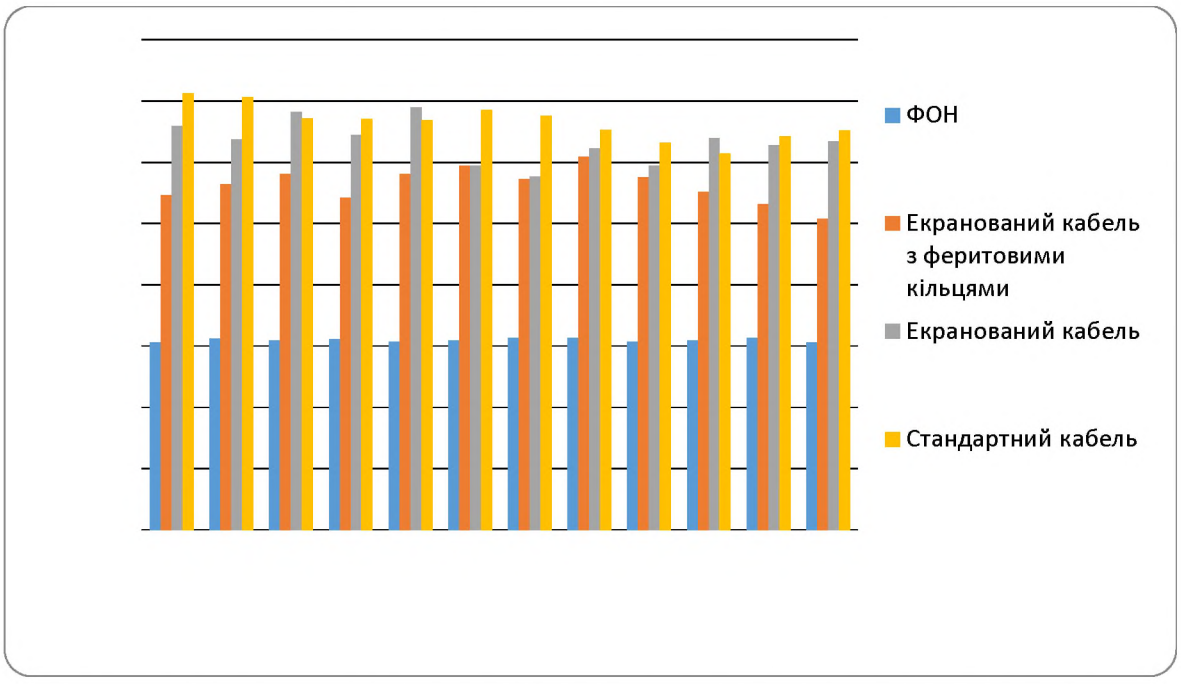


Рисунок 2.31 - Залежність рівнів ПЕМВ від типу інтерфейсного кабелю USB (Режим USB 2.0) (Режим USB 1.1

У даному випадку спостерігається значне зменшення рівня сигналу при використанні кабелю з феритовими кільцями. Це обумовлено тим, що феритові фільтри працюють як:

- індуктивність. ВЧ потужність відбивається назад до кабелю;

- поглинач. ВЧ потужність розсіюється в фериті.

Фільтр, установлений на багатожильний кабель, створює на ділянці кабелю синфазний трансформатор, який, пропускаючи протифазні сигнали (несучі корисну інформацію), відражає (не пропускає) синфазні завади.

5 Залежність рівнів ПЕМВ від типу матеріалу корпусу флеш-накопичувача

На даному етапі вимірювань проводилися дослідження залежності рівня ПЕМВ від типу матеріалу, з якого виготовлений корпус флеш-накопичувача. Для точності вимірювань застосовувалися флеш-накопичувачі одного виробника, з однаковими типами контролерів і схемами пам'яті. На першому етапі проводилися вимірювання рівня ПЕМІ флеш-накопичувача в корпусі, після чого флеш-накопичувач вилучався з корпусу і проводилося повторне вимірювання.

Вимірювалися металевий і пластиковий типи корпусів, фірм виробників Transcend і Kingston. За отриманими результатами побудовані графіки (рис. 2.32-2.35).

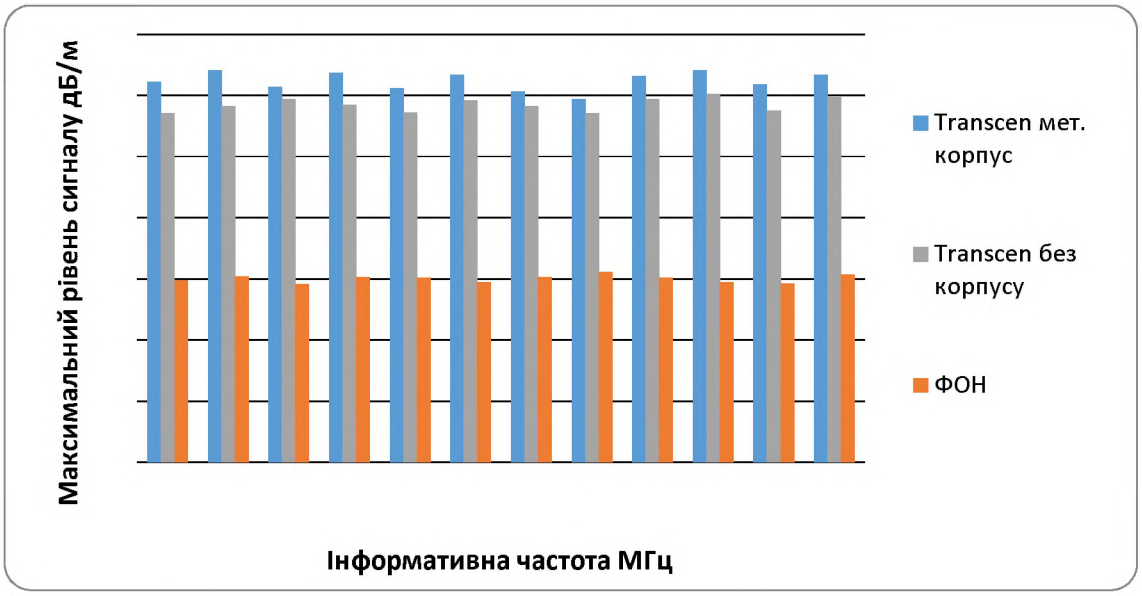


Рисунок 2.32 - Рівні ПЕМВ USB-Flash Transcend з металевим типом корпусу

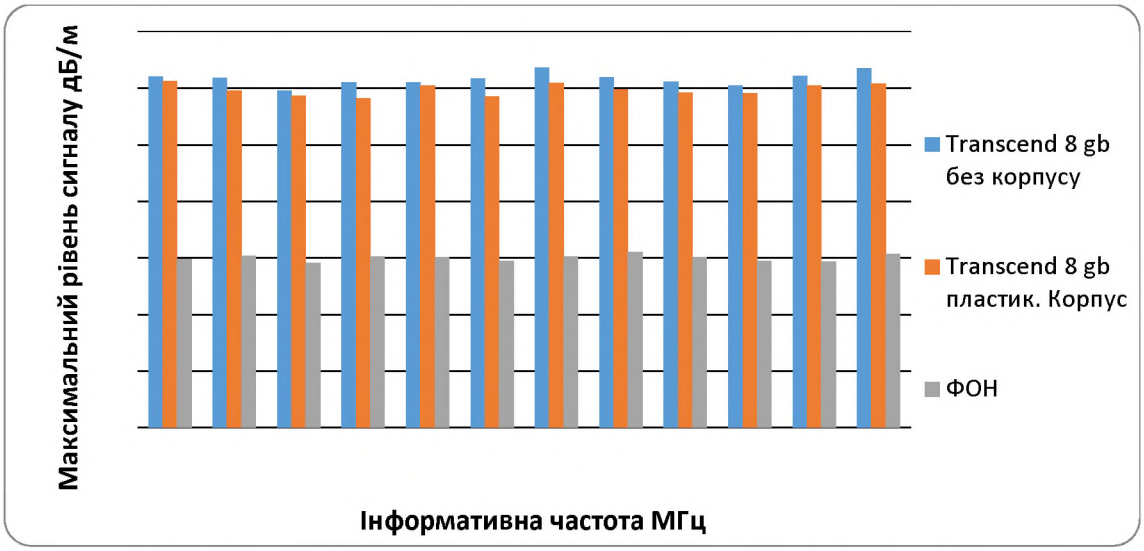


Рисунок 2.33 - Рівні ПЕМІ USB-Flash Transcend з пластиковим типом корпусу

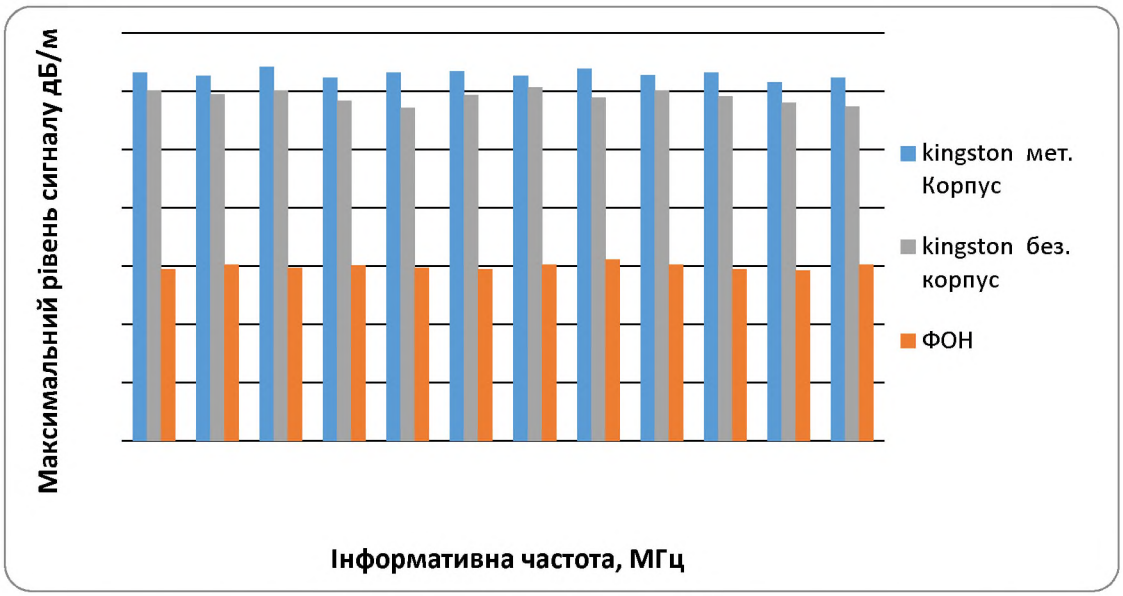


Рисунок 2.34 - Рівні ПЕМВ USB-Flash Kingston з металевим типом корпусу

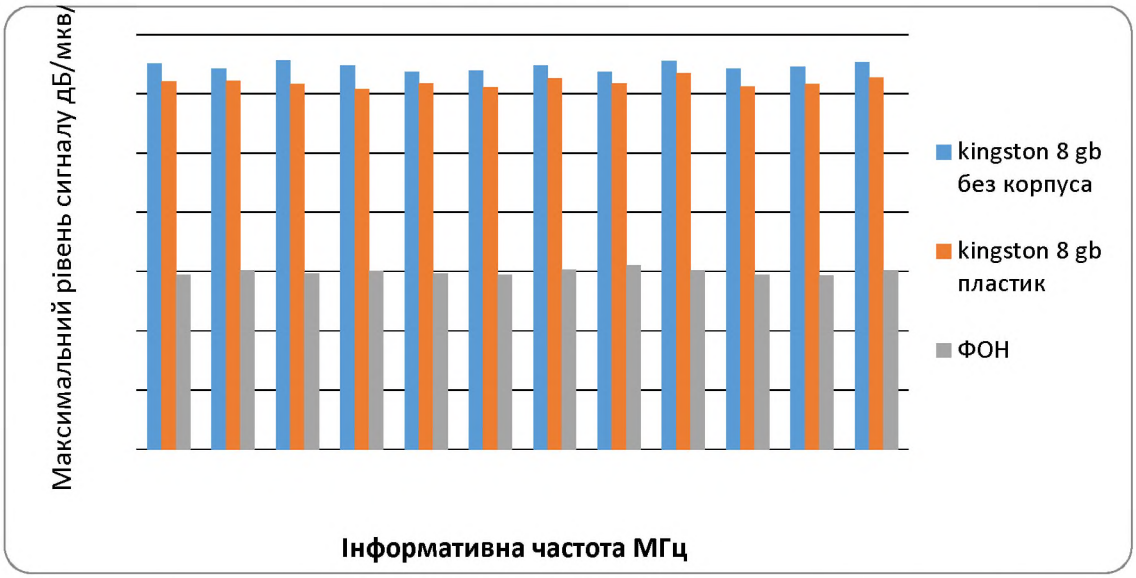


Рисунок 2.35 - Рівні ПЕМІ USB-Flash Kingston з пластиковим типом корпусу

Проаналізувавши отримані дані, можна зробити висновок про те, що має місто збільшення рівня сигналу при використанні металевого корпусу накопичувача. Це можна пояснити тим, що металевий корпус може виступати в якості антени. Контакти та елементи флеш-накопичувача щільно пов'язані з корпусом, в такому випадку може виникати антенний ефект, тим самим посилюючи рівень випромінювання. Так само було встановлено, що при

пошуку інформативних частот автоматизований комплекс виявляв набагато більшу кількість небезпечних частот при роботі флеш-накопичувача з металевим типом корпусу.

2.9 Рекомендації щодо мінімізації рівнів ПЕВМ при роботі з USB флеш-накопичувачами

За отриманих результатів можна зробити наступні висновки щодо мінімізації рівнів ПЕМВ при роботі з флеш-накопичувачами:

1 Результати дослідження впливу типу контролера флеш-накопичувача на рівень ПЕМВ показали, що тип контролера не суттєво впливає на рівень ПЕМВ при роботі флеш-накопичувача.

2 Результати дослідження впливу файлових систем на рівень ПЕМВ показали, що випромінювання флеш-накопичувачів, що працюють на файлової системі NTFS вище, ніж при роботі на файловій системі FAT32 або exFAT. У такому випадку , якщо при використанні флеш-накопичувача немає необхідності у роботі з файлами розміром більше 4 Гб, у цілях зниження рівня ПЕМВ рекомендовано використовувати файлову систему FAT32.

3 Результати дослідження впливу протокольного рівня usb на рівень ПЕМВ показали, що із застосуванням більш високого рівня протоколу інтерфейсу, а отже з підвищенням частоти обміну даних, зростає рівень ПЕМВ. У такому випадку, при роботі з флеш-накопичувачем, з точки зору підвищення рівня інформаційної безпеки, рекомендується використовувати самий нижній протокольний рівень USB, а саме 1.1. Для цього за допомогою BIOS необхідно вимкнути інші рівні USB 2.0 та USB 3.0, якщо такі присутні на ПЕОМ.

4 Результати дослідження впливу рівнів ПЕМВ від типу використовуваного usb подовжувача при роботі флеш-накопичувача показали, що відбувається значне зменшення рівня сигналу при використанні кабелю з феритовими кільцями. У такому випадку, якщо при роботі з флеш-накопичувачем є необхідність використання usb-кабелю, у цілях зменшення

рівнів ПЕМВ рекомендується використовувати екрановані usb-кабелі з феритовими фільтрами.

5 Результати дослідження впливу рівнів ПЕМВ від типу матеріалу, з якого виготовлений корпус флеш-накопичувача, показали, що при використанні металевого корпусу рівень ПЕМВ більший, ніж при використанні флеш-накопичувачів з іншими типами корпусів. Тобто випромінювання флеш-накопичувачів з металевими типами корпусів значно простіше виявити. У такому випадку рекомендується використовувати флеш-накопичувачі у пластикових корпусах.

Беручі до уваги вище представлені рекомендацій та в разі їх застосування при роботі з флеш-накопичувачами можна досягти зменшення рівнів ПЕМВ на 20-25 %. Застосування цих рекомендацій не потребує суттєвих часових або матеріальних затрат, тому доцільно обґрунтоване з точки зору підвищення рівня інформаційної безпеки від витоку інформації технічним каналом ПЕМВ.

2.10 Висновок

У спеціальній частині було розроблено порядок проведення експериментальних досліджень, проведено вимірювання параметрів сигналів, що надходять на флеш-накопичувач та експериментальне дослідження залежностей рівнів ПЕМВ флеш-накопичувачів від різних архітектурних і програмних чинників.

За результатами досліджень розроблені рекомендації щодо мінімізації рівня ПЕМВ при роботі з флеш-накопичувачами. При застосуванні цих рекомендацій можна досягти зниження рівня ПЕМВ на 20-25 %.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу є визначення того, чи буде використання запропонованих засобів та заходів інформаційної безпеки на підприємстві ТОВ «СпецПроєкт» вигідним. В даному розділі розрахуємо повну вартість розробки методик інформаційної безпеки, включаючи розглянуті попередньо рекомендації щодо мінімізації рівня ПЕМВ при роботі з флеш-накопичувачами.

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки.

3.2 Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{год} \quad (3.2)$$

Де $t_{тз}$ = 4 год - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 3 год - тривалість розробки концепції безпеки інформації у організації;

ta = 3 год – тривалість процесу аналізу ризиків;

tвз = 4 год – тривалість визначення вимог до заходів, методів та засобів захисту;

tозб = 3 год – тривалість вибору основних рішень з забезпечення безпеки інформації;

tовр = 2 год – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

tд = 4 год.– тривалість документального оформлення політики безпеки.

t = 4 год + 3 год + 3 год + 4 год + 3 год + 2 год + 4 год = 23 год

3.3 Розрахунок витрат на створення політики безпеки

$$Крп = Ззп + Змч, \quad (3.3)$$

де Крп – витрати на створення політики безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення політики безпеки.

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

$$Ззп = t * Зіб = 23 * 200 = 4600 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, год;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 200 грн/год.

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

$$Змч = t * Смч, грн.$$

де t – трудомісткість розробки політики безпеки інформації на ПК, год;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P * tнал * Се + \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{Fp} =$$

$$= 0{,}2 * 2 * 1{,}68 + \frac{(10000 * 0{,}2)}{1920} + \frac{6000 * 0{,}2}{1920} =$$

$$= 0{,}67 + 1{,}04 + 0{,}63 = 2{,}34 \text{ грн/год},$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0.3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,68 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 10000 грн.;

На – річна норма амортизації на ПК, 0.2 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,2 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 6000 грн.;

Fp – річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920 год.).

$$Змч = t * Смч = 23 * 2{,}34 = 53{,}82 \text{ грн.}$$

$$Крп = Ззп + Змч = 4600 + 53{,}82 = 4653{,}82 \text{ грн.}$$

3.4 Розрахунок (фіксованих) капітальних витрат

Оновлення ліцензії системного, прикладного і спеціалізованого ПЗ: Avast Antivirus Pro Plus - 525 грн (вартість ліцензії для одного ПК на рік), Windows 11 Pro — 1150 грн на рік, MS Office 2019 – 2210 грн на рік, Бухгалтерія А5 – 1000 грн на рік. Необхідно оновлення ПЗ для 4 комп'ютерів.

Загальна вартість закупівель ліцензійного ПЗ:

$$Кзпз = 4 * 4885 \text{ грн} = 19540 \text{ грн} \quad (3.4)$$

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн,$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 10000 грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 19540 грн;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

Кнавч - витрати на навчання адміністратора безпеки, становлять 5000 грн.

Крп – вартість розробки політики безпеки інформації, 4653,82 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки відсутні, оскільки не закуповується апаратне забезпечення.

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 10000 + 19540 + 4653,82 + 5000 = 41193,82 \text{ грн}$$

3.5 Розрахунок поточних (експлуатаційних) витрат.

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 5000 грн – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 2000 + 1500 = 3500 \text{ грн (за 1 місяць)} \qquad (3.5)$$

$$Сз = 3500 * 12 = 42000 \text{ грн (за 1 рік)}$$

де Зк – додаткова заробітна плата керівника, 24000 грн на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 18000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*4 комп'ютерів = 1,2 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 4 комп'ютерів = 7680 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,68 грн за 1 кВт/год – тариф на електроенергію на 01.01.2023 року.

$$Се = 1{,}2 * 7680 * 1{,}68 = 15482{,}88 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0{,}02 = 41193{,}82 * 0{,}02 = 823{,}88 \text{ грн}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Сз + Се + Стос =$$
$$= 5000 + 42000 + 15482{,}88 + 823{,}88 = 63306{,}76 \text{ грн.}$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	Розмір зар. плати	Кількість співробітників	Витрати на зар. плату на міс., грн
Директор	30000	1	30000
Менеджер з продажу	20000	1	20000
Заступник менеджера з продажу	15000	1	15000
Головний приймальник	15000	1	15000
Комірник	15000	1	15000
Керівник відділу підготовки техніки	14000	1	14000
Тестувальник	15000	1	15000
Консультант	14000	1	14000
Системний адміністратор	20000	1	20000
Помічник консультанта	14000	4	14000
Бухгалтер	20000	4	20000
		Сума	192000

Місячний фонд робочого часу складає 160 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = (Зс/Fр) * tв = (192000/160) * 4 = 4800 \text{ грн}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним

введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 8 год:

$$Пви = (192000/160) * 8 = 9600 \text{ грн}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = (20000/160) * 4 = 500$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 9600 + 500 + 5000 = 15100 \text{ грн}$$

Пзч = 5000 грн - вартість для витрат на заміну частин;

О = 4000000 грн - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = \frac{O}{Fp} * (tп + tв + tви) = \frac{4000000}{1920} * (3 + 4 + 8) = 31250 \text{ грн.}$$

Fr – це річний фонд часу роботи, 1920 годин;

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 8 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки при реалізації загрози складе:

$$U = Пп + Пв + V = 4800 + 15100 + 31250 = 51150 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n * U = 3 * 4 * 51150 = 613800 \text{ грн.}$$

де: і- число атакованих вузлів, 3 комп'ютери;

n – середнє число атак на рік, 4 рази.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням В – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; С – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найімовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C = 613800 * 0{,}25 - 63306{,}76 = 90143{,}24 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій То.

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

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

$$ROSI = E/K = 90143{,}24/41193{,}82 = 2{,}19$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1 / 2{,}19 = 0{,}46 \text{ року} = 5{,}5 \text{ місяців.}$$

3.6 Висновки до розділу 3

Розробка і впровадження політики інформаційної безпеки для ТОВ «СпецПроєкт» можна назвати економічно доцільними, так як витрати на її створення значно менші за суму збитків, завдяки невеликій вартості комплектуючих, необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

Тому в результаті:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 41193,82 грн;

- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 63306,76 грн.;
- загальний збиток від атаки на вузол складає 613800 грн.;
- ефект від впровадження системи інформаційної безпеки становить 90143,24 грн.;
- термін окупності капітальних інвестицій складатиме 5,5 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективним та успішним.

ВИСНОВКИ

Аналіз технічного каналу витоку інформації показав, що побічні електромагнітні випромінювання є головною причиною утворення каналів витоку інформації технічних засобів, зокрема флеш-накопичувачів. Тому контроль та вимірювання рівнів ПЕМВ є ключовим завданням засобів і систем радіоконтролю і спецдосліджень апаратури.

При виконанні роботи було розроблено порядок проведення експериментальних досліджень, проведено вимірювання параметрів сигналів, що надходять на флеш-накопичувач. Вимірювання проводилося при різних тест-режимах, а реєстрація параметрів вимірюваних сигналів здійснювалася за допомогою осцилографа.

За допомогою автоматизованого пошукового комплексу виявлення та реєстрації радіовипромінювань АКОР-2ПК з використанням тестових режимів було реалізовано дослідження залежності рівня ПЕМВ флеш-накопичувачів від різних архітектурних і програмних чинників. За результатами досліджень були розроблені рекомендації щодо зниження рівня ПЕМВ при роботі з флеш-накопичувачами.

В економічному розділі кваліфікаційної роботи виконано розрахунок витрат на впровадження засобів та заходів інформаційної безпеки на підприємстві. Їх економічну доцільність доведено.

Наукова новизна роботи полягає у виявленні чинників, що впливають на рівень побічних електромагнітних випромінювань при роботі з флеш-накопичувачами, та розробці рекомендацій щодо зниження рівнів ПЕМВ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Сталенков С.Є., Василевський І.В. Проблема ПЕМВН - М.: Вища школа, 1995. - 425 с.

2 Генне В. І. До питання оцінки рівня ПЕМВ цифрового електронного обладнання. / / Захист інформації. Конфідент. 1999. № 6. С. 61 ... 64.

3 Мусатов С., Білорусів Д. 12 питань щодо коректного вимірювання побічних електромагнітних випромінювань. / / Системи безпеки зв'язку і телекомунікацій. 2000. № 36. С. 64…67.

4 Н.Н. Горобец, А.В. Тривайло. Дослідження побічних електромагнітних випромінювань копм'ютерних блоків у діапазоні 15-500 Мгц. Радіофізика та електроніка. № 942 , випуск 17, 2010. С.55-62

5 Архітектура флеш-пам'яті NOR, NAND / Спосіб доступу: URL:http://dammlab.com/osnovi-pk/companenty_pc/arxitektura-flesh-pamyati-nor-nand-slc-i-mlc.html - Загол. з екрану.

6 АКОР-2ПК/ Спосіб доступу: http://www.akor.mksat.net/production.htm- Загол. з екрану.

7 Побічні електромагнітні випромінювання персонального комп'ютера та захист інформації. / Спосіб доступу :URL: http://www.w3.org/TR/REC-html40

8 Бузов Г.А., Калінін С.В., Кондратьєв А.В. Захист від витоку інформації технічними каналами: Навчальний посібник. - М.: Гаряча лінія - Телеком, 2005. - 416 с.

9 Файлова система NTFS (Електрон. ресурс) / Спосіб доступу: URL : http://ua.wikipedia.org/wiki/NTFS - Загол. з екрану

10 Розкладання сигналів по гармонійним функціям / Спосіб доступу: URL : http://bourabai.kz/signals/ts0403.htm - Загол. з екрану

11 Бегишев М.А. Козьмин В.А, Токарев А.Б Спільне виявлення та оцінка інформативності побічних електромагнітних випромінювань. Журнал "Спеціальна Техніка" № 2 2006 рік.

12 Гасіння побічних електромагнітних випромінювань / Спосіб доступу: http://www.security.ukrnet.net/d-book-3/chap_15.pdf- Загол. з екрану

13 Москаль Є.С., Торбєєва М.В. Виявлення та оцінка інформативності побічних електромагнітних випромінювань флеш-накопичувачів.// Інформаційні технології. Безпека та зв'язок: Матеріали всеукр. наук. – практ. конф. – Д.: Державний ВНЗ «Національний гірничий університет», 2012. – с. 33-34.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1	27	
6	А4	Розділ 2	50	
7	А4	Розділ 3	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Білічук.ppt

2 Кваліфікаційна робота_Білічук.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2 Білічука Р.А. на тему: «Обґрунтування засобів зменшення рівня побічних електромагнітних випромінювань при використанні флеш-накопичувача»

Кваліфікаційна робота, що представлена у вигляді пояснювальної записки на 104 сторінках і презентації на оптичному носії, виконана в повному обсязі згідно завдання.

У зв'язку з актуальністю проблеми витоку інформації за рахунок побічних електромагнітних випромінювань (ПЕМВ) та наведень при її обробці засобами обчислювальної техніки (ЗОТ) та широким розповсюдженням використання флеш-накопичувачів для обміну та збереження важливої інформації, тема кваліфікаційної роботи є актуальною.

У першому розділі обґрунтована актуальність захисту інформації з обмеженим доступом при роботі з флеш-накопичувачами, визначені критерії захищеності ЗОТ, проаналізовані принципи побудови та структура флеш-пам'яті, сформульовані основні задачі даної кваліфікаційної роботи.

У спеціальній частині обґрунтований метод пошуку інформативних сигналів, розроблений порядок проведення експериментальних досліджень рівнів ПЕМВ при роботі з флеш-накопичувачами та за результатами проведених досліджень розроблені рекомендації щодо зниження рівнів ПЕМВ, що виникають при роботі з флеш-накопичувачами.

Наукова новизна результатів даної кваліфікаційної роботи полягає у виявлені залежностей рівнів ПЕМВ при роботі з флеш-накопичувачами від різних чинників та розробці рекомендацій щодо мінімізації цих випромінювань.

Практичне значення роботи полягає у можливості застосування розроблених рекомендацій для підвищення рівня захищеності інформаційних ресурсів.

Перевагами кваліфікаційної роботи є розробка порядку проведення експериментальних досліджень ПЕМВ при роботі з флеш-накопичувачами, який враховує особливості роботи USB-інтерфейсу та флеш-пам'яті, та розробка рекомендацій щодо мінімізації рівнів ПЕМВ, що дозволить знизити ризик витоку інформації з обмеженим доступом, яка обробляється або передається на флеш-носії.

Серед недоліків роботи слід відзначити: недостатньо глибоке опрацювання теми; незначні відхилення від стандартів при оформленні.

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

В цілому робота задовольняє усім вимогам, а її автор Білічук Р.А. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**