Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломного проекту

магістр
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 «Інформаційна безпека»*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

спеціальність *Кібербезпека*
(код і назва спеціальності)

освітній рівень *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Захист інформації від впливу ненавмисних електромагнітних завад на основні технічні засоби, що обробляють інформацію з обмеженим доступом***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

(підпис) ***Білоусова Вікторія Русланівна*** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
проекту	**д.т.н., проф. Корнієнко В.І.**		
розділів:			
спеціальний	**ст. викл. Войцех С.І.**		
економічний	**к.е.н., доц. Волотковська Ю.О.**		
Рецензент			
Нормоконтроль	**доц. Гусєв О.Ю.**		

Дніпропетровськ
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ Корнієнко В.І.

«_____»_____20__року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту **125м-16-1** **Білоусовій Вікторії Русланівні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Захист інформації від впливу ненавмисних електромагнітних завад на основні технічні засоби, що обробляють інформацію з обмеженим доступом***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від 26.12.2017№ 2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***захист інформації від впливу ненавмисних електромагнітних завад***

Предмет досліджень ***аналіз електромагнітних завад та електромагнітної сумісності***

Мета НДР ***підвищення захисту від впливу електромагнітних завад на основні технічні засоби***

Вихідні дані для проведення роботи ***матеріали науко-дослідної та преддипломної практик***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***аналіз джерел безперебійного живлення та топології їх використання***

Практична цінність ***вимоги та розробка рекомендацій для використання джерел безперебійного живлення на об'єкті інформаційної діяльності***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Аналіз джерел безперебійного живлення та топології їх використання, а також вимоги та розробка рекомендацій для використання джерел безперебійного на об'єкті інформаційної діяльності

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Аналіз електромагнітних завад на основні технічні засоби	07.11.17-23.11.17
Аналіз та види електромагнітних завад та сумісності	24.11.17-09.12.17
Аналіз методів та засобів забезпечення електромагнітної сумісності	10.12.17-27.12.17
Економічне обґрунтування та вартість технічних засобів захисту інформації від ненавмисного електромагнітного впливу	27.12.17-09.01.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***розрахунок втрат та збитків, який дозволяє розрахувати термін окупності при умові впровадження засобів технічного захисту***

Соціальний ефект ***використання джерел безперебійного живлення запобігає Нанесенню збитків від ненавмисного електромагнітного випромінювання***

7 ДОДАТКОВІ ВИМОГИ

Оформлення роботи повинно відповідати ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»

Завдання видав _____ В.І. Корнієнко
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ В.Р. Білоусова
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ДЕК _____

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., __ додатків, __ джерел.

Об’єкт дослідження: Вплив ненавмисних електромагнітних завад на основні технічні засоби обробки інформації.

Мета дипломної роботи: аналіз ненавмисного впливу електромагнітних завад та розробка рекомендації, щодо підвищення захищеності технічних засобів.

У спеціальній частині було проведено аналіз методів за засобів захисту інформації від ненавмисного впливу електромагнітних завад, розроблено рекомендації щодо підвищення захищеності основних технічних засобів, запропоновано, які послаблюють електромагнітний вплив.

У роботі досліджено причини виникнення ненавмисних електромагнітних завад. Проведено аналіз завад та засобів їх усунення.

В економічному розділі виконано розрахунок капітальних витрат на введення технічних засобів захисту інформації, проведений розрахунок собівартості технічних засобів захисту інформації.

Наукова новизна полягає у виявленні найбільш вражаючих факторів небезпечного впливу електромагнітних завад на технічні засоби обробки інформації, вдосконаленні заходів по підвищенню захищеності таких засобів.

Застосування сучасних методів забезпечення захисту інформації на підприємстві для підвищення рівня захищеності, а також мінімізувати вірогідність збою технічних засобів.

Ключові слова: електромагнітна сумісність, електромагнітний вплив, технічні засоби, екранування, заземлення, джерела безперебійного живлення, інформація з обмеженим доступом.

РЕФЕРАТ

Пояснительная записка: ___с., __рис., __табл., __приложений, __ источ.

Объект исследования: Влияние непреднамеренных электромагнитных помех на основные технические средства обработки информации.

Цель дипломной работы: проанализировать непреднамеренное влияние электромагнитных помех и разработать рекомендации по повышению защищенности технических средств.

В специальной части был проведен анализ методов по средств защиты информации от непреднамеренного воздействия электромагнитных помех, разработаны рекомендации по повышению защищенности основных технических средств, которые ослабляют электромагнитное воздействие.

В работе исследованы причины возникновения непреднамеренных электромагнитных помех. Проведен анализ помех и средств их устранения.

В экономическом разделе выполнен расчет капитальных затрат на введение технических средств защиты информации, произведен расчет себестоимости технических средств защиты информации.

Научная новизна заключается в выявлении наиболее поражающих факторов опасного воздействия электромагнитных помех на технические средства обработки информации, совершенствовании мероприятий по повышению защищенности технических средств.

Применение современных методов обеспечения защиты информации на предприятии для повышения уровня защищенности, а также минимизация вероятности сбоя технических средств.

Ключевые слова: электромагнитная совместимость, электромагнитное воздействие, технические средства, экранирование, заземление, источники бесперебойного питания, информация с ограниченным доступом.

THE ABSTRACT

Explanatory note: ___ p., ___ fig., ___ tab., ___appendices, ___ sources.

The object of research: The influence of unintentional electromagnetic interference on the main technical means of information processing

Purpose of graduate work: the analysis of unintended effects of electromagnetic interference and the development of recommendations for improving the security of technical means.

In a special part, an analysis was made of methods for protecting information from unintentional exposure to electromagnetic interference, recommendations were developed to improve the protection of basic technical means that weaken the electromagnetic effect.

The causes of unintentional electromagnetic interference are investigated. The analysis of interference and means of their elimination is carried out.

In the economic section, the calculation of capital costs for the introduction of technical means of information protection, the calculation of the cost of technical means of information protection.

Scientific novelty consists in revealing the most damaging factors of the dangerous effect of electromagnetic interference on technical means of processing information, improving measures to improve the security of technical means.

The use of modern methods to ensure the protection of information in the enterprise to improve the level of protection, as well as minimize the probability of failure of technical means.

Key words: electromagnetic compatibility, electromagnetic interference, technical means, shielding, grounding, uninterruptible power supplies, information with limited access.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДТЗС – допоміжні технічні засоби та системи;

ІзОД – інформація з обмеженим доступом;

ОІД – об’єкт інформаційної діяльності;

ЕМВ – електромагнітні випромінювання;

ЕМЗ – електромагнітні завади;

ЕМО – електромагнітне оточення;

ЕМС – електромагнітна сумісність;

ЕОТ – електрообчислювальна техніка;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ до інформації;

ПЕОМ – персональний електрообчислювальний механізм;

ПК – персональний комп’ютер;

ТЗПІ – технічні засоби прийому, обробки, збереження та передачі інформації

ДЖБ – джерела безперебійного живлення

ЗМІСТ

ВСТУП

Сьогодні актуальність проблеми кібербезпека не викликає жодних сумнівів. Щоденно кожен з нас стикається з необхідністю використання інформаційних технологій, а саме це стосується використання технічних засобів.

Тому актуальності набуває саме впив електромагнітних завад. Ненавмисні ЕМЗ можуть призвести до порушення цілісності інформації, що обробляється технічними засобами прийому, обробки, збереження та передачі інформації, та її доступності. Це створює загрозу нанесення великих збитків об’єктам інформаційної діяльності.

Така ситуація вимагає підвищеної уваги до забезпечення електромагнітної сумісності технічних засобів. Ситуація ускладнюється тим, що обладнання дуже різноманітне за типом впливу, потужністю та частотним діапазоном.

Це необхідно враховувати при захисті інформації, що обробляється ТЗПІ, від впливу ненавмисних ЕМЗ.

РОЗДІЛ 1

ЕЛЕКТРОМАГНІТНІ ЗАВАДИ. СУМІСНІСТЬ ТЕХНІЧНИХ ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ

1.1. Основні терміни та визначення

В процесі інформаційної діяльності, основними видами якої є одержання, використання, поширення та зберігання інформації (у тому числі ІзОД), остання може зазнавати впливу загроз її безпеці, у результаті чого може відбутися витік, порушення цілісності і доступності інформації [1].

Це зумовлює необхідність технічного захисту ІзОД.

Технічний захист інформації (ТЗІ) - це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави [3].

Мета технічного захисту ІзОД - своєчасне виявлення загроз та запобігання порушенню цілісності, доступності інформації з обмеженим доступом і витоку її технічними каналами [4].

Технічний захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки спрямовано на запобігання порушенню цілісності, доступності інформації з обмеженим доступом або її витоку шляхом:

- несанкціонованого доступу;
- приймання електромагнітних випромінювань;
- побічних електромагнітних випромінювань і наводок;
- використання закладних пристроїв;
- впровадження комп'ютерних вірусів та іншого впливу [4].

Як правило, при цьому основна увага приділяється захисту інформації від її можливого витоку, навмисного силового деструктивного впливу та несанкціонованого доступу до інформації.

Але загрози порушення цілісності і доступності інформації під час використання технічних засобів для обробки інформації з обмеженим доступом можуть бути спричинені також впливом на ТЗПІ ненавмисних ЕМЗ, створених електронним (в тому числі побутовими приладами) та радіоелектронним обладнанням [9].

Слід відзначити, що питання впливу ненавмисних ЕМЗ тісно пов'язане із ЕМС технічних засобів.

Електромагнітна завада (електромагнітна перешкода) — небажане фізичне явище або вплив електричних, магнітних або електромагнітних полів, електричних струмів та напруг зовнішніх або внутрішніх джерел, через що порушується нормальна робота технічних засобів або погіршується їх технічні характеристики та параметри [9]

Через вплив електромагнітної завади може статися спотворення інформації, що зберігається, перетворюється, передається або обробляється.

Електромагнітна сумісність – це здатність радіоелектронних засобів і випромінювальних пристроїв одночасно функціонувати з обумовленою якістю в реальних умовах експлуатації з урахуванням впливу ненавмисних радіозавад і не створювати неприпустимих радіозавад іншим радіоелектронним засобам[9]

Технічний засіб може бути одночасно як рецептором, так і джерелом таких перешкод.

Рецептор – будь-який технічний пристрій, який реагує на електромагнітний вплив ЕМЗ[11]

В галузі ЕМС під будь-яким джерелом ЕМЗ розуміють джерело завади, яка виникає без попереднього наміру чи через недостатність технічних і організаційних заходів, або через особливості фізичних процесів.

Небажаний вплив на рецептор (засіб, що сприймає перешкоду) може бути безпосереднім або опосередкованим. При непрямому впливі відсутня пряма передача електромагнітної енергії рецептора. У цьому випадку вплив перешкоди полягає у зміні середовища функціонування, параметрів елементів, пристроїв технічного засобу або режимів їх роботи. Безпосередній вплив обумовлений передачею енергії перешкоди від джерела до рецептора її випромінюванням у простір або по провідниках (ланцюгах заземлення та електроживлення, з'єднувальних і комунікаційних лініях, кожухах технічних засобів).

У міжнародних стандартах та нормативних документах для класифікації впливу електромагнітних завад по ступеню ураження приладів використовуються критерії якості функціонування апаратури під дією ЕМЗ, що являють собою сукупність властивостей та параметрів, які характеризують працеспроможність технічних засобів під час дії завад. Критерії, зображені на рис. 1.1, застосовуються для формалізації опису роботи апаратури під дією тієї чи іншої завади [13]

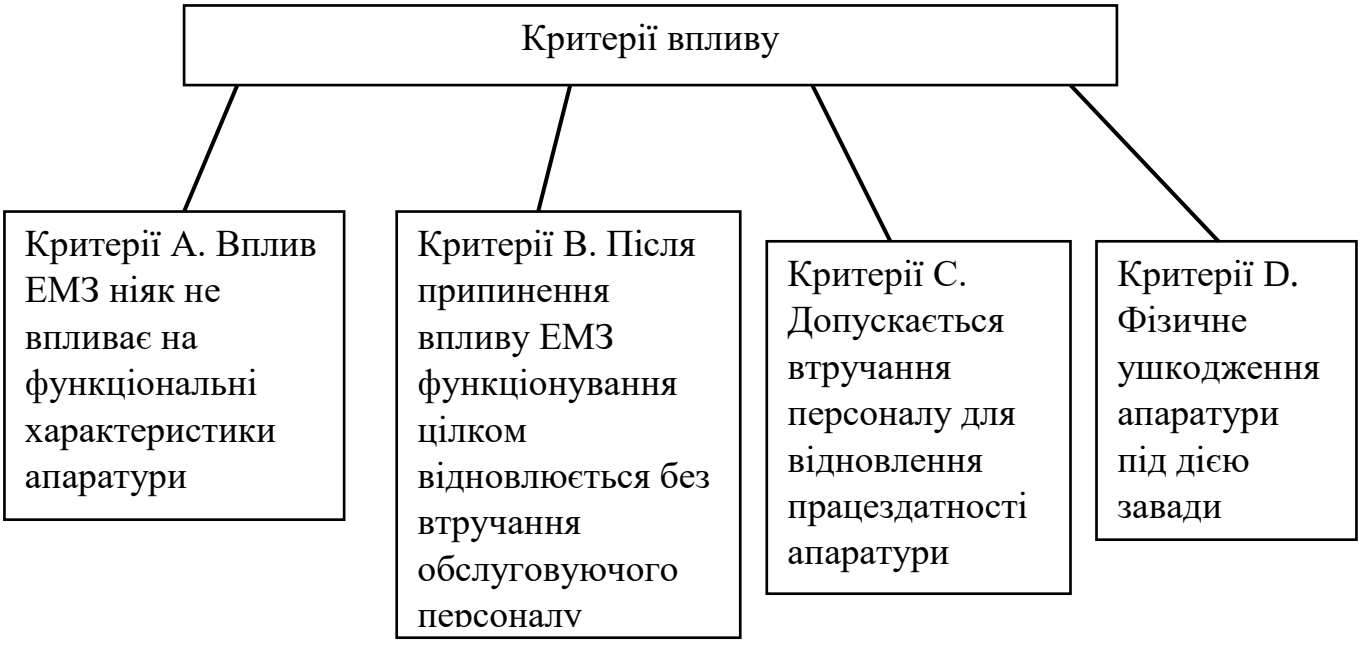

Рисунок 1.1 - Критерії впливу електромагнітних завад по ступеню ураження приладів

Критерій A

Вплив ЕМЗ ніяк не впливає на функціональні характеристики апаратури, робота якої до, під час і після впливу завад відбувається у повній відповідності до технічних умов або стандартів. Зазвичай виконання критерію А потребує апаратура, яка використовується для виконання функцій високої важливості в реальному масштабі часу. Це апаратура захисту і протиаварійної автоматики.

Критерій B

Допускається тимчасове погіршення функціональних характеристик апаратури в момент впливу завад. Після припинення впливу ЕМЗ функціонування цілком відновлюється без втручання обслуговуючого персоналу. Цей критерій найчастіше використовується для апаратури, що виконує задачі високої важливості, однак не в реальному масштабі часу. Досить специфічним моментом при визначенні відповідності апаратури критерію. В є допустимий час відновлення функціональних характеристик після впливу завад. Це актуально, наприклад, коли мова йде про цифрову апаратуру, вплив ЕМЗ на яку приводить до перезавантаження.

Критерій C

Аналогічний критерію В, але, на відміну від нього, допускає втручання персоналу для відновлення працездатності апаратури (наприклад, перезавантаження цифрової системи, яка "зависла", повторного набору номера і т. п.). Зазвичай використовується для апаратури, не призначеної для виконання відповідальних задач.

Критерій D

Фізичне ушкодження апаратури під дією завади. За зрозумілими причинами, цей критерій не може використовуватися для формулювання вимог до стійкості апаратури.

Незважаючи на високий рівень формалізації, застосування таких критеріїв часто вимагає додаткової інформації. Така конкретизація повинна виконуватися в стандартах на види продукції і технічних умовах [12].

Існують різні можливі шляхи сприймання ЕМЗ технічним засобом, а також шляхи поширення перешкод, створених ним самим (рис 1.2).

Електромагнітні перешкоди можуть розповсюджуватися як у просторі, так і через кондуктивний зв'язок.

Кондуктивний зв'язок є результатом омічного контакту між елементами схем або провідниками технічних засобів. Він може виникнути при недосконалій ізоляції або наявності спільних ланцюгів заземлення і т.п.

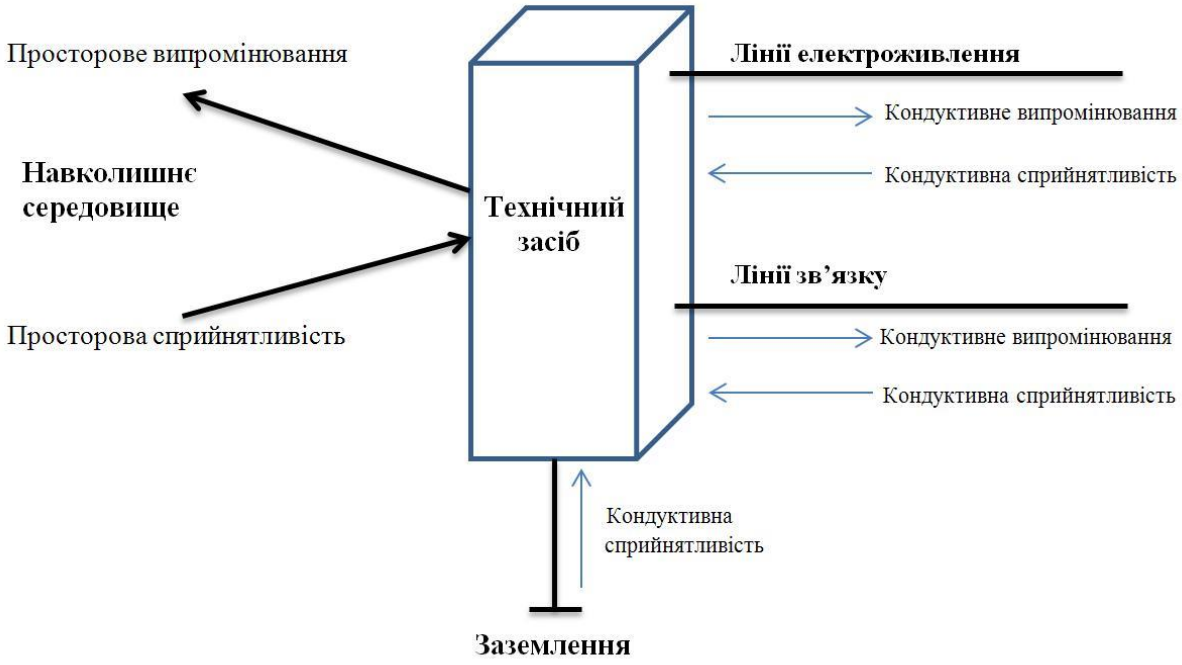

Рисунок 1.2 – Можливі шляхи сприймання та поширення перешкод технічними засобами

Електромагнітні перешкоди можуть розповсюджуватися як у просторі, так і через кондуктивний зв'язок.

Кондуктивний зв'язок є результатом омічного контакту між елементами схем або провідниками технічних засобів. Він може виникнути при недосконалій ізоляції або наявності спільних ланцюгів заземлення і т.п.

Просторова перешкода утворюється практично при роботі будь-якого технічного засобу, оскільки електромагнітне поле навколо працюючого технічного засобу займає якийсь простір в певній смузі частот на період своєї роботи. Незалежно від того, яким є поле для його джерела, для технічного засобу, що обробляє інформацію, яка захищається, воно є перешкодою [9].

1.2 Аналіз типів електромагнітних завад

Завади можна поділити на чотири види:

1. Навмисні завади – створюються шляхом формуванням середовищ їх поширення з метою забезпечення умов для несанкціонованого витоку або спотворення інформації з обмеженим доступом.

2. Ненавмисні завади – утворюються як результат побічного виникнення фізичних полів і середовищ їх поширення.

3. Природничі завади:

- Космічні шуми, реліктове випромінювання
- Радіовипромінювання Землі й об'єктів Сонячної системи
- Атмосферні завади Землі;

4. Штучні завади:

- Індустріальні або промислові завади електромагнітні випромінювання промислових машин, побутових електроприладів тощо;
- Станційні завади випромінювання від інших радіоелектронних засобів: радіостанцій, радіолокаторів тощо[29]

1.2.1 Випромінювачі електромагнітних завад

Кожний електронний пристрій є джерелом електромагнітних полів широкого частотного спектру, характер яких визначається призначенням і схемними рішеннями, потужністю пристрою, матеріалами, з яких він виготовлений, і його конструкцією.

Електромагнітні випромінювання (ЕМВ), що генеруються електронними пристроями, обумовлені протіканням струмів у їх електричних ланцюгах. Спектр ЕМВ електронного устаткування представляє собою сукупність гармонійних складових у деякому діапазоні частот (у деяких випадках кілька ГГц) [15].

Джерелами випромінювань є різноманітні технічні засоби (у тому числі ті, які обробляють інформацію з обмеженим доступом), а саме:

- побутова техніка;
- промислове обладнання;
- медичне обладнання;
- наукове обладнання;
- мережі електроживлення та лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи телеграфного, телекодового та факсимільного зв'язку;
- засоби гучномовного зв'язку;
- засоби звуко- і відеозапису;
- системи звукопідсилення мовлення;
- електронно-обчислювальна техніка;
- електронні засоби оргтехніки.

Джерелами ЕМВ є їхні елементи, вузли та провідники.

У персональному комп'ютері (ПК) ЕМЗ формуються наступними ланцюгами [7]:

– ланцюг, по якому передаються сигнали від контролера клавіатури до порту введення-виведення на материнській платі;
– ланцюги, по яких передається відеосигнал від відеоадаптера до електродів електронно-променевої трубки монітора;
– ланцюги, що формують шину даних системної шини комп'ютера;
– ланцюги, що формують шину даних усередині мікропроцесора;
– ланцюги формування та передачі сигналів синхронізації;
– ланцюги, що формують шину управління і шину адреси системної шини;
– ланцюги, які передають сигнали апаратних переривань;
– внутрішні ланцюги блоку живлення комп'ютера і т. п.

1.2.2 Класифікація електромагнітних завад

При класифікації ЕМЗ за їх походженням можна виділити наступні види завад:

– ненавмисні перешкоди природного походження (космічні та атмосферні перешкоди, шуми антенних систем і внутрішні шуми приймачів);
– ненавмисні перешкоди штучного походження;
– організовані перешкоди (навмисні), які можуть бути активними і пасивними.

Класифікація за наведеними видами завад приведена нижче на рис.1.3.

Рисунок 1.3 – Класифікація електромагнітних завад за їх походженням

Для визначення особливостей ненавмисних ЕМЗ розглянуто класифікації за такими класифікаційними ознаками: за класом ЕМЗ, за видом та за середовищем розповсюдження.

1.2.2.1 Класифікація електромагнітних завад за їх класом

Клас ЕМЗ - групування перешкод за їх основною ознакою, а саме за природою джерел перешкод. Згідно з цим електромагнітну перешкоду можна віднести до одного з чотирьох класів (рис. 1.4).

Рисунок 1.4 – Класифікація електромагнітних завад за їх класом

Станційна перешкода – відноситься до класу перешкод від антени радіопередавального пристрою. Вона проявляє свою дію на такий рецептор, як приймач на його робочій частоті або на сусідніх і побічних каналах прийому. Створюється основним випромінюванням завадного передавача або його гармонікою, або іншими неосновними випромінюваннями. У літературі часто використовується синонім «завадний сигнал».

Індустріальна перешкода – відноситься до класу перешкод від електротехнічних, електронних та радіоелектронних пристроїв (в останніх крім випромінювання через антену), що використовуються в побуті, промисловості, наукових дослідженнях тощо. Дія перешкод цього класу на рецептори проявляється в більшості випадків у вигляді імпульсних процесів, характеристики яких залежать від типу конкретного пристрою. Індустріальна перешкода є найбільш поширеною в діапазонах частот від десятків Гц до 1 ГГц, а в ряді випадків до більш високих частот (3 ГГц).

Природна перешкода – відноситься до класу перешкод, зумовлених природними фізичними процесами (явищами), у вигляді електромагнітних випромінювань, наприклад в атмосфері (атмосферні перешкоди), з частотами від одиниць Гц до 10 МГц або в космічному просторі (космічний шум) з частотами вище 1 МГц, у тому числі створені космічними тілами (Сонце, зірки). До класу природних перешкод слід віднести електростатичну перешкоду, що виникає внаслідок електризації різних тіл, в тому числі елементів конструкцій, і виявляється внаслідок струмів стікання накопичених електричних зарядів та (або) іскрових розрядів між елементами конструкції. Такі перешкоди виявляються в діапазоні частот від декількох Гц до 1 ГГц.

Контактна перешкода – відноситься до класу перешкод, які створюються перевипроміненням струмопровідних механічних контактів з нелінійною струмовою провідністю при їх опроміненні полем досить потужного радіопередавального пристрою. Перешкоди цього класу представляють собою сукупність імпульсних і шумових процесів. Контактні перешкоди характерні

для об'єктів, що рухаються, транспортного призначення, і їх рівень зростає із збільшенням швидкості руху об'єкта. Як правило, контактні перешкоди впливають на рецептор, встановлений на об'єкті, що рухається, на якому одночасно працює досить потужний радіопередавальний пристрій. [10]

1.2.2.2 Класифікація електромагнітних завад за їх видом

Вид ненавмисних ЕМЗ - групування перешкод за додатковими класифікаційними ознаками - частоті, енергетичному спектру, проявом у часі, відношенню перешкоди до засобу, що її сприймає (рецептора), відношенню рецептора до перешкоди і приналежності до окремих класів перешкод [30]. Класифікація за видами завад наведена на рис. 1.5.

Рисунок 1.5 - Класифікація електромагнітних завад за їх видом

1) За частотою:

Високочастотна перешкода - радіоперешкода, частота якої 9 кГц і вище (до оптичного діапазону).

Низькочастотна перешкода – перешкода, частота якої нижче 9 кГц.

2) За енергетичним спектром:

Синусоїдальна перешкода – перешкода, енергетичний спектр якої визначається однією синусоїдальною (косинусоидальною) складовою (наприклад, несуча частота радіопередавача).

Імпульсна перешкода - перешкода, енергетичний спектр якої в межах амплітудно-частотної характеристики (АЧХ) системи в тимчасовій області є або дискретним, якщо визначається рідкісними або одиночними перешкодами, або суцільним, якщо визначається перешкодами, які перекриваються в часі.

Шумова перешкода - перешкода, енергетичний спектр якої визначається приблизно постійними складовими в межах АЧХ системи при реєстрації за порівняно великий час (наприклад, внутрішній шум радіоприймача, космічний шум випромінювання Сонця, зірок і Галактики).

Модульована перешкода - станційна перешкода, енергетичний спектр якої визначається регламентованим типом модуляції і відповідним класом випромінювань (наприклад, випромінювання радіопередавального пристрою, що є корисними сигналами для певного виду рецептора і завадними сигналами для інших видів рецепторів).

Імпульсно-шумова перешкода - перешкода, енергетичний спектр якої має помітні імпульсні і шумові складові (наприклад, атмосферні перешкоди від розрядів грози при її значному видаленні від рецептора, контактні перешкоди і індустріальні перешкоди від деяких джерел, зокрема, від зварювального апарату).

3) За проявом у часі:

Безперервна перешкода - перешкода, рівень якої не зменшується нижче певного порогового значення за час не менше 1 с.

Тривала перешкода – перешкода, час дії якої більше 1 с.

Короткочасна перешкода - перешкода, час дії якої менше 0,2 с.

Рідкоімпульсна перешкода - перешкода, час дії якої розділено значними (більше 1 с) проміжками часу; в окремому випадку перешкода може проявлятися як поодинока.

Регулярна перешкода - перешкода, яка виникає і зникає через однакові (майже однакові) проміжки часу.

Нерегулярна перешкода - перешкода, виникнення і зникнення якої відбувається через різні випадкові проміжки часу.

Комутаційна перешкода - короткочасна перешкода, що виявляється в часі нерегулярно. Вона виникає із-за випадкових процесів комутації струму і напруги головним чином в ланцюгах харчування електротехнічних, електронних та радіоелектронних пристроїв. В більшості випадків представляє собою послідовність короткочасних пачок імпульсів в моменти відключення і підключення навантаження до ланцюга живлення. В мережах живлення 220/380 В зареєстровані комутаційні перешкоди з амплітудою 600 ... 1000 В при тривалості від десятків наносекунд до одиниць мікросекунд.

4) По відношенню перешкоди до рецептора:

Вузькосмугова перешкода - перешкода, ширина спектру якої менше або дорівнює ширині смуги пропускання рецептора.

Широкосмугова перешкода - перешкода, ширина спектру якої більше ширини смуги пропускання рецептора.

Зовнішня перешкода - перешкода, джерело якої знаходиться поза рецептором.

Внутрішня перешкода - перешкода, джерело якої знаходиться всередині рецептора (наприклад, власний шум вхідного тракту радіо або перешкода від вторинного джерела живлення, вбудованого в пристрій рецептора).

Міжсистемна перешкода - перешкода, джерело якої знаходиться в системі, яка не належить до розглянутої, що включає рецептор.

Внутрішньосистемна перешкода - перешкода, джерело якої знаходиться всередині розглянутої системи, але поза рецептором.

Внутрішньоапаратурна - перешкода, джерело якої знаходиться всередині конкретного апарату (перешкода від компонентів того ж апарату).

Адитивна перешкода - дія якої на рецептор проявляється у складанні з корисним сигналом (наприклад, складання власного шуму приймача із прийнятим сигналом).

Мультиплікативна перешкода - перешкода, дія якої на рецептор змінює не тільки амплітуду, але і фазу корисного сигналу за рахунок накладення на його огинаючу деякого випадкового процесу.

Когерентна перешкода - перешкода регулярного характеру, дія якої на корисний сигнал проявляється при наявності постійних фазових співвідношень між перешкодою й сигналом.

Некогерентна перешкода - перешкода нерегулярного характеру, дія якої на корисний сигнал виявляється при наявності випадкових і непостійних фазових співвідношень між перешкодою й сигналом (наприклад, імпульсна перешкода від будь-якого джерела індустріальних перешкод).

Симетрична перешкода - перешкода, дія якої на рецептор проявляється між двома незаземленими виводами джерела індустріальних перешкод або між фазовими проводами мережі живлення рецептора (або іншого електричного кола).

Несиметрична перешкода - перешкода, дія якої на рецептор проявляється між затиском джерела індустріальних перешкод (або мережі живлення, або будь-який інший електричної мережі) і ланцюгом заземлення.

5) По відношенню рецептора до перешкоди:

Припустима перешкода - перешкода, дія якої не знижує необхідної якості функціонування обладнання.

Неприпустима перешкода - перешкода, дія якої знижує необхідну якість функціонування РЕА обладнання до неприйнятного рівня.

Прийнятна перешкода - перешкода, дія якої знижує необхідну якість функціонування обладнання до рівня, прийнятого як задовільний в конкретних умовах.

Блокуюча перешкода - перешкода, яка виникає внаслідок нелінійності передатної характеристики вхідного тракту при впливі станційної перешкоди з частотою, що знаходиться поза основною смугою пропускання.

Перехресна перешкода - перешкода, дія якої проявляється у вхідному тракті пристрою як зміна амплітуд (перехресна амплітудна) або фаз (перехресна амплітудно-фазова) складових спектру корисного сигналу. Виникає через нелінійність передатної характеристики тракту при дії модульованої станційної перешкоди, частота якої знаходиться поза основною смугою пропускання.

Інтермодуляційна перешкода - перешкода, яка виникає внаслідок нелінійності передатної характеристики вхідного тракту пристрою при дії двох або більше станційних перешкод, частоти яких знаходяться поза основною смуги пропускання і мають певні співвідношення між собою і частотою корисного сигналу. [10]

1.2.2.3 Класифікація перешкод за середовищем розповсюдження

За середовищем розповсюдження ЕМЗ можна поділити на перешкоди, що передаються по провідниках, та просторові перешкоди.

Для більш детального розгляду вище вказаних перешкод дана класифікація була доповнена та розширена (рис. 1.6).

Рисунок 1.6 - Класифікація електромагнітних завад за видом середовища розповсюдження

Перешкода, передана по провідниках (кондуктивна), є результатом омічного контакту між двома технічними засобами. Вона може виникнути через гальванічний зв'язок при недосконалій ізоляції або наявності спільних ланцюгів заземлення і т.п.

Залежно від виду зв'язку кондуктивна перешкода може бути: ємкісною (електричну) і індуктивною (магнітною).

Ємнісна перешкода є результатом паразитної ємності, а індуктивна –

результатом взаємної індуктивності між технічним засобом-джерелом перешкоди і технічним засобом-рецептором.

Ємнісний зв'язок обумовлений впливом в основному електричного поля, коли воно є переважаючим в ближній зоні. Це відноситься до провідників, які мають великий опір щодо «землі». Прикладом цього може бути багатодротовий кабель.

Індуктивний зв'язок виникає між низькоомними провідниками, що мають малий опір щодо «землі» і утворюють за формою петлю (рамку), тобто є випромінювачами магнітного поля.

Просторова перешкода утворюється практично при роботі будь-якого технічного засобу. Вони являють собою електромагнітні поля в середовищі, яке

оточує технічний засіб. В залежності від тієї складової вектора напруженості електромагнітного поля завад, що суттєво переважає іншу, розрізняють електричні (з переважаючим значенням вектора E) і магнітні (з переважаючим значенням вектора H) поля завад.

Створювані технічним засобом у навколишньому просторі електромагнітні поля також можна поділити на:

- функціональні - випромінювані з метою передачі корисної інформації призначеними для цього радіоелектронними засобами через антенно-фідерні пристрої, їх рівень прагнуть підсилити;
- супутні (паразитні) - супроводжують роботу технічного засобу і є наслідком його технічної недосконалості, створюють завадний вплив на роботу сусідніх ТЗ; їх рівень прагнуть усунути або знизити до допустимих меж шляхом застосування конструкторських і схемних рішень, як правило, на етапі проектування і подальшого виробництва технічного засобу.

1.3 Механізм виникнення та випромінювання електромагнітних завад

Відомо, що характер поля змінюється в залежності від відстані до передавального пристрою. Воно діліться на дві зони, ближню й далеку. Для ближньої зони відстань менше довжини хвилі і поле має яскраво виражений магнітній (або електричний) характер, а в дальній зоні поле носить явний електромагнітний характер і поширюється у вигляді плоскої хвилі, енергія якої діліться порівну між електричною та магнітної компонентами.

Оскільки довжина хвилі визначає відстань, і, тим більше, призначення, принцип роботи та інші характеристики, можна класифікувати випромінювачі електромагнітних сигналів на низькочастотні та високочастотні.

Низькочастотні випромінювачі (підсилювальні пристрої різного функціонального призначення і конструктивного виконання).

Високочастотні випромінювачі (ВЧ автогенератори, модулятори ВЧ коливань і пристрої, що генерують паразитні ВЧ коливання).

Також одним із факторів, що впливають на поширення електромагнітного поля в реальному середовищі, є вид провідників.

Наприклад, якщо струм протікає через ділянку одного електричного дроту, то напруженість поля, що створюється цим джерелом зменшується в міру віддалення від нього за лінійним законом в залежності від відстані.

Для двох паралельно прокладених провідників, розташованих на відстані один від одного, напруженість поля в міру віддалення від такого джерела зменшується за квадратичним законом.

Якщо розглядати кілька кільцевих витків провідника, по яких протікає струм, то у даному випадку спадання поля в залежності від відстані визначається кубічним законом.

Наведені вище найпростіші приклади свідчать про відмінність законів спаду поля в залежності від відстані для різних елементарних джерел. На практиці картина електромагнітного поля, створюваного реальним джерелом, виглядає набагато складніше[13]

1.4 Аналіз впливу електромагнітних засобів на сервіси безпеки

Якщо технічний засіб знаходиться під впливом ненавмисних ЕМЗ, то найчастіше це призводить до відмови у вигляді збою, тобто його функціонування може бути порушено.

Збоєм називається відмова, що одноразово виникає та самоусувається. Збій — подія, яка полягає у тимчасовій втраті працездатності об'єкта, що характеризується виникненням помилки при виконанні встановлених задач[12].

Збої спотворюють інформацію і призводять до помилкового рішення задачі, тобто до неправильного функціонування. Складність проблеми полягає в тому, що збій триває невеликий проміжок часу, після чого система відновлює працездатність і встановити локалізацію спотворення інформації важко.

Таким чином, збої у роботі технічних засобів знижують надійність і продуктивність систем захисту інформації.

У зв’язку із ущільненням компонентів в інтегральних схемах є підстава вважати, що ймовірність збоїв буде зростати, тобто проблема буде ставати все більш актуальною.

1.4.1 Ненавмисний вплив електромагнітних завад

Основна увага, як правило, приділяється захисту інформації від її можливого витоку, силового деструктивного впливу та несанкціонованого доступу до інформації, тобто прямому захисту інформації від навмисних дій порушників.

Але не менш важливим є питання захисту інформації від впливу ненавмисних ЕМЗ на ТЗПІ.

В електромережі ненавмисні ЕМЗ виникають через неякісне енергопостачання, відсутність або невірність виконання контуру заземлення будівлі, відсутність або невірність виконання інших необхідних заходів захисту.

Ненавмисні просторові ЕМЗ - завади від електротехнічного устаткування будівлі, в якій знаходиться приміщення ОІД: магнітне поле, що створюється побутовою технікою, кабельними лініями, розподільними щитками та

силовими трансформаторами, негативно впливає, як на технічні засоби, так і на людей, які працюють у приміщенні[11]

Складна негативна електромагнітна обстановка створюється також на робочих місцях з комп'ютерною системою, основним джерелом завад на яких є відеомонітор ПЕОМ та блоки електроживлення пристроїв комп'ютерної техніки.

Найчастіше негативна ЕМО в приміщенні виникає через невірне розташування електротехнічного устаткування будівлі та робочих місць з комп'ютерною технікою, порушення стандартів і норм прокладання кабельних систем електроживлення і встановлення електротехнічного обладнання.

До небажаних наслідків можуть також призвести неправильні розташування та конфігурації технічних засобів, оскільки поряд із ними можуть знаходитись потужні джерела ЕМЗ або провідникові конструкції.

Захист інформації від впливу ненавмисних ЕМЗ на ТЗПІ передбачає таку внутрішню організацію процесу оброблення інформації, щоб своїми діями не сприяти її спотворенню, блокуванню або втраті.

У переліку завдань, що вирішуються в рамках цього напрямку захисту інформації, домінуюче положення займає проблема забезпечення ЕМС ТЗПІ[9]

Проблема ЕМС охоплює практично всі сфери інформаційної діяльності суспільства, де використовуються та експлуатуються електронні, радіоелектронні та електротехнічні засоби.

Без розв’язання проблеми забезпечення ЕМС є неможливою якісна, а головне безпечна, з точки зору захисту інформації, експлуатація ТЗПІ.

Вимоги щодо забезпечення ЕМС регламентуються міжнародними та європейськими нормативними документами та стандартами. Згідно з ними технічні засоби будь-яких видів та призначень повинні відповідати не тільки

вимогам, спрямованим на захист від сприймання радіоперешкод, але і забезпечувати ЕМС електронних апаратів в умовах експлуатації.

Підтвердження відповідності технічних засобів діючим вимогам до параметрів ЕМС виконують мережі національних спеціалізованих випробувальних лабораторій.

1.4.1.1 Вплив індустріальних електромагнітних завад

У роботі проведено дослідження проблеми впливу ненавмисних електромагнітних завад на технічні засоби ОІД, тому із вище перерахованих завад особливу увагу приділено індустріальним завадам.

Електромагнітні індустріальні радіозавади – це завади, які ненавмисно створюються електричними чи електронними пристроями в діапазонах радіочастот (десятки Гц ... 3 ГГц) (до індустріальних радіозавад не відносяться випромінювання, які створюються антенними трактами радіопередавачів).

Пристрої - джерела індустріальних радіозавад у відповідності до їх функцій відносно електричної енергії можуть бути розподілені на чотири класи: генератори, користувачі, перетворювачі та каталізатори енергії.

Параметром завади від обчислювальної техніки є величина, яка характеризує своїм значенням конкретну властивість завади від технічного засобу. Таким значенням може бути, наприклад, амплітуда напруги чи струму імпульсу завади, довжина імпульсу чи характеристики послідовності імпульсних завад (середня частота послідовності імпульсних завад). До основних характеристик джерел індустріальних радіозавад можна віднести напруженості їх полів, струми, напруги і потужності[11].

Нормами на індустріальні радіозавади називаються допустимі значення напруг, напруженостей полів, струмів і перерахованих значень потужностей індустріальних радіозавад, виражених в децибелах відносно відповідно 1 мкВ, 1

мкВ/м, 2 мкВт, установлені на статистичній основі і регламентовані в нормативно-технічній документації[11]

Джерела електромагнітних індустріальних завад:

- наукові та побутові ВЧ пристрої;
- пристрої із двигунами внутрішнього згорання;
- електротранспорт;
- пристрої, які експлуатуються у житлових помешканнях;
- електричні підстанції;
- радіоприймальні пристрої;
- лінії електропередачі;
- пристрої провідникового зв'язку.

Випромінювані індустріальні завади створюють "середній фон" просторових завад. Значення "середнього фону" індустріальних завад відрізняється в залежності від характеру місцевості (для міських промислових, міських житлових і сільських районів) і залежить від частоти.

Крім загального фону індустріальних радіозавад необхідно враховувати і індивідуальні, особливо від близько розташованих джерел.

Аналіз результатів вимірювань рівнів індустріальних завад [11] показав, що:

- завади від автозапалювання, особливо в діапазоні частот 32 ... 47 МГц, діють на відстанях до кількох сот метрів від джерела;
- завади від ліній електропередачі (ЛЕП) виявлялися в діапазоні 30 ... 42 МГц, вище 43 МГц вони не відчутні;
- суттєві рівні завад від електричного транспорту спостерігаються в діапазоні 1,5 ... 8 МГц;

– значні рівні завад у вигляді потужних сплесків від тиристорних випрямних пристроїв виявлені головним чином в діапазоні 14,75 ... 14,85 МГц.

Стосовно завад від засобів обчислювальної техніки, слід відмітити, що вони нерегулярні у часі. Але вони виявляються у мережі загального призначення у вигляді кондуктивних і, як наслідок, у вигляді випромінюваних завад, відчутних на значних відстанях (сотні метрів) від мережі живлення.

Частотні діапазони ЕМЗ окремих пристроїв ПЕОМ наведені у таблиці 1.[12]

Таблиця 1.1 - Частотні діапазони ЕМЗ пристроїв ЕОМ

Джерело	Діапазон частот
Монітор: - мережевий трансформатор блоку живлення - статичний перетворювач напруги в імпульсному блоці живлення - блок кадрової розгортки синхронізації - блок рядкової розгортки синхронізації	 50 Гц 20…10 кГц 48…160 Гц 15…110 кГц
Системний блок(процесор)	50 Гц…1000 МГц
Пристрою введення/виводу інформації	0 Гц 50 Гц
Джерела безперервного живлення	50 Гц 20…100 кГц

Електромагнітні завади, які сприймаються ПЕОМ, наведені нижче у таблиці 1.2[11]

Таблиця 1.2 – Електромагнітні завади, які сприймаються ЕОМ

Завада	Характеристика
Симетрична завада від ЕОМ	Завада від ЕОМ, яка спостерігається у вигляді напруги довільної форми між фазним і нульовим чи двома фазними вводами провідників від джерела первинного електроживлення чи між вводами провідників лінії зв'язку обчислювальної машини
Несиметрична завада від ЕОМ	Завада від ЕОМ, яка спостерігається у вигляді напруги довільної форми між вводами провідників від джерела первинного електроживлення чи вводом провідника лінії зв'язку ЕОМ і затискачем заземлення корпусу
Провал напруги живлення в обчислювальній машині	Зовнішня завада ЕОМ, яка являє собою зниження напруги електроживлення обчислювальної машини від номінального значення в інтервалі часу, який перевищує сталу часу перехідної функції за напругою джерел вторинного електроживлення ЕОМ
Перенапруження в мережі живлення ЕОМ	Зовнішня завада ЕОМ, яка являє собою підвищення напруги в джерелі первинного електроживлення ЕОМ від номінального значення в інтервалі часу, який перевищує сталу часу перехідної функції за напругою джерел вторинного електроживлення ЕОМ

Продовження таблиці 1.2

Завада	Характеристика
Нееквіпотенціальність заземлення ЕОМ	Зовнішня завада ЕОМ, яка являє собою різницю потенціалів між затискачем заземлення корпусів даної ЕОМ і приладу, який не є її частиною, але з'єднується з нею провідниками лінії зв'язку
Індукована електрорушійна сила на обчислювальну машину (наводка)	Завада обчислювальній машині (частині ЕОМ), яка виникає внаслідок непередбаченої схемою і конструкцією обчислювальної машини (частини ЕОМ) передачі за зв'язками напруги, струму, заряду чи магнітного потоку від джерела завади в частину ЕОМ, яка розглядається, в залежності від того, є чи ні джерело завад, яке викликає наводку, частиною ЕОМ. Відрізняють відповідно власну і зовнішню наводку. В залежності від фізичної природи зв'язку відрізняють ємнісну, індуктивну наводку і наводку загальному повному опорові
Розряд на корпус обчислювальної машини	Зовнішня завада ЕОМ, яка являє собою розряд зарядженого конденсатора чи провідникового тіла на провідниковий корпус ЕОМ
Поле завад обчислювальної машини	Завада ЕОМ, яка являє собою електромагнітне поле у просторі, який оточує ЕОМ чи її частину, створене зовнішнім чи власним джерелом

1.4.2 Навмисний вплив електромагнітних завад

Силовий деструктивний вплив на сьогоднішній день є серйозною проблемою з точки зору систем захисту інформаційних об'єктів.

Навмисне деструктивний вплив - це імпульси руйнуючого або вражаючого (деструктивного) впливу штучного походження, що здатні дистанційно і без шуму впливати на інформаційну систему.

Найбільшою мірою силовий деструктивний вплив відноситься до потужних мобільних технічних засобів, які можуть діяти як на території, що охороняється, так і на значній відстані. В даний час засоби силового деструктивного впливу можуть не тільки вивести апаратури з ладу, а й блокувати нормальне її функціонування[31].

Технічні засоби деструктивного впливу компактні, мають високу проникаючу здатність і ефективність дії, потаємні у застосуванні.

Головною метою при їх застосуванні є забезпечення відповідної потужності електромагнітного імпульсу, що впливає на систему з ланцюгів живлення або по каналах зв'язку.

Силовий деструктивний вплив на електронне обладнання інформаційної системи може бути реалізований трьома основними каналами:

- по мережі живлення;
- по провідних лініях зв'язку;
- по ефіру з використанням потужних коротких електромагнітних імпульсів.

На відміну від інших способів знищення інформації, обладнання чи методів проникнення на об'єкт, що охороняється, застосування технічних засобів деструктивного впливу потребує значно менших інтелектуальних і матеріальних витрат. Крім того, наслідки від такої атаки на об'єкт можуть бути сприйняті постраждалими як звичайні порушення функціонування об'єкта, наприклад, порушення в мережі електроживлеення об'єкт[31]

1.5 Аналіз факторів, що впливають на поширення електромагнітного поля завад

Проаналізувавши функціональні вузли апаратури, що обробляє інформацію, як самостійні джерела електромагнітного поля, можна виділити наступні фактори, що впливають на поширення цього поля:

- Просторова конфігурація самостійного джерела, як правило, дуже складна. Навіть найпростіший з'єднувальний монтаж елементів на друкованій платі має досить розгалужену структуру. Напруженість електромагнітного поля від такого джерела також має досить складну структуру;
- Напруженість електромагнітного поля у довільній точці простору визначається суперпозицією полів, визначених випромінюваннями елементарних ділянок розглянутого самостійного джерела випромінювання;
- Картина електромагнітного поля випромінювання від ТЗ, що обробляє інформацію, суттєво відрізняється в різних напрямках від нього;
- Закон спаду електромагнітного поля різний для різних джерел. Причому, це твердження вірне навіть для однакових з точки зору виробництва пристроїв [18].

Це обумовлено фізичними розбіжностями в параметрах елементної бази самого пристрою, можливістю застосування в однотипних пристроях елементів, що відрізняються один від одного за другорядними параметрами, які не впливають на працездатність виробу, відмінностями у взаємному розташуванні та з'єднанні елементів;

- Характер випромінювання від ТЗ може змінюватися у часі;
- Закон спаду поля в просторі залежить від ряду зовнішніх чинників.

1.5.1 Параметри електромагнітного поля ненавмисних завад

1.5.1.1 Аналіз допустимих рівнів електромагнітного поля

Для того, щоб усі технічні засоби могли функціонувати не піддаючись впливу ненавмисних ЕМЗ, встановлено допустимі норми напруги і напруженості поля радіозавад пристроїв промислового, побутового і наукового призначення. За енергетичним спектром групи електромагнітних полів чітко розділені на два частотних піддіапазона: перший піддіапазон – 5 Гц…2 кГц, другий піддіапазон – 2 кГц… 400 кГц. Цей факт використовується при випробуваннях комп'ютерної техніки, коли при оцінці її якості вимірюють рівні полів, що створюються, в широкій смузі пропускання. Вибір зазначених частот виміру визначається особливістю частотного спектра полів, які створюються дисплеями ПЕОМ.

В таблиці 1.3 наведені діапазони значень електромагнітних полів, які були отримані при вимірюванні робочих місць з ПЕОМ[11].

Найменування вимірюваних параметрів	Діапазон частот 5 Гц - 2 кГц	Діапазон частот 2 - 400 кГц
Напруженість змінного електричного поля, (В/м)	1,0 – 35,0	0,1 – 1,1
Індукція змінного магнітного поля, (нТл)	6,0 – 770,0	1,0 – 32,0

Для аналізу норм на рівні електромагнітних полів з використанням різних діючих стандартів розглянуто дані шведського стандарту MPR II, Санітарних правил и норм 2.2.2.542-96 "Гігієнічні вимоги до відеодисплейних терміналів, персональних ЕОМ і організації работи", а також Стандарту безпеки ТСО'95[17], що поширюється на весь персональний комп'ютер, тобто на монітор, системний блок, клавіатуру, і стосується ергономічних властивостей, випромінювань режимів енергозбереження та екології.

У таблиці 1.4 наведено результати порівняння даних, отриманих зі стандартів. Норми на рівні електромагнітних полів, регламентовані діючими стандартами, у двох частотних піддіапазонах мають певні відмінності.

Таблиця 1.4

Діапазон частот	MPR II	СанПіН 2.2.2.542-96	ТСО 95
Електростатичний потенціал	±500 В	±500 В	±500 В
Електричне поле 5 Гц…2 кГц (смуга 1)е поле	≤25 В/м	≤25 В/м	≤10 В/м
2 кГц…400 кГц (смуга 2)	≤25 В/м	≤25 В/м	≤1 В/м
Діапазон частот	MPR II	СанПіН 2.2.2.542-96	ТСО 95
Вище 400 кГц	-	-	-
Магнітне поле 5 Гц…2 кГц (смуга 1)	≤250 нТл	≤250 нТл	≤200 нТл
2 кГц…400 кГц (смуга 2)	≤25 нТл	≤25 нТл	≤25 нТл
Вище 400 кГц	-	-	

Аналіз цих даних дозволяє зробити висновок, що для вимірювань електромагнітних полів не може використовуватись широкосмугові вимірювальні прилади, оскільки вони не дозволяють чітко ідентифікувати рівень полів в кожному з названих вище піддіапазонів частот.

Неефективне також використання для таких вимірювань вузькосмугових (селективних) вимірювальних приймачів, оскільки при цьому процес виміру та визначення сумарної енергії поля в заданому діапазоні частот за результатами виміру його спектральних складових буде дуже складним та тривалим.

1.5.3 Аналіз допустимих значень напруги та напруженості поля електромагнітних завад

Пристрої, які призначені для експлуатації на промислових та інших підприємствах, розташованих поза межами житлових будинків, повинні відповідати наступним вимогам, наведеним у таблиці 1.5.

Таблиця 1.5 - Допустимі значення напруженості поля завад від пристроїв, розташованих поза межами житлових будинків

Параметр	Характеристика
Відстань випромінювання, м	30 – від установки при вихідному випуску, 10 – від межі території підприємства при випробуваннях в умовах експлуатації
Допустиме значення напруженості поля, дБ, у смузі частот 0,15...1000 МГц	70 – на робочих частотах і частотах гармонік у межах виділених частотних смуг 32 – на частотах гармонік та інших побічних частотах поза виділеними частотними смугами

Пристрої, які призначені для експлуатації в житлових будинках чи установах, електричні мережі яких підключені до електричних мереж житлових будинків, повинні відповідати вимогам, наведеним у таблиці 1.6.

Таблиця 1.6 - Допустимі значення напруги та напруженості поля завад від пристроїв, підключених до електричних мереж житлових будинків

Параметр	Характеристика
Місце підключення	Мережні затискачі установки. Розподільний щит електроживлення пристрою при випромінюваннях в умовах експлуатації
Відстань випромінювання, м	10 – від установки при випуску і при випромінюваннях в умовах експлуатації
Допустима напруга радіозавад, дБ, у смузі частот 0,15...30 МГц	52

Продовження таблиці 1.6

Параметр	Характеристика
Допустиме значення напруженості поля, дБ, у смузі частот 0,15...1000 МГц	32 – на робочих частотах і частотах гармонік у межах виділених частотних смуг та поза виділеними частотними смугами

На електротехнічні пристрої побутового, комунального та наукового призначення, які експлуатуються в житлових будинках чи підприємствах, електричні кола яких підключені до мереж житлових будинків, норми квазіпікових значень напруг радіозавад (в децибелах відносно 1 мкВ) не повинні перевищувати значень, які наведені графічно на рисунках 1.7-1.12.

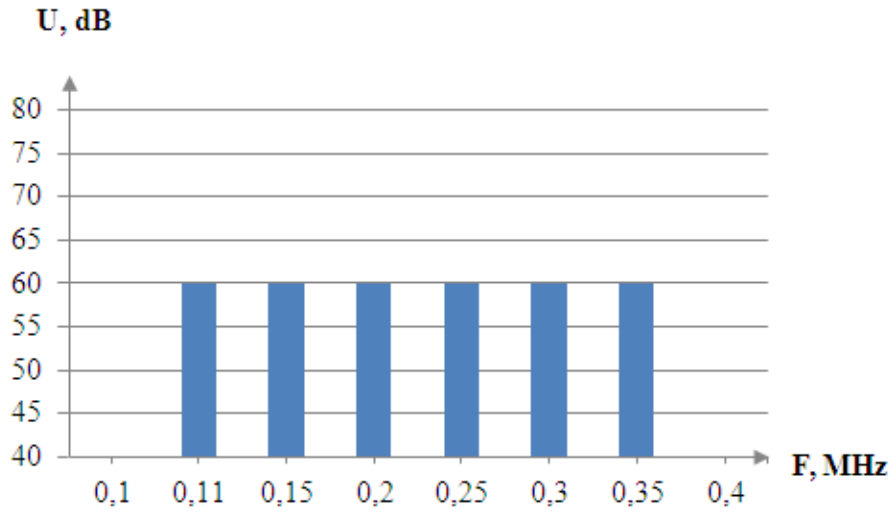

Рисунок 1.7 - Максимально допустимі норми значень напруг радіозавад на мережних затискачах електроприладів (крім переносних електричних інструментів, ліфтів, а також електроприладів з терморегуляторами)

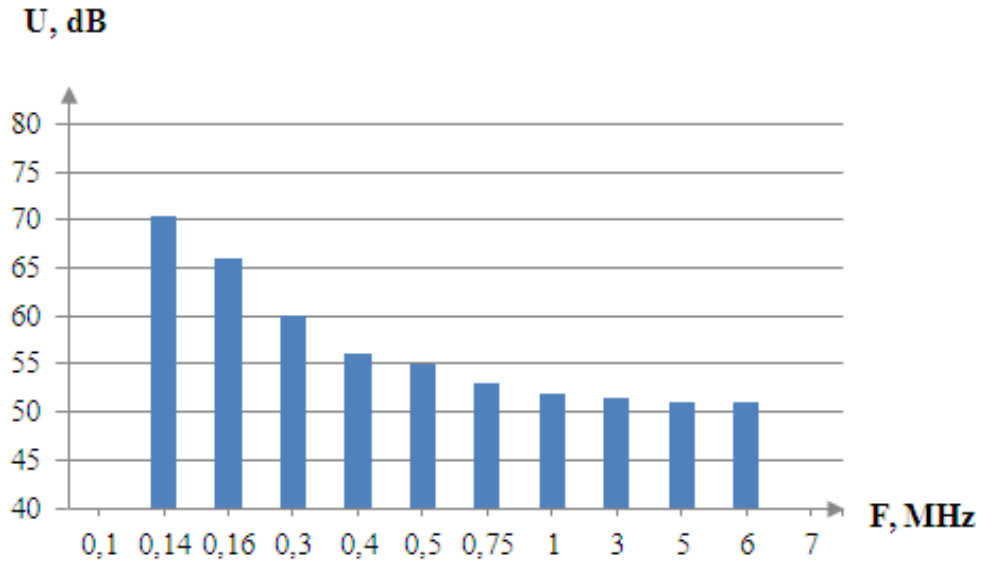

Рисунок 1.8 - Максимально допустимі норми значень напруг на мережних затискачах переносних електричних інструментів, ліфтів

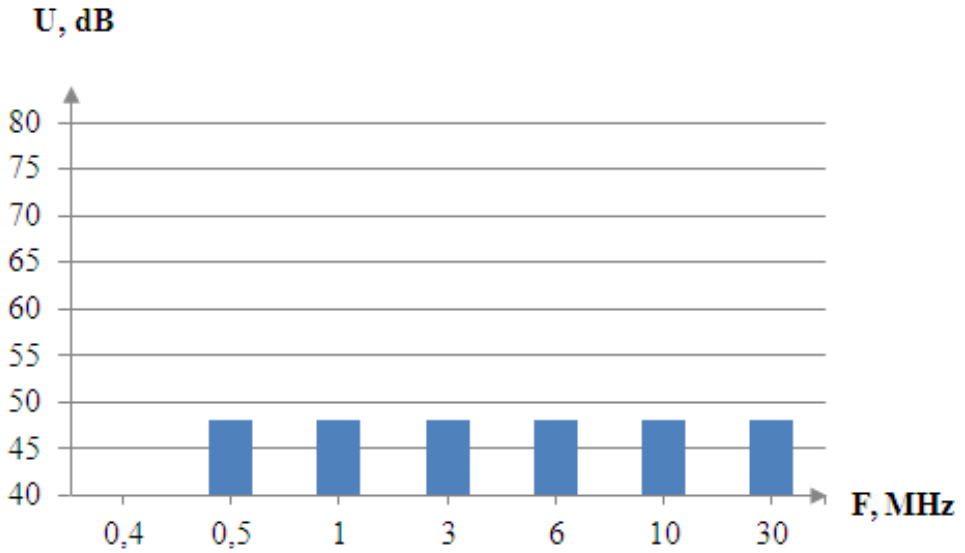

Рисунок 1.9 - Максимально допустимі норми значень напруг на мережних затискачах електроприладів та допустимі норми для переносних електричних інструментів, ліфтів у діапазоні 0,5-30 МГц

На частотах 0,5 і 2,5 МГц допустимими значеннями напруг (напруженостей полів) радіозавад слід вважати більші значення.

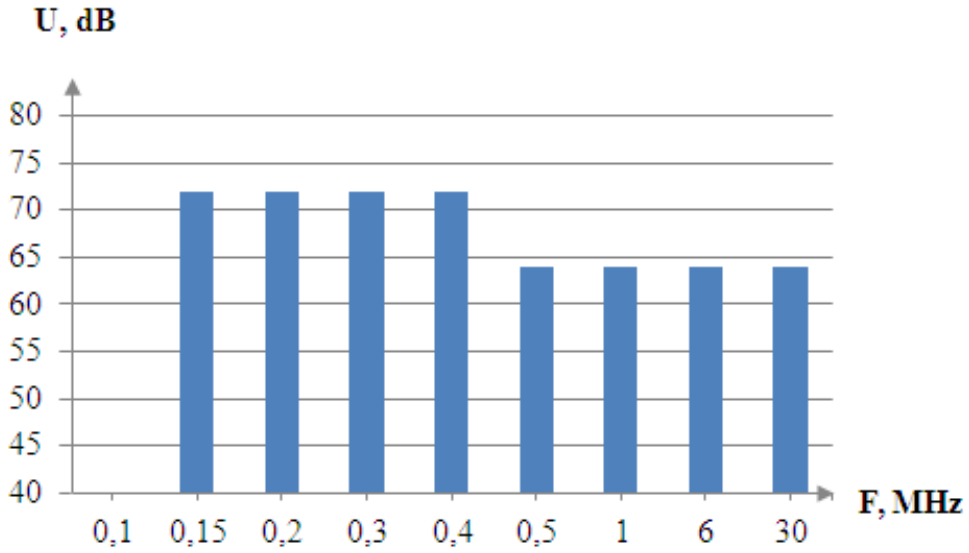

Рисунок 1.10 - Максимально допустимі норми значень напруг на затискачах для приєднання зовнішніх пристроїв (електричних навантажень, виконуючих пристроїв, органів керування, регулювання, комутації тощо)

Значення напруженості поля радіозавад (в децибелах відносно 1 мкВ/м) не повинні перевищувати допустимих значень випромінювання радіозавад, які наведені графічно на рисунках 1.11 – 1.12.

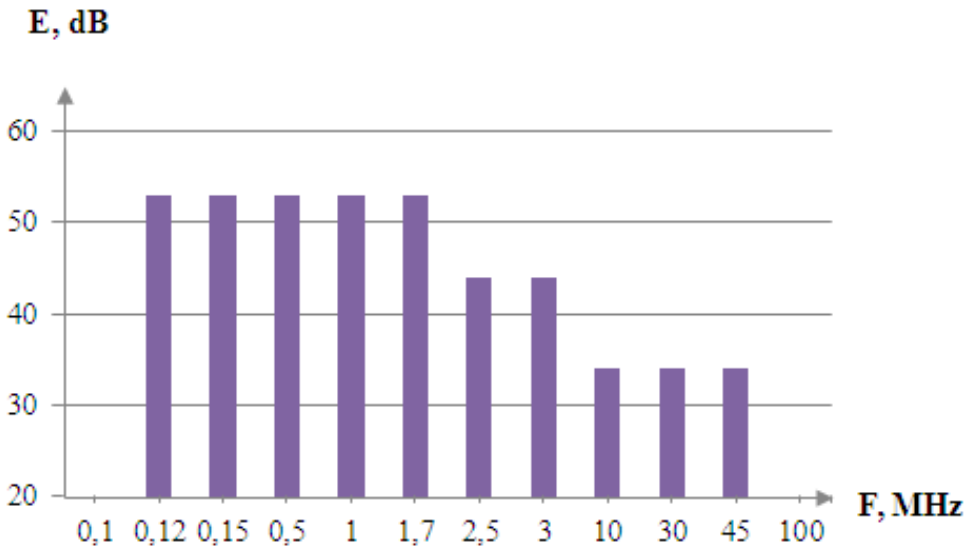

Рисунок 1.11 - Максимально допустимі норми значень напруженості поля радіозавад для електроприладів з автономним живленням, які не підключені до електричної мережі

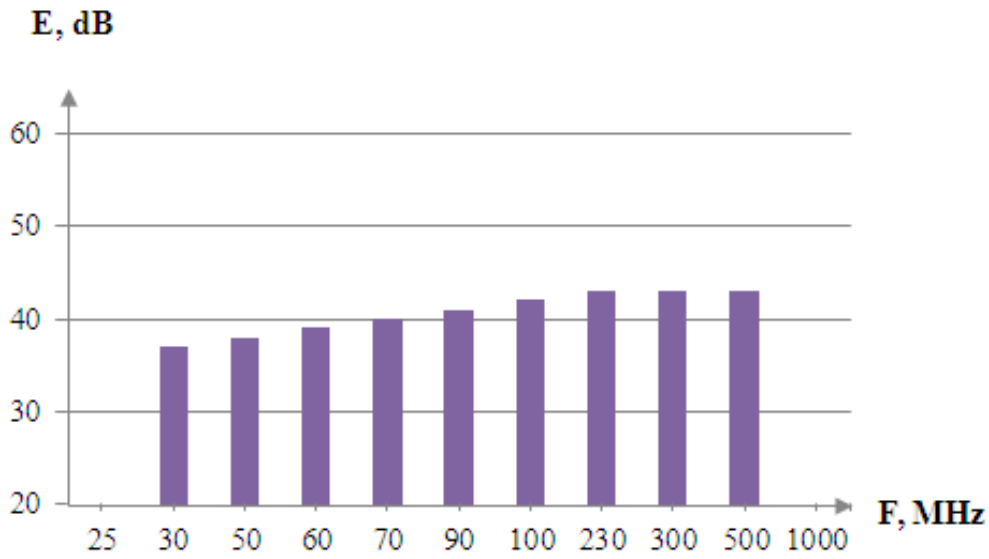

Рисунок 1.12 - Максимально допустимі норми значень напруженості поля радіозавад для електроприладів з автономним живленням і тих, які підключені до електричної мережі

Побудовані графіки та таблиці дозволяють побачити чітку картину допустимих норм напруги та напруженості поля ЕМЗ для різних типів приладів у різних частотних діапазонах.

Висновки за розділом 1

У даному розділі було розглянуто поняття вплив електромагнітних випромінювань та електромагнітна сумісність технічних засобів. Механізм виникнення електромагнітних завад Був проведений аналіз завад за видом, класом та середовищем розповсюдження.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ТА ЗАХИСТУ ВІД ВПЛИВУ ЕЛЕКТРОМАГНІТНИХ ЗАВАД

2.1 Екранування

2.1.1 Екранування технічних засобів

Одним із істотних недоліків більшості технічних засобів обробки інформації, які використовуються на ОІД, є наявність можливості спотворення, знищення інформації або навіть втрати працездатності через вплив зовнішніх ненавмисних електромагнітних випромінюванням (імпульсу).

Екранування - це один із заходів захисту технічних засобів від впливу зовнішніх електромагнітних полів, а також локалізації будь-яких випромінювань, що унеможливлює їх виток у зовнішньому середовищі.

Для захисту від шкідливого впливу електромагнітного випромінювання використовуються наступні заходи екранування:

- еканування всього технічного засобу обробки інформації;
- екранування окремих елементів технічних засобів;
- екранування робочих місць;
- індивідуальне екранування;
- використання екрануючих поглинаючих засобів.

Розрізняють електростатичне, магнітостатичне та електромагнітне екранування.

Електростатичне і магнітостатическое екранування засновані на замиканні екраном (який має в першому випадку високу електропровідність, а в другому - магнітопровідність) відповідно електричного і магнітного полів.

Електростатичне екранування призводить до замикання електростатичного поля на поверхню металевого екрана та відведення електричних зарядів на землю (на корпус пристрою) [14].

Основна задача електростатичного екранування – зменшення ємнісних зв’язків між елементами, що потребують захисту що забезпечуються шляхом накопиченням статичної електрики на екрані з послідуючим відводом зарядів на землю[10].

Необхідною умовою при реалізації електростатичного екранування є надійне заземлення екрану. При застосуванні металевих екранів досягається повне усунення впливу електростатичного поля[14].

Ефективність екранування визначається в основному с співвідношенням ємностей зв'язку між джерелом і рецептором наведення до і після застосування електростатичного екрану. Зменьшення ємності зв'язку збільшує ефективність екранування[5].

Ефективність електростатичного екранування також залежить від величін електропровідності екрану та опору кола заземлення. Чим вища електропровідність екрану та кола заземлення, тим вище ефективність електростатичного екранування. Товщина екрану та його магнітні властивості на ефективність екранування практично не впливають.

Екрануюча здатність металевого листа істотно залежить від якості з'єднання екрану з корпусом приладу і частина екрану одна з одною. Принципово важливим є відсутність з'єднувальних дротів між частинами екрана і корпусом.

У діапазонах метрових і більш коротких довжин хвиль з'єднувальні провідники довжиною в кілька сантиметрів можуть різко погіршити ефективність екранування. На хвилях дециметрового та сантиметрового діапазонів з'єднувальних провідників та шин між екранами неприпустимо. Для отримання високої ефективності екранування електричного поля в цих випадках необхідно

застосовувати безпосереднє суцільне з'єднання окремих частин екрану одну з одною[14].

Наявність вузьких щілин і отворів в металевому екрані, розміри яких порівняно малі з довжиною хвилі, практично не погіршує екранування електричного поля.

Зі збільшенням частоти ефективність екранування знижується.

Основні вимоги до електричних екранів, можна сформулювати наступним чином[14,5]:

– конструкція екрану повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрану, не виходячи за його межі;
– в області низьких частот (при глибині проникнення (δ) більше товщини (d), тобто при δ > d) ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрана з корпусом пристрою і мало залежить від матеріалу екрану і його товщини;
– в області високих частот (при d < δ) ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідністю і магнітною проникністю.

При необхідності зниження рівня наводок на низких частотах від 0 до 3 ... 10 кГц.

Основні вимоги до магнітостатичних екранів можна звести до наступних[14]:

– магнітна проникність матеріалу екрану повинна бути якомога вищою. Для виготовлення екранів бажано використовувати магніто м’які матеріали з високою магнітною проникністю (наприклад, пермалой);
– збільшення товщини стінок екрана призводить до підвищення ефективності екранування, однак при цьому слід можливі конструктивні обмеження через масу і габаритами екрану;

– стики, розрізи і шви в екрані повинні розміщуватися паралельно лініям магнітної індукції магнітного поля. Їх кількість повинна бути мінімальною;

– заземлення екрана не впливає на ефективність магнітостатичного екранування.

Ефективність магнітостатичного екранування підвищується при застосуванні багатошарових екранів. Вона також залежить від частоти електромагіного поля та електричних властивостей матеріалу екрана. Чим нижче частота, тим нижче ефективність екрану, через що доводиться робити його більшої товщини для досягнення того ж екрануючого ефекту.

Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого металу товщиною 0,5 ... 1,5 мм діє дуже ефективно. При виборі товщини і матеріалу екрану слід враховувати механічну міцність, жорсткість, стійкість проти корозії, зручність виконання стиковки окремих деталей і творення між ними перехідних контактів з малим опором, зручність пайки, зварювання та ін[19].

Для частот вище 10 МГц мідна, і тим більше срібна плівка товщиною більше 0,1 мм дає значний екрануючий ефект. Тому на частотах вище 10 МГц цілком припустимо застосування екранів з фольгованого стеклотекстоліту або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям.

На високих частотах застосовується виключно електромагнітне екранування. Дія електромагнітного екрана заснована на тому, що високочастотне електромагнітне поле послаблюється ним же створеним (завдяки створеним в товщі екрану вихровим струмам) полем зворотного напрямку.

При екрануванні магнітного поля заземлення екрана не впливає на ефективність магнітного екранування.

Екранування магнітного випромінювання досягається в результаті дії двох фізичних явищ:

- шунтування магнітних силових ліній поля в екран із феромагнітних матеріалів (з $\mu >> 1$), обумовленого суттєво меншим магнітним опором матеріалу екрана, ніж навколишнього повітря;
- виникнення під дією магнітного екрануючого поля в струмопровідному середовищі екрану індукційних вихрових струмів, що створюють вторинне магнітне поле, силові лінії якого протилежні магнітним силовим лініям первинного поля.

Необхідна ефективність екрану залежно від його призначення і величини рівня електромагнітного випромінювання зазвичай знаходиться в межах 60 ... 120дБ[10]

Електромагнітне екранування забезпечується за рахунок віддзеркалення частини випромінювання від поверхні екрану та поглинання частини випромінювання екраном.

В якості матеріалів для електромагнітних екранів обирають ті, які мають високу електропровідність: латунь, алюміній.

2.1.2 Екранування дротів та з’єднувальних ліній

Разом із блоками апаратури екрануванню підлягають монтажні дроти і з’єднувальні лінії.

Щоб зменшити рівень електромагнітних випромінювань, необхідне ретельне виконання з'єднання оболонки дроту (екрана) з корпусом апаратури. Підключення оболонки має здійснюватися шляхом безпосереднього контакту (краще за все шляхом пайки або зварювання) з корпусом[18]

Разом із тим з'єднання оболонки дроту з корпусом в одній точці не послаблює в навколишньому просторі магнітне поле, що створюється через протікання струму по дроту.

Для екранування магнітного поля необхідно створити поле такої ж величини і зворотного напрямку. З цією метою необхідно весь зворотний струм кола, що екранується, направити через екрановану оплітку дроту[18].

Висока ефективність екранування забезпечується при використанні витої пари, захищеної екрануючою оболонкою.

На низьких частотах треба використовувати більш складні схеми екранування - коаксіальні кабелі з подвійною опліткою (тріаксіальні кабелі)[18].

На більш високих частотах, коли товщина екрана значно перевищує глибину проникнення поля, необхідності у подвійному екрануванні немає. У цьому випадку зовнішня поверхня грає роль електричного екрана, а по внутрішній поверхні протікають зворотні струми.

Застосування екрануючої оболонки істотно збільшує ємність між дротом і корпусом, що в більшості випадків небажано. Екрановані дроти мають більші габарити і незручні при монтажі, потребують запобігання випадкових з’єднань зі сторонніми елементами і конструкціями.

Довжина екранованого монтажного проводу повинна бути менше чверті довжини найкоротшої хвилі спектру сигналу, що передається по дроту.

Для зменшення взаємного впливу монтажних ланцюгів слід вибирати довжину монтажних високочастотних проводів найменшою, для чого елементи високочастотних схем, пов'язані між собою, слід розміщувати в безпосередній близькості, а неекрановані проводи високочастотних кіл - при перетині під прямим кутом[18]

При паралельному розташуванні такі проводи повинні бути максимально віддалені один від одного або розділені екранами, у якості яких можуть бути використані несучі конструкції електронної апаратури (кожух, панель і т.д.).

Екрановані проводи та кабелі слід застосовувати в основному для з'єднання окремих блоків і вузлів один з одним.

Екрани кабельні виконуються у формі циліндра з суцільних оболонок, у вигляді спірально намотаною на кабель плоскою стрічкою або у вигляді обплетення з тонкого дроту. Екрани при цьому можуть бути одношаровими і багатошаровими комбінованими, виготовленими зі свинцю, міді, сталі, алюмінію та їх поєднань (алюміній-свинець, алюміній-сталь, мідь-сталь-мідь і т.д.)[20].

У кабелях із зовнішніми пластмасовими оболонками застосовують екрани стрічкового типу в основному з алюмінієвих, мідних і сталевих стрічок, накладених спірально або поздовжньо уздовж кабелю[18]

В області низьких частот корпуси багатоштирькових низькочастотних роз'ємів є екранами і повинні мати надійний електричний контакт із загальною шиною або землею приладу, а зазори між роз'ємом і корпусом повинні бути закриті електромагнітними ущільнювальними прокладками.

В області високих частот коаксіальні кабелі повинні бути узгоджені по хвильовому опору з високочастотними роз'ємами, які використовуються. При закладенні коаксіального кабелю в високочастотні роз'єми жила кабелю не повинна мати натяг у місці з'єднання з контактом роз'єму, а сам кабель повинен бути жорстко прикріплений до шасі апаратури поблизу виводу[18]

Для ефективного захисту від впливу низькочастотних полів застосовуються екрани, виготовлені з феромагнітних матеріалів з великою відносної магнітної проникністю. При наявності такого екрану лінії магнітної індукції проходять в основному по його стінках, що мають малий опір у порівнянні з опором повітряного простору усередині екрану[18]

Якість екранування таких полів залежить від магнітної проникності екрану і опору магнітопровода, який буде тим менше, чим більша товщина екрану, що йдуть упоперек напряму ліній магнітної індукції.

Найбільш економічним способом екранування інформаційних ліній зв'язку між технічними засобами вважається групове розміщення їх інформаційних

кабелів в екрануючий розподільний короб. Коли такого короба не має, то необхідно екранувати окремі лінії зв'язку[18]

Для захисту ліній зв'язку від наводок необхідно розміщувати лінію в екрануючу оплітку або фольгу, заземлену в одному місці, щоб уникнути протікання по екрану струмів, викликаних нееквіпотенціальністю точок заземлення[18]. Також треба мінімізувати площа контуру, утвореного прямим і зворотним проводами лінії. Якщо лінія – це одиночний дріт, а обернений струм тече по деякій заземлюючій поверхні, то необхідно максимально наблизити дріт до поверхні. Якщо лінія утворена двома проводами, то їх необхідно скрутити, утворивши кручену пару.

Найкращий захист як від електричного, так і від магнітного полів забезпечують інформаційні лінії зв'язку типу екранованого біфіляра, тріфіляра (трьох скручених разом проводів, з яких один використовується в якості електричного екрана), тріаксільного кабелю (ізольованого коаксіального кабелю, поміщеного в електричний екран), екранованого плоского кабелю (плоского багатодротового кабелю, покритого з однієї або обох сторін мідною фольгою)[18].

2.2 Фільтрація

Окрім прямого впливу електромагнітних випромінювань на елементи інформаційних систем, необхідна організація захисту від наводок у кабелі живлення та інших колах, що виходять з приміщення, яке підлягає захисту. З цією метою застосовують різні способи фільтрації.

З позицій технічного захисту інформації фільтрація - це один з методів локалізації небезпечних сигналів, які циркулюють в ТЗПІ.

Фільтрацію в технічному засобі реалізують для виключення впливу зовнішніх ЕМЗ на рецептор по всіх з'єднаннях і входах, а також для захисту кабельних ліній від перешкод, які створюються самим засобом. Крім цього фільтри використовуються для виключення впливу перешкод в ланцюгах управління, контролю і комутації.

Для реалізації фільтрації у колах живлення ТЗПІ застосовують розподільні трансформатори і завадоподавляючі фільтри.

Розподільні трансформатори - використовуються для розв'язки первинного та вторинного ланцюгів за сигналами наводки, тобто до вторинного ланцюга трансформатора не повинні проникати наводки, що з'являються в ланцюзі первинної обмотки. Причина проникнення - наявність небажаних резистивних і ємнісних зв'язків між наводками.

Фільтри нижніх частот, що встановлюються в силові та сигнальні вводи в приміщення, відносяться до пасивних засобів захисту.

Фільтр звичайно представляє собою Г-, Т- або П-подібні LC-ланки, що включаються в розрив фази і нульового проводів мережі живлення.

Фільтри в силових колах мають одну або декілька П-подібних ланок. У якості складових елементів фільтрів часто використовуються прохідні конденсатори. Прохідний конденсатор - конденсатор, одна з обкладок якого включається в розрив лінії, що несе значний струм.

Мережеві фільтри в колах живлення ТЗПІ виконують 2 основні функції:

- захист апаратури від зовнішніх імпульсних перешкод;
- захист від наводок, що створюються самою апаратурою.

Завадоподавляючі фільтри використовуються для послаблення небажаних сигналів на різних ділянках частотного діапазону. Основне їх призначення - пропускати без значного послаблення сигнали з частотами, що лежать за межами цієї смуги.

Основні вимоги до захисних фільтрів:[11]

- величина робочої напруги і струму фільтра повинні відповідати напрузі й струму фільтрованого кола;
- величина ослаблення небажаних сигналів в діапазоні робочих частот повинна бути менше необхідної;

- ослаблення корисного сигналу в смузі прозорості фільтру повинно бути незначним;
- габарити і маса повинні бути мінімальними;
- фільтри повинні забезпечувати функціонування при певних умовах експлуатації (температура, вологість, тиск) і механічних тисках (удари, вібрації і т.д.);
- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

До фільтрів кіл живлення висувають наступні додаткові вимоги:

- загасання, що вноситься такими фільтрами в кола постійного або змінного струму основної частоти, повинні бути мінімальним (наприклад, 0.2дБ і менше) і мати велике значення (більше 60 дБ) у смузі придушення (вона повинна бути досить широкою (до 10 ГГц));
- мережеві фільтри повинні ефективно працювати при великих значеннях струмів, високих напругах і високих рівнях потужності затримуваних електромагнітних коливань.

Конструктивно фільтри поділяються на:

- фільтри на елементах з зосередженими параметрами (LC-фільтри) - для роботи на частотах до 300МГц;
- фільтри з розподіленими параметрами (смугові, коаксіальні або хвилеводні) для роботи на частотах понад 1 ГГц;
- комбіновані (для роботи на частотах 300 мГц - 1 ГГц).

Цей фільтр встановлюється між щитом живлення будівлі і системою розводки силових кіл по будівлі (поверху).

Для досягнення високого загасання фільтри повинні бути заземленими, причому заземлення має бути ефективним у всьому розглянутому діапазоні частот.

Якщо фільтр неекранований, а сигнал подається за допомогою неекранованих проводів, то згасання буде не більше 40 - 60 дБ.

Для згасання більше 60 дБ необхідно застосовувати екрановані фільтри з роз'ємами і екрановані проводи[18]

У будь-якому випадку правильне використання фільтрів під час монтажу обладнання системи, яка обробляє інформацію, що підлягає захисту, дозволить запобігти її спотворення або втрату під впливом ненавмисних елктромагнітних завад.

2.3 Заземлення

На високих частотах виявляється так званий поверхневий, або скін-ефект, який запобігає проникненню електромагнітних полів всередину екрану. Ефект полягає в тому що, чим вище частота змінного струму через провідник, тим ближче до поверхні провідника тече цей струм.

Тому навмисна або випадкова електромагнітна хвиля відбивається від зовнішньої поверхні екрану. На це фізичне явище не впливає заземлення. Але на низьких частотах, коли опір екрану зменшується і струми починають вільно поширюватися по екрану і захисній мережі, заземлення стає вкрай необхідним.

Заземлення екрана на одному кінці дроту забезпечує додатковий захист сигналу від низькочастотних електричних полів, а захист від магнітних полів створюється за рахунок сплетення провідників у виту пару.

При заземленні з двох сторін утворюється струмова петля, в якій випадкове магнітне поле генерує струм. Його напрям такий, що створюване ним магнітне поле нейтралізує впливає випадкове або навмисне поле. Таким чином, шляхом двостороннього заземлення здійснюється захист від впливу випадкових магнітних полів.

При використанні двостороннього заземлення для випадкових або навмисно створених струмів створюється альтернативний шлях по мережі заземлення. Якщо струми стають занадто великими, кабельний екран може не впоратися з ними.

У цьому випадку для того, щоб відвести випадкові струми від екрана, необхідно забезпечити інший шлях, наприклад, паралельну шину для «землі». Рішення про її створення залежить від якості мережі заземлення, системи розводки живлення що застосовується, величини паразитних струмів в мережі заземлення, електромагнітних характеристик середовища і т. п.

Екранування ТЗПІ та з'єднувальних ліній ефективно тільки при їх правильному заземленні.

На практиці у ролі заземлювачів найчастіше використовуються:

- стрижні з металу, що мають високу електропровідність, занурені у земли і з'єднані з наземними металоконструкціями технічних засобів;
- сіткові заземлювачі, виготовлені з елементів з високою електропровідністю і занурені в землю (в якості доповнення до заземлювальних стрижнів).

При підвищених вимогах до величини опору заземлення (опір заземлення ТЗПІ не повинен перевищувати 4 Ом[19]) застосовують багаторазове заземлення, що складається з ряду одиночних симетрично розташованих заземлювачів, з'єднаних між собою.

Заземлення технічних засобів систем інформатизації та зв'язку має бути виконано відповідно до певних правил. Основні вимоги, які пред'являються до системи заземлення, полягають у наступному[15]:

- система заземлення повинна включати загальний заземлювач, заземлюючий кабель, шини і дроти, що сполучають заземлювач з об'єктом;
- опори заземлюючих провідників, а також шин заземлення повинні бути мінімальними;
- кожен елемент, що заземлюється, повинен бути приєднаний до заземлювача або до заземлюючої магістралі за допомогою

окремоговідведення. Послідовне включення в заземлюючий провідник декількох елементів забороняється;

- у системі заземлення мають бути відсутні замкнуті контури, утворені з’єднаннями або небажаними зв'язками між сигнальними колами і корпусами пристроїв, між корпусами пристроїв і землею;
- слід уникати використання загальних провідників у системах екрануючих заземлень, захисних заземлень і сигнальних кіл;
- якість електричних з'єднань в системі заземлення повинна забезпечувати мінімальний опір контакту, надійність і механічну міцність контакту в умовах кліматичних впливів і вібрації;
- контактні з'єднання повинні виключати можливість утворення оксидних плівок на контактуючих поверхнях і пов'язаних з цими плівками нелінійних явищ;
- контактні з'єднання повинні виключати можливість утворення гальванічних пар для запобігання корозії в колах заземлення;
- забороняється використовувати в якості заземлюючого пристрою нульові фази електромереж, металоконструкції будівель, що мають з'єднання із землею, металеві оболонки підземних кабелів, металеві труби систем опалення, водопостачання, каналізації.

Величина заземлення в основному визначається не опором заземлення, а опором заземлювальної магістралі. При цьому загальний опір заземлення буде тим менше, чим далі один від одного розташовані окремі заземлювачі.

У ролі заземлювачів найчастіше застосовуються сталеві труби довжиною 2 ... 3 м і діаметром 35 ... 50 мм і сталеві смуги перетином 50 ... 100 мм[19].

Заземлювачі слід з'єднувати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення за умовами механічної міцності і отримання достатньої провідності рекомендується брати не менше (24 • 4) мм2[19].

Магістралі заземлення поза будівлею необхідно прокладати на глибині близько 1,5 м, а всередині будівлі - по стіні або спеціальними каналами таким чином, щоб їх можна було оглядати зовні. З'єднують магістралі із заземлювачем тільки за допомогою зварювання[19].

2.4 Засоби безперебійного живлення

У наш час ПК або будь яка інша електронна апаратура інформаційно-обчислювальних систем має джерело живлення. Без живлення апаратура не зможе працювати. В такому випадку є доцільним використання джерел безперебійного живлення.

Джерела безперебійного живлення– це пристрій, що вмикається між джерелом живлення (розетки електромережі) і споживачем (комп’ютер), якому забезпечує живлення у разі зникнення напруги основного джерела, використовуючи для цього енергію своїх акумуляторних батарей. Незважаючи на кількість різних схематичних рішень в індустрії джерел безперебійного живлення склалися деякі типові схеми топології джерел безперебійного живлення[31].

Розрізняють 4 види джерел безперебійного живлення:

- Off-line;
- Line-Interactive;
- Дельта-технології;
- On-line

Джерело безперебійного живлення типу Off-line

Топологія Очікування (Stand by (Off-Line))

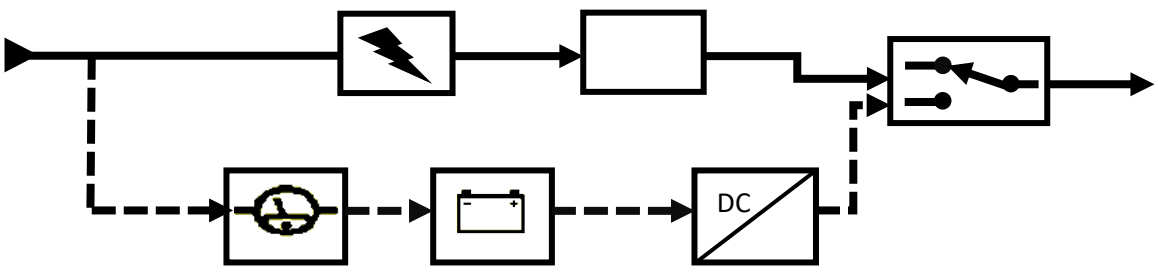

Рисунок 2.4.1

1. surge suppressor - обмежувач напруги
2. filter –фильтр
3. battery charger - зарядное устройство
4. battery - аккумулятор
5. inverter – инвертор
6. transfer switch - перемикач

Джерело безперебійного живлення , побудований за даною схемою, нерідко називають терміном «Off-Line». У кожний момент часу він може знаходитись в одному із двох режимів - Stand-by чи On-line. У разі, коли напруга у мережі знаходиться у допустимих межах (Standby mode – визначає час переходу у другу стадію енергозберігаючого режиму чи вимикає можливість переходу), transfer switch(перемикач) переключений на протікання струму навантаження по ланцюгу «обмежувач напруги – фильтр» ("Surge suppressor - Filter"). У цьому режимі джерело безперебійного живлення нічим не відрізняється від звичайного мережевого фільтру. Ніякої стабілізації напруги не відбувається. Під час роботи у цьому режимі також відбувається заряд акумуляторних батарей джерела безперебійного живлення [31]

У випадку виходу напруги мережі за допустимі межі перемикача (transfer switch) перемикається на живлення навантаження по ланцюгу «акумулятор – інвертор (Онлайн – режим) ("Battery - DC/AC inverter" (On-line mode)), тобто від енергії акумуляторної батареї преобразуючи інвентором в AC 220V.

Так як переключення батареї контактів та запуску інвертора не можуть відбуватись миттєво, живлення напруги буде перервано на деякий час(Transfer Time). Більшість Standby UPS забезпечують час передачі порядка 4-8 мс. Особливість даної системи у тому, що переключення в On-Line під час виходу напруги мережі за допустимі межі відбувається негайно, а повернення у Standby

mode – з обов’язковою затримкою у декілька секунд. Інакше, при багаторазових стрибків напруги в мережі, відбувалося б безперервне перемикання Standby/On-Line і назад, що привело б до значних спотворень струму навантаження і можливого виходу його з ладу або до збою в його роботі.

При цьому слід врахувати, що дана схема зазвичай не володіє можливістю стабілізації напруги при роботі в Standby mode і, отже, переходить в On-Line при кожному відхиленні напруги мережі. Розрядка акумуляторної батареї відбувається набагато швидше, ніж зворотний заряд. Потужність зарядного пристрою (battery charger'a) для даної схеми зазвичай вибирається порівняльно до малої, і витрати енергії від батареї у час затухання не компенсує.

Отже, для застосування у разі низької якості живлючої мережі дана топологія ДБЖ малопридатні по двум причинам[31]:

А.) При частих переходах в On-Line батареї досить швидко розряджається, не встигаючи відновить заряд за час Standby mode,у результаті чого ДБЖ втрачає здатність забезпечити аварійне живлення навантаження протягом необхідного часу;

Б.) Часте повторення циклів розряд / заряд скорочує термін служби акумуляторних батареї.

Проте, за даною схемою побудовано багато дешевих ДБЖ 2..5-річної давності розробки (APC Back-UPS, Para Systems MinuteMan A-series, PowerCom UPS-600, Sendon UPS-500, Leadman LU-550 и т.п.) з потужністю від 0.2 до 1.5-2 kVA.

Переваги:

- простота і, отже, дешевизна;
- високий ККД і, отже, низькі експлуатаційні витрати.

Недоліки:

- відсутність стабілізації напруги та частоти у штатному режимі;

- великий час переключення на живлення від батареї і, отже короткочасні зникнення або викиду напруги при навантаженні;
- втрата фази під час перемикання;
- Під час незначному падінні та стрибків напруги джерело безперебійного живлення переходить у режим роботи від вбудованих акумуляторів.
- Відсутність фільтрації напруги;
- Під час великого стрибка напруги можливо вихід з ладу і ДЖБ, і ПК.

Основне застосування: захист некритичного навантаження від вимкнення у районах стабільної напруги без серйозних перешкод. У цілому, дані ДЖБ можна характеризувати як компроміс між прийнятним рівнем захисту від неполадок у електромережі та ланцюгів.

Недоліки:

- ступенчатая стабілізація напруги;
- відсутність хорошої фільтрації напруги;
- час переходу на акумулятори і зворотний 2-6 мс, вірогідність "підвісання" обладнання в цей момент невелика;
- регулюючі напруги вузлів можуть породжувати стійкі викривлення вихідного сигналу та непередбачувані перехідні процесиДжерело безперебійного живлення типу Line-Interactive

Топологія Line-Interactive (Single Conversion)

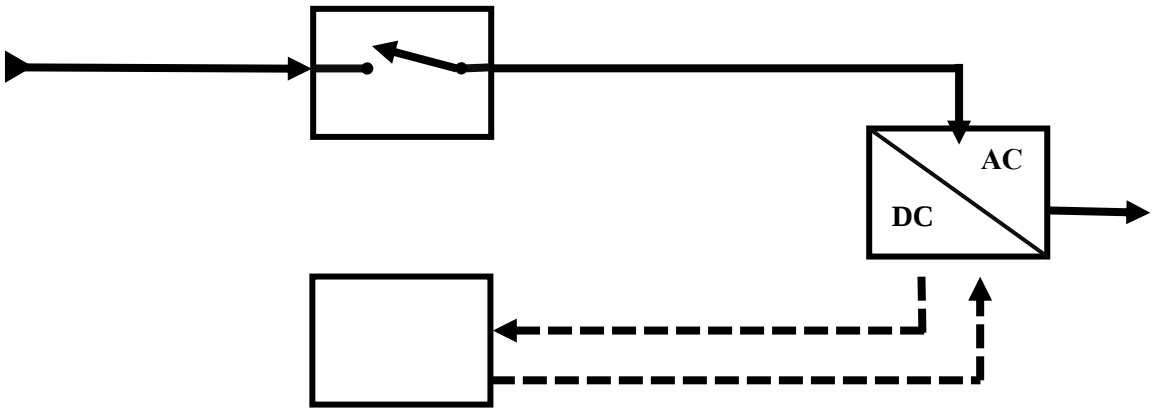

Рисунок 2.2

Transfer switch - перемикач

Battery - акумулятор

Inverter - Інвертор

← Charging (Normal) - заряджання

Discharging (Power Fail) → розрядка

У даній схемі інвертор завжди приєднаний до виходу джерела безперебійного живлення і являє собою складний вузол, на який покладається завдання стабілізації і фільтрації мережевої напруги, стеження за його рівнем, контролю заряду батареї при нормальній напрузі мережі (у моделях Smart-UPS) і переходу на батарейне живлення при аварійних рівнях мережевої напруги.

Завдяки значному діапазону стабілізації напруги, ця схема здатна працювати в нормальному режимі за умов, коли standby джерело вже перейшов на батарейне живлення. Це робить дану схему найбільш пригодною до роботи у електромережі невісокої якості[31]

По даній топології побудовані багато джерела безперебійного живлення середнього цінового класу (BEST Fortress, APC Smart-UPS и Back-UPS Pro, Neuhaus SmartLine и его прототип Fenton PowerPal, PowerCom KING). Типовий діапазон потужності від 0,4 до 3 кВА

Топологія Standby/On-Line Hybrid

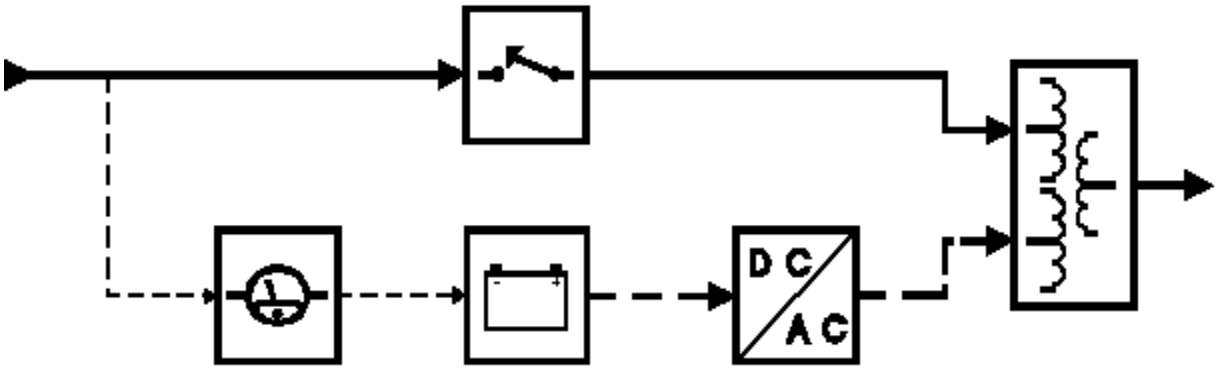

Рисунок 2.3 Відбір потужності від Standby DC/DC converter'a у даній топології відбувається тільки у випадку виявлення збою у живлюючій мережевій напрузі – у решту часу він може бути або вімкненим, або працювати «у холосту».

Battery charger має відносно малу напругу, подібно Standby UPS. У випадку нормальнох мережевої напруги, воно випрямляється і фільтрується, після чого надходить на інвертор, перетворюючий його зворотньо в AC 220V.

Переваги цієї схеми, як і "Double Conversion On-Line", є висока стабільність вихідної напруги та мінімальна тривалість перехідних процесів під час збоїв напруги у живлюючій мережі. Фірми – виробники нерідко декларують такі ДБЖ, як "On-Line", хоча це повністю відповідає істині.

По даній схемі побудовані такі джерела безперебійного живлення, як "Unipower" фірми Unison, “Personal Rowerware”фірми Exide та Powercom ONH-600. Типовий діапазон потужності для ДБЖ у даній топології від 0,5 до 5 кВА.

Топологія Standby-Ferro

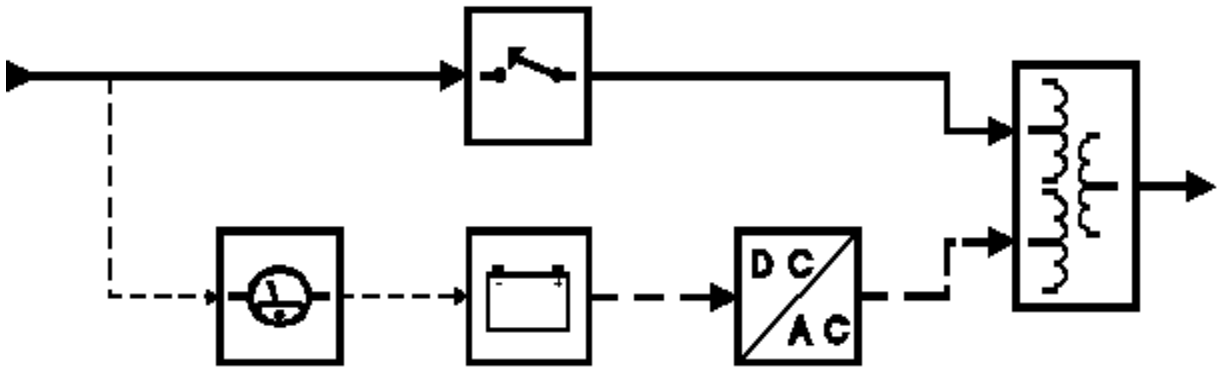

Рисунок 2.4 - Standby-Ferro

1. Rectifier - Випрямляч
2. Battery Charger - зарядний пристрій
3. Battery - Акумулятор
4. Standy DC-to-DC Converter - Стандартний перетворювач постійного струму в постійний струм
5. Combiner - комбайнер
6. Invertor - Інвертор

Ця схема базується на спеціальному трехобмоточном трансформатора При нормальному напрузі мережі через transfer switch потрапляє на трансформатор та через нього до напруги. У випадку відмова мережі живлення здійснюється інвертором через іншу обмотку, transfer switch у цей час розімкнуть.

Інветор запускається тільки тоді, коли виявлено відмова мережі та розімкнут tra.яnsfer switch. Трансформатор у даній схемі працює такж, як форерезонансний стабілізатор напруги та згладжування «сходинок», виникаючих пр роботі інвертора. Повна гальванічна розв'язка ланцюгів навантаження від електромережі забезпечує кращий захист ніж будь-який можливий фільтр.

Однак, феррорезонансний стабілізатор сам по собі вносить помітні спотворення та перехідні процеси, які в деяких випадках можуть виявитися небезпечнішими, ніж вихідні збої мережі живлення. Чи не єдина серія широко відомих ДБЖ, побудованих за такою схемою - "FERRUPS" фірми Best Power. Типові потужності від 0,5 до 15 кВА.

У момент перемикання джерела безперебійного живлення з мережевого на батарейне живлення, або навпаки, проходит певний час, перш ніж комутуючі засоби (релє) перекинуть контакті та інвертор війде у стабільний робочий режим. У цей час навантаження залишається без живлення(або напруга його живлення не відповідає нормам) на декілька мілісекунд.

Це називається Transfer Time. В принципі, для обладнання з імпульсними джерелами живлення (системні блоки комп'ютерів, монітори) короткочасні «провали» живлення не являють серьйозних проблем – конденсатори їх безперебійного живлення запасають досить енергії, щоб пережити цю дрібну неприємність без збоїв в роботі пристрою.

Але тим меньш, у момент комутації потенційна вірогідність збоїв набаго вище, ніж при нормальній роботі. Найгірші показники по цьому параметру Standby та Standby-Ferro UPS у найгіршому випадку їх Transfer Time може досягати 8-16мілісекунд[31].

Джерела безперебійного живлення здатні виконувати такі основні функції

1. Поглинання порівняльно малих і короткотимчасових викидів напруги;
2. Фільтрація напруги живлення, зниження рівня шумів;
3. Забезпечення резервного електроживлення навантаження протягом деякого часу після зникнення напруги в мережі;
4. Захист від перевантаження та короткого замикання.

Додатково до цього багато моделей ДБЖ під управлінням спеціалізірованного программного забезпечення можуть виконувати такі функції:

1. Автоматичний shutdown обслуговується обладнанням при тривалій відсутності напруги у мережі, а також перезапуск обладнання при відновленні мережевого живлення;
2. Моніторинг та запис в log-файл стану джерела живлення (температура, рівень заряду батареї);
3. Відображення рівнів напруги та потужності, споживчованого навантаження;
4. Відстеження аварійних ситуацій та видачу попереджуючих сигналів(звукові сигнали, запуск зовнішніх програм);
5. Включення та виключення напруги по внутрішньому таймеру в заданий час.

Безперебійник може забезпечити резервне живлення обладнання від своїх батарей. Все залежить від паспортної потужності, більшість ДБЖ забезпечують роботу обладнання протягом 5-15 хвилин після переходу на батарейне живлення.

Таблица 2.1Пристрої захисту за умови завад

Вид завад	Наслідки для ПК	Пристрій захисту	Ступінь захисту
Високовольтні викиди (High voltage Spikes)	Скидання ОС. Вихід з ладу апаратури	ДЖБ Off-line ДЖБ Line-interactive ДЖБ Delta Conversion ДЖБ On-line	Да Да Да Да
Відхід частоти Підсадка напруги (Browmout)	«Зависання» комп'ютерних систем. Вихід з ладу накопичувачів. Втрата даних	ДЖБ Off-line ДЖБ Line-interactive ДЖБ Delta Conversion ДЖБ On-line	Ні Частково Частково Да
	Втрата даних. Вихід з ладу апаратури	ДЖБ Off-line ДЖБ Line-interactive ДЖБ Delta Conversion ДЖБ On-line	Частково Частково Да Да

Продовження таблиці 2.1

Вид завад	Наслідки для ПК	Пристрій захисту	Ступінь захисту
Всплески напруги (Power Surges)	Скидання ОС. Виникнення помилок. Вихід з ладу апаратури. Мерехтіння освітлення.	ДЖБ Off-line ДЖБ Line-interactive ДЖБ On-line	Ні Частково Да
Зникнення напруги (Power Failure)	Втрата даних. Непередбачувані наслідки.	ДЖБ Off-line ДЖБ Line-interactive ДЖБ Delta Conversion ДЖБ On-line	Да Да Да Да

Висновки до розділу 2

У даному розділі було проведено аналіз джерел безперебійного живлення. Виділено недоліки та переваги даного пристрою. Розглянуто топологію джерел безперебійного живлення, схеми, а також механізм роботи пристроїв.

РОЗДІЛ 3

РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ТА ЗАХИСТУ ВІД ВПЛИВУ ЕЛЕКТРОМАГНІТНИХ ЗАВАД НА ОІД

3.1. Рекомендації з технічного захисту інформації в АС і ЗОТ від витоку каналами ПЕМВН

Рекомендації із захисту інформації від перехоплення випромінювань технічних засобів об'єкта ЕОТ

Навколо ОТЗ повинна забезпечуватися контрольована територія, за межами якої відношення "інформативний сигнал/шум" не перевищує норм. З цією метою ОТЗ рекомендується розташовувати у внутрішніх приміщеннях об'єкта, бажано, на нижніх поверхах.[7]

У випадку неможливості забезпечення цієї умови необхідно:

- замінити ОТЗ на захищені;

- провести часткове або повне екранування приміщень чи ОТЗ;

- установити системи просторового зашумлення;

- замінити незахищені ТЗ на захищені;

- застосувати завадозаглушувальні фільтри.

В екранованих приміщеннях (капсулах) рекомендується розміщувати високочастотні (ВЧ) ОТЗ. Як правило, до них відносяться процесори, запам'ятовувальні пристрої, дисплеї тощо.

Рекомендації із захисту інформації від перехоплення наводок на незахищені технічні засоби та ДТЗС, що мають вихід за межі КТ

У незахищених каналах зв'язку, лініях, проводах та кабелях ОТЗ і ДТЗС, що мають вихід за межі КТ, установлюються завадозаглушувальні фільтри.

Проводи і кабелі прокладаються в екранованих конструкціях.

Монтаж кіл ТЗ, що мають вихід за межі КТ, рекомендується проводити екранованим або прокладеним в екранувальних конструкціях симетричним кабелем.

Кабелі ОТЗ прокладаються окремим пакетом і не повинні утворювати петлі. Перехрещення кабелів ОТЗ і ДТЗС, що мають вихід за межі КТ, рекомендується проводити під прямим кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

Незадіяні проводи і кабелі демонтуються або закорочуються та заземляються[7].

3.1.1 Рекомендації із захисту інформації від витоку колами заземлення

Система заземлення ТЗ ЕОТ не повинна мати вихід за межі КТ і повинна розміщуватися на відстані не менше 10-15 м від них.

Заземлювальні проводи повинні бути виконані з мідного дроту (кабелю) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом.

Не рекомендується використовувати для системи заземлення ТЗ ЕОТ природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо), які мають вихід за межі КТ.

Для усунення небезпеки витоку інформації металевими трубопроводами, що виходять за межі КТ, рекомендується використовувати струмонепровідні вставки (муфти) довжиною не менше 1 м.

За наявності в ТЗ ЕОТ "схемної землі" окреме заземлення для них створювати не потрібно. Шина "схемна земля" повинна бути ізольованою від захисного заземлення та металоконструкцій і не повинна утворювати замкнену петлю.При неможливості провести заземлення ТЗ ЕОТ допускається їх "занулення"[5]

3.1.2. Рекомендації із захисту інформації від витоку колами електроживлення

Найбільш ефективно гальванічну та електромагнітну розв'язку кабелів електроживлення ТЗ ЕОТ від промислової мережі забезпечує їх розділова система типу "електродвигун-генератор". Електроживлення допускається також здійснювати через завадозаглушувальні фільтри.

Електроживлення повинно здійснюватись екранованим (броньованим) кабелем.

Кола електроживлення ТЗ ЕОТ на ділянці від ОТЗ до розділових систем чи завадозаглушувальних фільтрів рекомендується прокладати у жорстких екранувальних конструкціях.

Не допускається прокладання в одній екранувальній конструкції кабелів електроживлення, розв`язаних від промислової мережі, з будь-якими кабелями, що мають вихід за межі КТ.

Забороняється здійснювати електроживлення технічних засобів, що мають вихід за межі КТ, від захищених джерел електропостачання без установлення завадозаглушувальних фільтрів.

Для об'єктів 2 - 4 категорій допускається не проводити роботи із захисту кіл електроживлення, якщо всі пристрої і кабелі електропостачання об'єкта ЕОТ, включаючи трансформаторну підстанцію низької напруги із заземлювальним пристроєм, розміщені у межах КТ.

3.1.3. Рекомендації із застосування системи просторового зашумлення об'єктів ЕОТ

Пристрої просторового зашумлення застосовуються у випадках, коли пасивні заходи не забезпечують необхідної ефективності захисту об'єкта ЕОТ.

Установленню підлягають тільки сертифіковані Державною службою України з питань технічного захисту інформації (ДСТЗІ) засоби просторового зашумлення, до складу яких входять:

- надширокосмугові генератори електромагнітного поля шуму (генератор шуму);

- система рамкових антен;

- пульт сигналізації справності роботи системи.

Установлення генераторів шуму, монтаж антен, а також їх обслуговування в процесі експлуатації здійснюють підприємства, установи й організації, що мають відповідну ліцензію ДСТЗІ.

Живлення генераторів шуму повинно здійснюватися від того ж джерела, що і живлення ТЗ ЕОТ. Антени рекомендується розташовувати поза екранованим приміщенням[6]

3.1.4. Основні рекомендації з обладнання та застосування екранувальних конструкцій

Екранувальні кабельні конструкції разом з екранувальними конструкціями ТЗ ЕОТ повинні створювати екранувальний замкнений об'єм.

Виведення кабелів з екранувальних конструкцій і введення в них необхідно здійснювати через завадозаглушувальні фільтри.

Екранувальні кабельні конструкції можуть бути жорсткими і гнучкими. Основу жорстких конструкцій становлять труби, короби та коробки; основу гнучких конструкцій - металорукави, взяті в обплетення, і сітчасті рукави.

Для екранування проводів і кабелів застосовуються водогазопровідні труби. Рекомендується застосовувати сталеві тонкостінні оцинковані труби або сталеві електрозварені.

З'єднання нероз'ємних труб здійснюється зварюванням, роз'ємних - за допомогою муфти та контргайки.

Для екранування проводів і кабелів застосовуються короби прямокутного перерізу. Їх переваги у порівнянні з трубами - можливість прокладання кабелю з роздільними роз'ємами. Короби виготовляються з листової сталі. На кінцях секцій короба повинні бути фланці для з'єднання коробів між собою та з іншими екранувальними конструкціями. Для одержання надійного електричного контакту поверхня фланців повинна мати антикорозійне струмопровідне покриття.

Гнучкі конструкції служать для з'єднання жорстких екранувальних кабельних конструкцій з екранувальними конструкціями ТЗ ЕОТ та одночасно є компенсаторами температурних та монтажних деформацій.

Як екран може бути використаний металорукав типу РЗ за ТУ 223688- 77, поміщений у сталеве оцинковане обплетення. Для збільшення ефективності екранування рекомендується застосовувати комбіновані екрани, що складаються з мідного і сталевого обплетень.

3.3. Рекомендації та вимоги на основі технічного регламенту з електромагніної сумісності

3.3.1Загальні вимоги.

Обладнання повинне бути спроектоване та виготовлене з урахуванням сучасного стану розвитку техніки таким чином, щоб:

1) рівень створюваних обладнанням електромагнітних завад не перевищував рівень, за якого радіо-, телекомунікаційне або інше обладнання не може функціонувати за призначенням;

2) обладнання мало такий рівень завадостійкості до електромагнітних завад, очікуваних під час його використання за призначенням, який дає змогу цьому обладнанню функціонувати без неприпустимого погіршення якості його використання за призначенням.

3.3.2. Особливі вимоги до стаціонарних установок.

Монтаж та використання компонентів за призначенням.

Стаціонарна установка повинна бути змонтована із застосуванням належних інженерних практик та з урахуванням інформації про використання за призначенням її компонентів з метою забезпечення відповідності вимогам, визначеним у пункті 1 цих вимог[30]

Висновки за розділом 3

У розділі було проаналізовано нормативні документи технічного захисту інформації. Необхідно впровадити обов’язкове виконання даних інструкцці для забезпечення захисту від впливу електромагнітних завад на основні технічні засоби, які оброблюють інформацію з обмеженим доступом.

РОЗДІЛ 4

ВИЗНАЧЕННЯ ВИТРАТ НА ПРОЕКТУВАННЯ ТА ЕКСПЛУАТАЦІЮ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Техніко-економічне обґрунтування доцільності дипломної роботи

У дипломній роботі проаналізовано методи та засоби захисту від ненавмисного впливу інформації з обмеженим доступом. У спеціальній частині запропоновано варіанти захисту від ненавмисного електромагнітного впливу з використанням засобів електромагнітної сумісності:

- Прилад високочастотного шуму стаціонарний РІАС–1С;
- Генератор акустичного шуму стаціонарний РІАС–2ГС;
- Антена рамкова жорстка РІАС–1АЖ.

Вище приведений перелік засобів технічного захисту інформації, який включає в себе захист від ненавмисних електромагнітних випромінювань.

В якості об’єкта ОІД обрано офіс, у якому здійснюється обробка інформації з обмеженим доступом. У ньому розміщені ТЗПІ та допоміжні технічні засоби та системи (ДТЗС).

До складу ТЗПІ входить типовий набір технічних засобів, необхідних для приймання, обробки, зберігання та передачі інформації: ПЕОМ (системний блок, ЖК-монітор), копіювально-розмножувальна техніка;

До складу ДТЗС входить наступна побутова техніка: кондиціонер (2 шт.), плазма (2 шт.), електрочайник (1 об’єкт).

Мета економічного розділу: техніко-економічне обґрунтування доцільності впровадження на ОІД рекомендованих засобів захисту витоку інформації.

У даному розділі розглянемо 3 альтернативні засоби захисту інформації. Для оцінки рентабельності впровадження одного із варіантів, треба визначити капітальні та експлуатаційні витрати для кожного з варіантів та порівняти їх значення.

4.2 Визначення капітальних витрат

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу сукупної вартості володіння (ТСО). Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

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

До капітальних (фіксованих) витрат, що повинні бути враховані під час реалізації наданих у дипломній роботі рекомендацій, варто віднести наступні:

– витрати на первісні закупівлі засобів захисту інформації;

– витрати на залучення зовнішніх консультантів;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання та налагодження системи інформаційної безпеки).

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

$$К = К_е + К_{зк} + К_н ,$$

де $К_е$ – вартість закупівлі засобів захисту інформації, грн;

$К_{зк}$ – витрати на залучення зовнішніх консультантів, грн;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, грн.

Усі витрати, окрім витрат на закупівлю альтернативних засобів захисту інформації є однаковими для кожного із запропонованих варіантів реалізації рекомендацій. Вони розраховані та наведені нижче у таблиці 4.1.

Таблиця 4.1 – Послуги з технічного захисту інформації на об'єкті інформаційної діяльності (капітальні витрати)

№ з/п	Найменування послуг	Одиниця виміру	Вартість одиниці (грн.)	Кількість	Загальна вартість (грн.)
1	Перевірка відповідності рівня електромагнітного оточення виділеного приміщення нормам та виявлення ненавмисних електромагнітних випромінювань та наводок від однієї персональної електронно-обчислювальної машини (ПЕОМ), копіювально-розмножувальної техніки, електромеханічну друкарську машинки, телевізора, радіоприймача тощо	шт	700	12	8400
2	Спецдослідження об'єкта електронно-обчислювальної техніки (ЕОТ)	шт	3000	3	9000
	ВСЬОГО:				17400

Тобто, $К_{зк} + К_{н} = 17400$ грн.

4.2.1 Вартість технічних засобів захисту інформації від ненавмисного електромагнітного впливу.

– Прилад високочастотного шуму стаціонарний PIAC–1C вартість 8760,00 грн

Прилад високочастотного шуму стаціонарний PIAC–1C

Призначений для створення електромагнітних перешкод в ефірі в діапазоні частот від 180 Гц до 2

ГГц.

До складу приладу входять генератор високочастотного шуму стаціонарний РІАС–1ГС та антени рамкові м’ягкі РІАС–1АМ (4 шт.).

Коефіцієнт якості шуму - не менше 0,8. Коефіцієнт міжспектральних кореляційних зв’язків - не менше 2,0. Нормований рівень спектральної щільності напруженості електричного і магнітного компонентів нормованого електромагнітного поля шуму - не менше 30 дБ. Максимальне інтегральне значення вихідної потужності - не менше 10 Вт.

– Генератор акустичного шуму стаціонарний РІАС–2ГС вартість 8970,00 грн

Генератор акустичного шуму стаціонарний РІАС–2ГС

Призначений для захисту об’єктів від витоку конфіденційної інформації акустичними та віброакустичними каналами шляхом генерації шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц

Максимальна вихідна потужність акустичного та електромеханічного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга акустичного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом - не менше 5 В. Максимальна вихідна потужність п’єзоелектричного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга п’єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В. Прилад забезпечиує глибину регулювання окремо низько- та високочастотних складових шумового сигналу у робочому діапазоні частот не менше 20 дБ.

– Антена рамкова жорстка РІАС–1АЖ вартість 4608,00 грн

Антена рамкова жорстка РІАС–1АЖ

Призначена для створення та випромінення сигналу електромагнітних перешкод в ефірі в діапазоні частот від 180 Гц до 30 МГц.

Коефіцієнт якості шуму - не менше 0,8. Коефіцієнт міжспектральних кореляційних зв’язків - не менше 2,0. Нормований рівень спектральної щільності напруженості електричного і магнітного

компонентів нормованого електромагнітного поля шуму - не менше 30 дБ. Максимальне інтегральне значення вихідної потужності - не менше 3 Вт.

4.2.2 Капітальні витрати

Капітальні витрати на встановлення приладу високочастотного шуму стаціонарний РІАС–1С становить:

$К1 = К_{е\,1} + К_{зк} + К_{н.}$;

К1 = 8 760 грн +17 400 грн = 26 160 грн.

Капітальні витрати на встановлення генератора акустичного шуму стаціонарний РІАС–2ГС становить:

$К2 = К_{е\,2} + К_{зк} + К_{н.}$;

К2 = 8 970 грн + 17 400 грн = 26 370 грн.

Капітальні витрати на встановлення антени рамкова жорстка РІАС–1АЖ становить:

$К3 = К_{е\,3} + К_{зк} + К_{н.}$;

К3 = 4 608 грн + 17 400 грн = 22 008 грн.

4.3 Визначення експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.

Після впровадження кожного із запропонованих заходів захисту необхідно провести атестацію комплексу технічного захисту інформації ОІД та державну експертизу по введенню комплексної системи захисту інформації. Тому експлуатаційні витрати (таблиця 4.2) будуть однаковими для всіх засобів технічного захисту інформації.

Таблиця 4.2 – Послуги з технічного захисту інформації на об’єкті інформаційної діяльності (експлуатаційні витрати)

№ з/п	Найменування послуг	Одиниця виміру	Вартість одиниці (грн.)	Кількість	Загальна вартість на 1 рік (грн.)
1	Атестація комплексу технічного захисту інформації об’єкту інформаційної діяльності (проводиться 1 раз на рік)	шт	2000	1	2000
2	Проведення державної експертизи по введенню комплексної системи захисту інформації (проводиться 1 раз на 5 років**,** тому вартість її проведення складає 9000 : 5 = 1800 грн на рік)	шт	9000	1	1 800
	ВСЬОГО:				3800

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки при впровадженні будь-якого із розглянутих засобів технічного захисту інформації складають: С1 = С2 = С3 = 3800 грн.

4.4 Оцінка величини збитку

Для розрахунку вартості збитку можна застосувати наступну модель оцінки на прикладі підприємства «Х-1000».

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; 2 години.

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; 4 години.

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин; 10 годин.

Зо – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць; 8855 грн на місяць.

Зс – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць; 7500 грн на місяць.

Чо – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.; 2.

Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.; 6.

О – обсяг чистого прибутку атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі; 300 000 грн у рік.

I – число атакованих вузлів або сегментів корпоративної мережі; 1.

N – середнє число можливих атак на рік. 2

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п \ ,$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$$\frac{\sum 7500*6}{160} \ *4 = 1\ 125 \text{ грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн; 4600 грн.

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн; 6000 грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} \ ;$$

$$\frac{\sum 7500*6}{160} \ *10 = \ 2\ 812{,}50 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \ ;$$

$$П_{пв} = \frac{\sum 8855*2}{160} \ *4 = \ 442{,}75 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}),$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

$$V = \frac{300\,000}{2080} * (4 + 4 + 10) = 145 * 18 = 2610 \text{ грн}$$

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

$$B = \sum\sum U*\text{N}*\text{I}.$$

$$\text{B} = (1\,125 + 4600 + 6000 + 2610)*2*1 = 28670 \text{ грн}$$

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

$$\text{E} = \text{B}\cdot\text{R} – \text{C},$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

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

$$\text{E} = 28670*0.3–3800=4\,801 \text{ грн}.$$

Тепер розрахуємо термін окупності, який показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E}, \text{ років;}$$

$$T_{ОК1} = \frac{24320}{4801} = 5,06$$

$$T_{ОК2} = \frac{24530}{4801} = 5,1$$

$$T_{ОК3} = \frac{20168}{4801} = 4,2$$

4.5 Висновки

Проведено техніко-економічне обґрунтування дипломної роботи. Було розраховано капітальні та експлуатаційні витрати, а також визначили оцінку величини збитку та терміну окупності впровадженої системи інформаційної безпеки.

ДОДАТОК А. Перелік матеріалів дипломної роботи

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Розділ 4.doc

11 Висновки.doc

12 Список використаної літератури.doc

13 Додаток А.doc

14 Додаток Б.doc

15 Додаток В.doc

Презентація.pptx

ДОДАТОК Б. Відгуки керівників розділів

Б.1 Відгук керівника економічного розділу

Керівник розділу _____ Ю.О. Волотковська

(підпис) (ініціали, прізвище)

ДОДАТОК В. ВІДГУК

на дипломну роботу магістра на тему:

Захист інформації від впливу ненавмисних електромагнітних завад на основні технічні засоби, що обробляють інформацію з обмеженим доступом

студентки групи 125м-16-1

Білоусова Вікторія Русланівна

Пояснювальна записка складається зі вступу, чотирьох розділів і висновків, розташованих на ___ сторінках, та містить ___ рисунків, __ таблиць і __ джерел.

Метою дипломної роботи був аналіз впливу ненавмисних електромагнітних завад та електромагнітної сумісності на основні технічні засоби, що обробляють інформацію з обмеженим доступом.

У ході виконання роботи вирішені наступні завдання: проаналізовано електромагнітні завади та сумісності, виявлені джерела завад, проведено аналіз методів та засобів захисту від ненавмисних електромагнітних завад за допомогою джерел безперебійного живлення.

В економічному розділі виконаний розрахунок капітальних витрат на введення технічних засобів захисту інформації, проведений розрахунок собівартості технічних засобів захисту інформації.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор Білоусова Вікторія Русланівна заслуговує на оцінку «_____»___» та присвоєння кваліфікації «професіонал з організації інформаційної безпеки».

Керівник дипломної роботи, д.т.н., проф. В.І. Корнієнко

Керівник спец. част., ст. викл. С.І. Войцех

Р Е Ц Е Н З І Я

на дипломну роботу магістра на тему:

Захист від впливу ненавмисних електромагнітних завад на основні технічні засоби, що обробляють інформацію з обмеженим доступом

студентки групи 125м-16-1

Білоусова Вікторія Русланівна

Пояснювальна записка складається зі вступу, чотирьох розділів і висновків, розташованих на ___ сторінках, та містить ___ рисунків, __ таблиць і __ джерел.

Актуальність теми:

Питання впливу ненавмисних електромагнітних впливів стає більш актуальним в силу швидкої еволюції в сфері інформаційних технологій.

Використання сучасних методів і засобів захисту є ефективниму від витоку інформації з обмеженим доступом.

В даному випадку, захист інформації базується на джерелах безперебійного живлення, як одного з методів безперервності ведення бізнесу.

У роботі проаналізовані наступні методи захисту від впливу ненавмисних завад:

- екранування;
- фільтрація;
- заземлення;
- джерела безперебійного живлення.

Наукова новизна полягає, насамперед, у застосуванні сучасних методів забезпечення захисту інформації на підприємстві для підвищення рівня захищеності, а також мінімізувати вірогідність збою технічних засобів.

В цілому дипломна робота задовольняє усім вимогам, а її автор Білоусова Вікторія Русланівна заслуговує на оцінку «_____».

Рецензент