Державний університет

інформаційно – комунікаційних технологій

Факультет: Систем інформаційного і технічного захисту

Спеціальність : 125 Кібербезпека

Тема дипломної роботи:

Захист від впливу навмисних електромагнітних завад на технічні засоби обробки інформації з обмеженим доступом

Автор : студент IV курсу, групи СЗД-41

Буланий Валентин Павлович

Науковий керівник : Д.т.н., проф., Ахрамович Володимир Миколайович

Київ – 2023

Зміст

Список умовних скорочень

ЕМЗ – електромагнітні завади ;

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

TPM (trusted platform modules) – захищені мікросхеми ;

IDS/IPS (Intrusion Detection and Prevention Systems) – Системи виявлення та запобігання вторгнень ;

ТЗПІ - технічні засоби прийому, обробки, збереження та передачі інформації;

Вступ

В наш час актуальність проблеми кібербезпеки не викликає жодних сумнівів . Щодня кожен з нас стикається з необхідністю використання інформаційних технологій , а саме це може стосуватися технічних засобів.

Тому актуальності набуває саме вплив електромагнітних завад. Навмисні ЕМЗ можуть призвести до порушення цілісності інформації , яка обробляється технічними засобами прийому , обробки , збереження та передачі інформації , та її доступності . Це створює величезну небезпеку населенню і може обернутися великими збитками об’єктам інформаційної діяльності .

Так як розподіл і обробка стають все більш критичними і складними завданнями і водночас з ними зростає загроза з боку навмисних ЕМЗ , які можуть викликати порушення безпеки , виток конфіденційної інформації та навіть призвести до неправильної роботи технічних засобів обробки інформації.

Ця ситуація вимагає підвищеного рівня уваги до забезпечення вищого рівня безпеки та електромагнітної сумісності технічних засобів . Також ситуація ускладнюється тим , що обладнання дуже різноманітне за типом впливу , потужності та частотними діапазонами . Все це необхідно враховувати при захисті інформації що обробляються ТЗПІ , від впливу навмисних ЕМЗ .

Метою даної дипломної роботи є дослідження проблеми впливу навмисних ЕМЗ на технічні засоби обробки інформації з обмеженим доступом та розробка ефективних методів та засобів захисту . дослідження спрямовані на виявлення потенційних небезпек , аналізу впливу електромагнітних завад на роботу технічних засобів та розробку рекомендацій щодо застосування захисних заходів

У даній роботі будуть розглянуті основні види навмисних електромагнітних завад , їх можливості для технічних засобів обробки інформації та існуючі методи та засоби захисту . Буде проведено аналіз сучасного стану проблеми та огляд наукових досліджень і розробок в цій галузі.

На основі проведеного аналізу будуть запропоновані рекомендації та розроблені практичні рішення для забезпечення ефективного захисту технічних засобів обробки інформації від навмисних електромагнітних завад . Результати дослідження та розробки сприятимуть поліпшенню безпеки і захищеності інформаційних систем і сприяють забезпеченню стабільної та надійної роботи технічних засобів обробки інформації з обмеженим доступом .

В цілому ця дипломна робота має на меті розширити наше розуміння на проблеми захисту від навмисних електромагнітних завад на технічні засоби

обробки інформації з обмеженим доступом та надати на практиці рекомендації для забезпечення безпеки та захищеності .

Розділ 1

Вплив навмисних електромагнітних завад на технічні засоби обробки інформації

1.1 Основні терміни

Сам процес інформаційної діяльності , основними видами якого є використання , одержання , поширення та зберігання інформації (в тому числі Інформація з обмеженим доступом) . Інформація з обмеженим доступом може попасти під вплив загроз її безпеці у результаті чого може статися витік , порушення цілісності і доступності інформації .

Технічний захист інформації - це діяльність спрямована на забезпечення інженерно технічними заходами порядку доступу , цілісності та унеможливлює блоку інформації , яка може ставити під загрозу передбачену законом державну таємницю , конфіденційної інформації , також цілісності та доступності відкритої інформації , важливої для особи , суспільства , держави .

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

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;

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 .

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 .

Через вплив електромагнітної завади може статися спотворення інформації , що перетворювалася , передавалася або оброблялася .

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.

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

Рецептор – будь-який технічний пристрій, який реагує на електромагнітний вплив ЕМЗ .

1.2. Огляд загроз, які виникають внаслідок навмисних електромагнітних завад

Загрози , які виникають внаслідок навмисних електромагнітних завад, є важливим етапом дослідження з проблеми захисту технічних засобів обробки інформації. Дослідження цих загроз дозволяє зрозуміти характер і можливі наслідки електромагнітних завад на системи обробки інформації з обмеженим доступом.

Основні загрози, що виникають внаслідок навмисних електромагнітних завад, включають:

1. Електромагнітні пульси: Ця загроза виникає внаслідок короткочасного інтенсивного випромінювання електромагнітних хвиль. Електромагнітні пульси можуть спричинити неконтрольовані ефекти на електроніку технічних засобів обробки інформації, такі як пошкодження або зміна стану елементів, порушення роботи мікросхем та інші небажані наслідки.

2. Перешкоди в електромагнітному спектрі: Ця загроза виникає внаслідок навмисного випромінювання електромагнітних сигналів у певних діапазонах частот. Це може призвести до інтерференції з нормальною роботою технічних засобів обробки інформації, зниження якості сигналу, порушення передачі даних та інших проблем.

3. Радіочастотні впливи: Ця загроза виникає внаслідок навмисного випромінювання радіочастотних сигналів, які можуть перешкоджати нормальному функціонуванню технічних засобів обробки інформації. Радіочастотні впливи можуть спричинити зміни в передачі та отриманні сигналу, порушення комунікації та збій в роботі системи.

Виявлення та аналіз цих загроз дозволяє розробити ефективні стратегії захисту технічних засобів обробки інформації від навмисних електромагнітних завад.

1.3 Виявлення потенційних наслідків навмисних ЕМЗ

Завади на технічні засоби обробки інформації відіграє важливу роль у розумінні проблеми безпеки і захисту в цій сфері. Дослідження цих наслідків дозволяє розкрити можливі наслідки та ризики, які можуть виникнути внаслідок впливу навмисних електромагнітних завад на технічні засоби обробки інформації з обмеженим доступом.

Основні потенційні наслідки навмисних електромагнітних завад на технічні засоби обробки інформації включають:

Втрату даних: Навмисні електромагнітні завади можуть спричинити втрату або пошкодження інформації, збереженої на технічних засобах обробки. Це може мати серйозні наслідки для функціонування системи та втрату цінних даних.

Порушення працездатності: Навмисні електромагнітні завади можуть призвести до порушення нормального функціонування технічних засобів обробки інформації. Це може проявлятися у зниженні продуктивності, збоїв у роботі системи, перебоїв у доступі до інформації тощо.

Виток конфіденційної інформації: Навмисні електромагнітні завади можуть створювати ризик витоку конфіденційної інформації. Це може стати на шляху до несанкціонованого доступу до цінної інформації та потенційного розголошення конфіденційних даних.

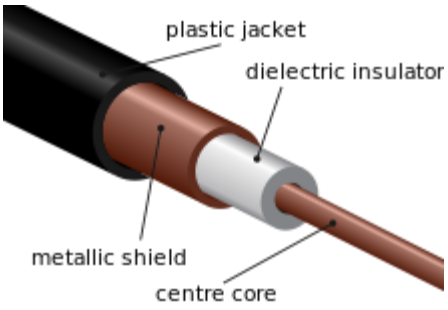
Можливість злому систем: Навмисні електромагнітні завади можуть послаблювати захисні механізми технічних засобів обробки інформації, створюючи можливості для несанкціонованого доступу та злому системи. Це може призвести до компрометації безпеки та порушення захищеної інформації.

Виявлення та аналіз потенційних наслідків навмисних електромагнітних завад на технічні засоби обробки інформації є важливим етапом дослідження, оскільки це надає підґрунтя для розробки ефективних захисних стратегій та рекомендацій для забезпечення безпеки і надійності таких систем.

1.4 Методи та засоби захисту від навмисних електромагнітних завад

Для ефективного захисту таких систем від електромагнітних завад, необхідно використовувати спеціальні методи та засоби.

Один із методів захисту - електромагнітне екранування. Цей метод полягає у використанні матеріалів з високою електропровідністю, які створюють бар'єр для електромагнітних хвиль та перешкоджають їх проникненню до технічних засобів обробки інформації. Електромагнітне екранування зменшує рівень електромагнітних завад, що потрапляють в систему, тим самим забезпечуючи покращену захищеність.



Поперечний переріз коаксіального кабелю що показує екранування та інші шари . Рис 1.1

Рис 1. 1

Фільтри є ще одним ефективним засобом захисту. Вони використовуються для фільтрації небажаних електромагнітних сигналів та шумів, які можуть впливати на роботу технічних засобів обробки інформації. Фільтри дозволяють виділити потрібний сигнал і виключити небажані компоненти, тим самим забезпечуючи більшу стійкість системи до електромагнітних завад.

Захист від електромагнітних пульсів також є важливим аспектом в контексті захисту від навмисних електромагнітних завад. Цей метод включає в себе застосування спеціальних пристроїв та систем, які здатні виявляти електромагнітні пульси та реагувати на них, забезпечуючи захист технічних засобів обробки інформації. Такий захист дозволяє запобігти негативним наслідкам від впливу електромагнітних пульсів, які можуть спричинити втрату даних, порушення працездатності та інші проблеми.

1.5 Аналіз ефективності та обмежень різних методів та засобів захисту та їх придатності для технічних засобів обробки інформації з обмеженим доступом.

Проведено детальні аналізи різних методів та засобів захисту , що використовуються для захисту технічних засобів обробки інформації від навмисних електромагнітних завад .

Оцінки ефективності методів та засобів захисту виконується з урахуванням здатності ефективно запобігати та усувати негативні наслідки впливу навмисних електромагнітних завад . Визначено , що електромагнітне екранування , фільтри та захист від електромагнітних імпульсів є одним з найпоширенішим та найефективнішим з методів захисту .

Аналізуючи обмеження різних методів та засобів захисту, було виявлено, що електромагнітне екранування може бути витратним та складним у реалізації для деяких систем з високим рівнем електромагнітного впливу. Фільтри мають певні фізичні обмеження щодо частотного діапазону та можуть не забезпечувати достатнього рівня фільтрації для деяких типів електромагнітних завад. Захист від електромагнітних пульсів також має свої особливості, зокрема, потребує високотехнологічного обладнання та спеціалізованих знань для ефективного застосування.

Придатність різних методів та засобів захисту для технічних засобів обробки інформації з обмеженим доступом залежить від конкретних вимог і характеристик системи, а також від забезпечення належного балансу між ефективністю захисту та вартістю реалізації. Враховуючи ці фактори, будуть запропоновані рекомендації щодо вибору та використання певних методів та засобів захисту залежно від конкретних вимог та обмежень системи.

Цей аналіз є важливим кроком у подальшому дослідженні та розробці ефективних заходів захисту від навмисних електромагнітних завад для технічних засобів обробки інформації з обмеженим доступом.

1.6 Наукові дослідження та розробки в галузі захисту від навмисних електромагнітних завад

Наукові дослідження пов'язані з захистом від навмисних електромагнітних завад представляють значний внесок у розвиток цієї галузі. Ось кілька актуальних досліджень, які я вирішив використати в своїй роботі

1. Наукове дослідження "Аналіз вразливості технічних засобів обробки інформації на основі моделювання електромагнітного впливу". У цьому дослідженні автори провели детальний аналіз вразливості різних типів технічних засобів обробки інформації на основі електромагнітного впливу. Вони використали математичні моделі та експериментальні дані для виявлення можливих наслідків навмисних електромагнітних завад та визначення ефективних методів захисту.(Рис 1.2)

Рис 1.2

2. Наукове дослідження "Розробка нових методів електромагнітного екранування для захисту технічних засобів обробки інформації". В цьому дослідженні дослідники пропонують нові підходи до електромагнітного екранування, які забезпечують більш ефективний захист від навмисних електромагнітних завад. Вони розробляють нові матеріали та конструкції екранів, які зменшують проникнення електромагнітних сигналів і забезпечують високу ефективність захисту.(Рис 1.3)

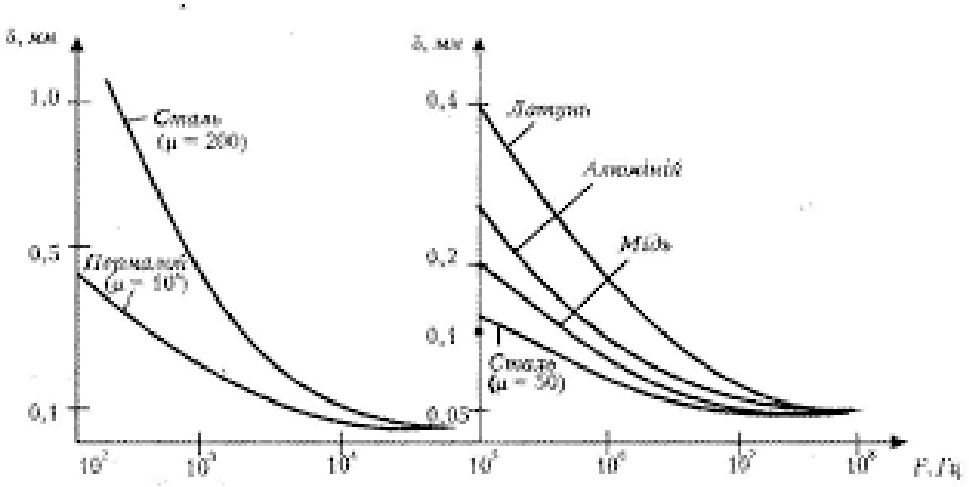


Рис 1. 3: Залежність ефективної глибини проникнення для різних матеріалів

Зазвичай на практиці коефіцієнт екранування виражається в децибелах

$$\text{В} = 20lg\left|\frac{E}{E^c}\right| = 20lg\left|\frac{H}{H^c}\right|$$

Відношення одиниць вимірювання :1Нп = 8,69 дБ (1 дБ= 0,115Нп).

Ефективність екранування – величина ,що обернена до коефіцієнта екранування , тому зі збільшенням частоти ефективність екранування зменшуються , що показано на рис .1.4 були досліджені частотні залежності коефіцієнтів екранування

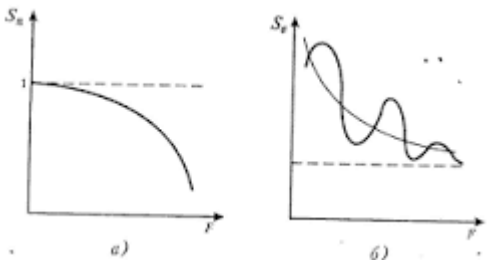


Рисунок 1.4 – Частотна залежність екранування поглинанням(а) та відбиттям(б)

3. Наукове дослідження "Використання шумоподібних сигналів для захисту технічних засобів обробки інформації від радіочастотних впливів". У цьому дослідженні вчені досліджують можливість застосування шумоподібних сигналів для захисту від радіочастотних впливів. Вони досліджують характеристики шумоподібних сигналів та розробляють методи їх використання для маскування і захисту інформації від навмисних електромагнітних завад.

1.7 Методи та засоби захисту та їх недоліки

Ці дослідження спрямовані на виявлення потенційних загроз, розробку нових методів та засобів захисту, а також на оцінку ефективності вже існуючих рішень:

1. Дослідження ефективності електромагнітного екранування: Це дослідження може включати аналіз різних матеріалів, конструкцій та технологій екранування для захисту технічних засобів обробки інформації від навмисних електромагнітних завад.

2. Розробка фільтрів та супресорів електромагнітних завад: Це дослідження може включати розробку нових методів фільтрації та пригнічення навмисних електромагнітних завад, що дозволяють зменшити їх вплив на технічні засоби обробки інформації.

3. Аналіз використання криптографічних методів: Це дослідження може досліджувати ефективність криптографічних методів захисту інформації від навмисних електромагнітних завад, таких як алгоритми шифрування та підписування.

4. Використання методів обмеження електромагнітних пульсів: Це дослідження може досліджувати методи та засоби для захисту технічних засобів обробки інформації від навмисних електромагнітних пульсів, таких як захист електромагнітною затвореною оболонкою та фільтрація вхідних сигналів.

5. Розробка методів виявлення та аналізу навмисних електромагнітних завад: Це дослідження може включати розробку алгоритмів та програмного забезпечення для виявлення та аналізу навмисних електромагнітних завад, що дозволяють реагувати на них та вживати відповідні захисні заходи.

Важливо зазначити, що деталі та обсяг розділу про наукові дослідження будуть залежати від конкретних досліджень тому постараюсь розповісти про кожен пункт і те які в них є недоліки

1.1 Електромагнітне екранування використовується для зменшення чи блокування проникнення електромагнітних сигналів до технічних засобів обробки інформації.

У дослідженні ефективності електромагнітного екранування можна вивчити різні аспекти, зокрема:

1.Матеріали для екранування: Дослідження може включати аналіз різних матеріалів, які використовуються для електромагнітного екранування, таких як метали, сплави, плівки та композитні матеріали. Дослідники можуть досліджувати їх електромагнітні властивості, проводити експерименти з різними матеріалами для визначення їх ефективності у блокуванні електромагнітних сигналів.

2.Конструкції екранування: Дослідники можуть розглядати різні конструкції електромагнітного екранування, включаючи корпуси, оболонки, контейнери та упаковки. Вони можуть досліджувати вплив різних конструкцій на ефективність екранування та розробляти оптимальні конструкції для захисту технічних засобів обробки інформації.

3.Методи вимірювання ефективності: Дослідження може включати розробку методів та приладів для вимірювання ефективності електромагнітного екранування. Це можуть бути спеціальні тестові стенди або експериментальні установки, які дозволяють виміряти рівень електромагнітних сигналів, які проникають через екранування.

4.Моделювання та симуляція: Дослідники можуть використовувати різні програмні засоби для моделювання та симуляції електромагнітного екранування. Вони можуть розробляти комп'ютерні моделі, які дозволяють аналізувати ефективність екранування при різних умовах, таких як частота електромагнітних сигналів, геометрія екранування та властивості матеріалів.

Потенційні обмеження та недоліки електромагнітного екранування в контексті захисту від навмисних електромагнітних завад можуть включати наступне:

1. Фізичні обмеження: Ефективність електромагнітного екранування може залежати від фізичних обмежень, таких як розмір, форма та геометрія екранувальної структури. У разі об'єктів великих розмірів або складної форми може бути важко забезпечити повну блокування електромагнітних сигналів.

2.Частотні обмеження: Ефективність електромагнітного екранування може залежати від частотного діапазону, в якому працюють навмисні електромагнітні завади. Деякі матеріали та конструкції екранування можуть бути більш ефективними в деяких частотних діапазонах, але менш ефективними в інших. Це може вимагати розробки комплексних заходів з екранування для забезпечення захисту від широкого спектра частот.

3.Електромагнітні проникнення: Деякі електромагнітні сигнали можуть проникати через екранування через прорізи, тріщини, дефекти або недосконалості в матеріалах або конструкції. Це може створювати можливість для проникнення електромагнітних завад до захищених систем.

4.Вартість та складність: Деякі методи електромагнітного екранування можуть бути витратними та складними у впровадженні. Використання спеціальних матеріалів, конструкцій та процесів може збільшити вартість проекту та ускладнити виготовлення та монтаж екранувальних структур.

5.Електромагнітна сумісність: Екранування може впливати на електромагнітну сумісність (ЕМС) системи, особливо при високих частотах. Воно може викликати перехресні завади між компонентами системи або впливати на передачу та отримання сигналів. Це може потребувати додаткових заходів для забезпечення належної ЕМС системи після встановлення екранування.

2.1 Розробка фільтрів та супресорів електромагнітних завад є одним з методів захисту від навмисних електромагнітних завад. Ці пристрої використовуються для фільтрації або приглушення небажаних електромагнітних сигналів, що допомагає забезпечити нормальну роботу технічних засобів обробки інформації з обмеженим доступом.

Основні переваги розробки фільтрів та супресорів електромагнітних завад включають:

1.Ефективність: Фільтри та супресори можуть бути спеціально налаштовані для приглушення конкретних частот або діапазонів частот, що дозволяє ефективно блокувати небажані електромагнітні сигнали. Це дозволяє знизити ризик впливу навмисних завад на технічні засоби обробки інформації.

2.Гнучкість: Фільтри та супресори можуть бути розроблені з урахуванням конкретних вимог і характеристик системи. Вони можуть бути вбудовані

безпосередньо в технічні засоби обробки інформації або використовуватися як зовнішні пристрої. Це забезпечує гнучкість в їхньому використанні та інтеграції.

3.Низька вартість: Фільтри та супресори можуть бути виготовлені з доступних матеріалів та компонентів, що дозволяє знизити їхню вартість. Це робить їх економічно вигідними для застосування в різних системах обробки інформації з обмеженим доступом.

Однак, розробка фільтрів та супресорів електромагнітних завад також має деякі недоліки, серед яких можна виділити:

1.Погіршення сигналу: Фільтрація небажаних електромагнітних сигналів може призводити до погіршення корисного сигналу. Якщо фільтр не налаштований належним чином або має недостатню пропускну здатність, це може призвести до втрати або спотворення корисної інформації.

2.Обмеження частотного діапазону: Деякі фільтри та супресори можуть мати обмеження щодо діапазону частот, на якому вони ефективно працюють. Це може вимагати використання декількох фільтрів або спеціалізованих пристроїв для захисту від широкого спектру електромагнітних завад.

3.Фізичні обмеження: Розмір, вага та конструкція фільтрів та супресорів можуть бути обмеженими фізичними параметрами системи. Наприклад, великі розміри або важкі ваги фільтрів можуть ускладнити їхнє встановлення та інтеграцію в технічні засоби обробки інформації.

3.1. Аналіз використання криптографічних методів у контексті захисту від навмисних електромагнітних завад. Ці криптографічні методи використовуються для захисту конфіденційності, цілісності та аутентичності інформації, а також для забезпечення безпеки передачі даних.

Основні переваги використання криптографічних методів включають:

1.Конфіденційність: Криптографічні алгоритми дозволяють шифрувати дані, забезпечуючи їхню конфіденційність. Це означає, що навмисні особи, які намагаються отримати доступ до захищених даних, не зможуть їх розшифрувати без належного ключа.

2.Цілісність: Криптографічні методи дозволяють перевірити цілісність даних, що означає виявлення будь-яких змін або спотворень в переданих або збережених даних. Це важливо для виявлення можливих навмисних змін, які можуть бути спричинені електромагнітними завадами.

3.Аутентичність: Криптографічні методи дозволяють перевірити автентичність джерела даних або ідентифікувати особу, яка підписала певні дані. Це допомагає запобігти підробці або введенню недостовірних даних.

Незважаючи на переваги, криптографічні методи також мають деякі недоліки, які варто врахувати:

1.Використання ресурсів: Криптографічні алгоритми можуть бути обчислювально витратними, особливо при обробці великих обсягів даних або при використанні складних алгоритмів. Це може призводити до збільшення часу обробки та споживання енергії.

2.Ключовий управління: Криптографічні методи вимагають належного управління ключами для шифрування та розшифрування даних. Без належного управління ключами може виникнути ризик компрометації конфіденційної інформації.

3.Вразливість до квантових обчислень: З появою квантових комп'ютерів, деякі традиційні криптографічні алгоритми можуть стати вразливими до атак, що базуються на квантових обчисленнях. Це ставить під сумнів безпеку захищеної інформації у майбутньому.

4.1. Використання методів обмеження електромагнітних пульсів (EMP) є одним із способів захисту від впливу навмисних електромагнітних завад на технічні засоби обробки інформації. EMP виникають внаслідок інтенсивних вибухових подій або штучного створення потужних електромагнітних полів. Використання методів обмеження EMP може допомогти запобігти пошкодженню або втраті працездатності електронних пристроїв.

Основні методи обмеження електромагнітних пульсів включають:

1.Екранування: Екранування полягає в застосуванні спеціальних матеріалів або конструкцій, які здатні відбивати або поглинати електромагнітні хвилі. Це допомагає зменшити рівень електромагнітних завад, які досягають внутрішніх електронних компонентів.

2.Фільтрація: Фільтрація включає використання спеціальних фільтрів для пригнічення електромагнітних сигналів у певних діапазонах частот. Це дозволяє зменшити імпульсні шуми та завади, які можуть пошкодити електронні компоненти.

3.Заземлення: Заземлення є важливим елементом захисту від EMP. Використання належного заземлення може відвести надлишковий електромагнітний потік в землю, запобігаючи його накопиченню в системі.

4.Захист електронних компонентів: Деякі електронні компоненти можуть бути особливо вразливими до EMP. Використання спеціальних захисних пристроїв, таких як діоди, перемички або викидні резистори, може допомогти вберегти ці компоненти від пошкоджень.

Незважаючи на переваги, цей метод також має свої недоліки:

1.Висока вартість: Реалізація ефективних методів обмеження EMP може бути витратною, особливо для великих систем або комплексних пристроїв.

2.Обмежена ефективність: Деякі EMP можуть мати дуже високу енергію та широкий діапазон частот, що може ускладнити їх ефективне обмеження за допомогою традиційних методів.

3.Вплив на функціональність: Застосування методів обмеження EMP може вплинути на функціональність електронних пристроїв, особливо у випадку високочастотних додатків. Це може вимагати компромісу між захистом від EMP і забезпеченням потрібного рівня функціональності.

5.1 Розробка методів виявлення та аналізу навмисних електромагнітних завад є важливим аспектом в галузі захисту від впливу навмисних електромагнітних завад на технічні засоби обробки інформації з обмеженим доступом. Ці методи спрямовані на раннє виявлення потенційних навмисних електромагнітних завад і аналіз їх впливу на системи обробки інформації.

Основні напрямки розробки методів виявлення та аналізу навмисних електромагнітних завад включають:

1.Електромагнітне спостереження: Цей підхід полягає в розміщенні спеціальних сенсорів і приймачів, які здатні реєструвати і аналізувати електромагнітні сигнали. Вони дозволяють виявити аномальні зміни в електромагнітному спектрі, що можуть свідчити про наявність навмисних електромагнітних завад.

2.Аналіз змін параметрів: Цей підхід використовує аналіз змін параметрів роботи системи, таких як електричний струм, напруга, частота і температура. Навмисні електромагнітні завади можуть спричиняти зміни цих параметрів, і виявлення таких змін може свідчити про наявність завад.

3.Використання алгоритмів машинного навчання: Методи машинного навчання можуть бути використані для розробки моделей, які навчаються виявляти та класифікувати навмисні електромагнітні завади на основі накопичених даних. Це дозволяє автоматизувати процес виявлення та аналізу завад.

Незважаючи на переваги, цей метод виявлення та аналізу також має свої недоліки:

1.Складність аналізу: Навмисні електромагнітні завади можуть бути досить складними для виявлення і аналізу. Вони можуть бути дуже слабкими або маскуватися іншими сигналами, що робить їх виявлення складним завданням.

2.Великий обсяг даних: Збір та аналіз великого обсягу даних, необхідних для виявлення навмисних електромагнітних завад, може вимагати значних обчислювальних ресурсів та складних алгоритмів обробки даних.

3.Ложні спрацювання: Методи виявлення можуть мати високу ймовірність ложних спрацювань, коли нормальні сигнали помилково інтерпретуються як навмисні електромагнітні завади. Це може призводити до помилкових або незаслужених тривог.

1.8. Вивчення технічних засобів обробки інформації з обмеженим доступом та їх вразливостей

У цьому підрозділі я детально розберу і опишу декілька технічних засобів обробки інформації з обмеженим доступом які використовуються в сучасних системах да опис їх апаратної та програмної складових , функціональних можливостей і їх вразливостей :

1.1 Фізичні бар'єри та контроль доступу є важливими технічними засобами для захисту технічних засобів обробки інформації з обмеженим доступом. Вони мають на меті фізично обмежити доступ до пристроїв і забезпечити лише авторизованим особам доступ до системи. Основні елементи фізичних бар'єрів та контролю доступу включають:

1.Периметральна охорона: Це включає в себе встановлення фізичних перешкод, таких як огорожі, стіни або паркан, навколо об'єкту, що має бути захищеним. Такі периметральні бар'єри допомагають запобігти несанкціонованому доступу до пристроїв обробки інформації.

2.Контроль доступу: Це означає встановлення системи, яка обмежує фізичний доступ до приміщень або областей, де розташовані технічні засоби обробки інформації. Такі системи можуть включати в себе картки доступу, біометричні сканери (відбитки пальців, розпізнавання обличчя тощо) або кодові замки.

3.Відеоспостереження: Це включає в себе використання камер спостереження для контролю доступу та нагляду за зонами, де знаходяться технічні засоби обробки інформації. Відеоспостереження може записувати активність, що дозволяє виявити та розслідувати потенційні випадки несанкціонованого доступу чи порушення безпеки.

Оцінка вразливостей фізичних бар'єрів та контролю доступу полягає у визначенні можливих слабких місць, де можливий несанкціонований доступ. Основні вразливості включають:

1.Втрату або крадіжку карток доступу або інших засобів ідентифікації: Якщо картки доступу або інші засоби ідентифікації потрапляють в руки неавторизованих осіб, це може вести до несанкціонованого доступу.

2.Використання силових методів: Фізичні бар'єри можуть бути уразливі до силових методів, таких як фізична руйнівна сила або використання знарядь, що дозволяють обходити або знищувати бар'єри.

3.Соціальна інженерія: Атаки з використанням соціальної інженерії можуть впливати на людей, щоб отримати несанкціонований доступ до захищених зон. Наприклад, шахраї можуть вмовити співробітника розкрити пароль або надати доступ до приміщення.

4.Технічні уразливості: Деякі системи контролю доступу можуть мати технічні уразливості, які можуть бути використані для обходу або підробки ідентифікаційних засобів.

Оцінка вразливостей фізичних бар'єрів та контролю доступу вимагає систематичного аналізу, ідентифікації потенційних ризиків та прийняття заходів для зменшення цих ризиків. Застосування комплексного підходу, який поєднує фізичні бар'єри з електронним контролем доступу та використанням відеоспостереження, може забезпечити більш надійний рівень захисту і зменшити вразливості системи.

1.2 Шифрування даних є одним з ключових методів захисту інформації в сучасних системах обробки даних з обмеженим доступом. Воно використовується для перетворення звичайного тексту (незашифрованого) у шифрований текст за допомогою алгоритму шифрування. Шифрування забезпечує конфіденційність інформації шляхом ускладнення доступу до неї без відповідного ключа. Основні типи шифрування включають:

1.Симетричне шифрування: Цей тип шифрування використовує один і той самий ключ для як шифрування, так і розшифрування даних. Він є швидким і ефективним, але вимагає безпечного обміну ключем між відправником і одержувачем.

2.Асиметричне шифрування: Цей тип шифрування використовує пару ключів - публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний ключ - для розшифрування. Він забезпечує більшу безпеку, оскільки приватний ключ залишається виключно володарю, але вимагає більшої обчислювальної потужності.

3.Хеш-функції: Хеш-функції використовуються для перетворення вихідного повідомлення в унікальний хеш-код фіксованої довжини. Хеш-функції не можуть бути розшифровані, їх використовують для перевірки цілісності даних і створення цифрових підписів.

Оцінка вразливостей шифрування полягає у визначенні можливих шляхів атак на криптографічні алгоритми. Деякі можливі вразливості шифрування включають:

1.Криптоаналіз: Це процес визначення ключа або розшифрування шифрованого повідомлення шляхом аналізу шифрованого тексту. Криптоаналітики можуть використовувати різні методи, такі як атака з використанням словника, атака методом перебору і аналіз статистики, для зламу шифру.

2.Квантові обчислення: Розробка квантових комп'ютерів може привести до появи нових алгоритмів, які здатні швидко розкрити деякі типи шифрування, які використовуються сьогодні.

3.Ключовий обмін: Безпека шифрування може бути порушена, якщо ключі викрадені або скомпрометовані. Зловмисники можуть намагатися здобути доступ до ключів шляхом фізичних атак, атак з використанням соціальної інженерії або злому системи керування ключами.

Для зменшення вразливостей шифрування важливо використовувати сильні криптографічні алгоритми, регулярно оновлювати ключі, використовувати безпечні протоколи передачі даних і забезпечувати безпеку зберігання ключів. Також важливо враховувати останні розвитки в області криптографії та регулярно оновлювати системи шифрування, щоб уникнути нових вразливостей.

1.3 Фахові апаратні рішення в контексті захисту від впливу навмисних електромагнітних завад на технічні засоби обробки інформації з обмеженим доступом використовуються для забезпечення фізичної безпеки та обмеження доступу до цих засобів. Вони включають у себе різноманітні апаратні пристрої, модулі та механізми, що використовуються для захисту електронних систем від зовнішніх електромагнітних впливів та несанкціонованого доступу.

Основні фахові апаратні рішення включають:

1.Електромагнітні екрани та корпуси: Ці апаратні рішення використовуються для створення бар'єру проти проникнення електромагнітних сигналів до внутрішніх компонентів системи. Вони забезпечують електромагнітне екранування, що допомагає запобігти несанкціонованому доступу до інформації шляхом блокування електромагнітного випромінювання та навмисних електромагнітних завад.

2.Фізичні замки та ключі: Ці апаратні рішення використовуються для контролю доступу до системи. Вони можуть включати механічні замки, смарт-карти, біометричні сканери (відбитків пальців, сканери сітки очей тощо) та інші

методи аутентифікації, які дозволяють обмежити фізичний доступ лише авторизованим користувачам.

3.Захищені мікросхеми (trusted platform modules - TPM): Це апаратні пристрої, що використовуються для зберігання криптографічних ключів та виконання криптографічних операцій. TPM забезпечує апаратну безпеку і використовується для захисту від атак на ключі та виконання криптографічних операцій.

4.Мікроконтролери безпеки: Ці апаратні рішення вбудовані в технічні засоби обробки інформації і забезпечують безпеку на рівні пристрою. Вони виконують функції, такі як шифрування, аутентифікація, контроль цілісності та інші заходи безпеки.

Оцінка вразливостей фахових апаратних рішень варіюється в залежності від конкретної імплементації та налаштувань використовуваного обладнання. Основні вразливості можуть включати:

1.Фізичний доступ: Якщо зловмисники отримують фізичний доступ до апаратних рішень, вони можуть намагатися провести атаку на обладнання, зламати його або скопіювати конфіденційну інформацію. Тому важливо забезпечити адекватну фізичну безпеку і контроль доступу до обладнання.

2.Застарілі алгоритми або слабкі налаштування: Якщо використовуються застарілі алгоритми шифрування або недостатньо складні налаштування, це може створити вразливість для атак зловмисників, які використовують криптоаналітичні методи для злому захисту.

3.Недостатнє управління ключами: Якщо керування ключами здійснюється неправильно, може бути порушена безпека шифрування. Крадіжка або втрата ключів може дозволити зловмиснику отримати доступ до зашифрованих даних.

4.Соціальна інженерія: Зловмисники можуть намагатися використовувати соціальну інженерію, щоб отримати несанкціонований доступ до обладнання або отримати конфіденційну інформацію від авторизованих користувачів.

Для забезпечення високого рівня безпеки необхідно враховувати ці вразливості та вживати відповідні заходи захисту, такі як застосування сильних алгоритмів шифрування, належне управління ключами, фізична безпека і контроль доступу, а також навчання персоналу про соціальну інженерію та потенційні загрози.

1.4 IDS/IPS є важливим компонентом захисту технічних засобів обробки інформації з обмеженим доступом. Їх основна мета полягає в виявленні та

реагуванні на потенційні вторгнення або аномалії в мережевому трафіку та системних журналах.

Системи виявлення та запобігання вторгнень можуть бути розподілені на два основні типи: системи виявлення вторгнень (Intrusion Detection Systems, IDS) і системи запобігання вторгнень (Intrusion Prevention Systems, IPS).

1.Системи виявлення вторгнень (IDS): Ці системи аналізують мережевий трафік та системні журнали для виявлення незвичайних активностей або аномалій, які можуть вказувати на вторгнення. IDS виявляють атаки на основі підписів (відомих векторів атак) та на основі аномалій (відхилення від нормального патерну).

2.Системи запобігання вторгнень (IPS): Ці системи, на відміну від IDS, не тільки виявляють вторгнення, але й активно реагують на них, блокуючи атаки або виконуючи інші заходи для запобігання пошкодженням системи. IPS може автоматично генерувати правила для мережевих пристроїв, щоб блокувати шкідливий трафік або виконувати інші дії для запобігання вторгненням.

Оцінка вразливостей систем виявлення та запобігання вторгнень залежить від різних факторів, таких як конфігурація системи, рівень оновлення відомих підписів атак, ефективність алгоритмів виявлення аномалій, розміщення датчиків та інші. Деякі можливі вразливості систем IDS/IPS включають:

1.Вразливість підписів: IDS, що використовують підписи атак, можуть бути обмануті, якщо атака використовує новий або змінений вектор атаки, який не входить у відому базу підписів.

2.Перевантаження мережі: Інтенсивний мережевий трафік може перевантажити систему IDS/IPS, знижуючи її ефективність та здатність виявлення вторгнень.

3.Сфальсифіковані пакети: Деякі атаки можуть використовувати сфальсифіковані пакети або методи, щоб обманути систему IDS/IPS, змінивши її реакцію або приховуючи свою активність.

4.Вразливості системи IDS/IPS: Самі системи IDS/IPS можуть мати вразливості, які можуть бути використані для обходу або компрометації системи.

5.Велика кількість фальшивих позитивів: Системи IDS/IPS можуть породжувати велику кількість фальшивих позитивів, тобто помилково визначати звичайний трафік як атаку. Це може призвести до перевантаження персоналу безпеки та зниження ефективності системи . Для зменшення вразливостей систем IDS/IPS рекомендується постійно оновлювати підписи атак, використовувати аналіз аномалій, уважно конфігурувати систему та регулярно проводити аудит

безпеки. Крім того, важливо мати резервні системи IDS/IPS для забезпечення безперебійного функціонування в разі компрометації однієї системи.

Розділ 2

Методи та засоби забезпечення електромагнітного захисту від впливу навмисних електромагнітних завад

2.1 Заземлення

2.1.1. 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:

1. стрижні з металу, що мають високу електропровідність, занурені у землю і з'єднані з наземними металоконструкціями технічних засобів;
2. 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 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:

1. система заземлення повинна включати загальний заземлювач, заземлюючий кабель, шини і дроти, що сполучають заземлювач з об'єктом;
2. опори заземлюючих провідників, а також шин заземлення повинні бути мінімальними;

3. кожен елемент, що заземлюється, повинен бути приєднаний до заземлювача або до заземлюючої магістралі за допомогою окремого відведення. Послідовне включення в заземлюючий провідник декількох елементів забороняється;

4. 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;

5. слід уникати використання загальних провідників у системах екрануючих заземлень, захисних заземлень і сигнальних кіл;

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

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

8. контактні з'єднання повинні виключати можливість утворення гальванічних пар для запобігання корозії в колах заземлення;

9. 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. 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. 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.

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:

1. захист апаратури від зовнішніх імпульсних перешкод;

2. 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:

1. величина робочої напруги і струму фільтра повинні відповідати напрузі й струму фільтрованого кола;

2. величина ослаблення небажаних сигналів в діапазоні робочих частот повинна бути менше необхідної;

3.ослаблення корисного сигналу в смузі прозорості фільтру повинно бути незначним;

4. габарити і маса повинні бути мінімальними;

5. фільтри повинні забезпечувати функціонування при певних умовах експлуатації (температура, вологість, тиск) і механічних тисках (удари, вібрації і т.д.);

6. конструкції фільтрів повинні відповідати вимогам техніки безпеки.

До фільтрів кіл живлення висувають наступні додаткові вимоги:

1. 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));

2. мережеві фільтри повинні ефективно працювати при великих значеннях струмів, високих напругах і високих рівнях потужності затримуваних електромагнітних коливань.

Конструктивно фільтри поділяються на:

1.фільтри на елементах з зосередженими параметрами (LC-фільтри) - для

роботи на частотах до 300МГц;

2. фільтри з розподіленими параметрами (смугові, коаксіальні або хвилеводні) для роботи на частотах понад 1 ГГц;

3. 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 .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 електромагнітних завад.

2.3 Екранування

Одним із істотних недоліків більшості технічних засобів обробки інформації, які використовуються на об’єкт інформаційної діяльності , 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:

1. екранування всього технічного засобу обробки інформації;

2. екранування окремих елементів технічних засобів;

3. екранування робочих місць;

4. індивідуальне екранування;

5. використання екрануючих поглинаючих засобів.

Розрізняють електростатичне, магнітостатичне та електромагнітне екранування.

Електростатичне і магнітостатичне 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) .

Основна задача електростатичного екранування – зменшення ємнісни зв’язків між елементами, що потребують захисту що забезпечуються шляхом накопиченням статичної електрики на екрані з послідуючим відводом зарядів на землю. Необхідною умовою при реалізації електростатичного екранування є надійне заземлення екрану. При застосуванні металевих екранів досягається повне усунення впливу електростатичного поля. 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.

Ефективність електростатичного екранування також залежить від величин 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. 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:

1. конструкція екрану повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрану, не виходячи за його межі;

2. 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;

3. 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;

4. магнітна проникність матеріалу екрану повинна бути якомога вищою. Для виготовлення екранів бажано використовувати магніто м’які матеріали з високою магнітною проникністю (наприклад, пермалой);

5. збільшення товщини стінок екрана призводить до підвищення ефективності екранування, однак при цьому слід можливі конструктивні обмеження через масу і габаритами екрану;

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

7. 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 . 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:

1. шунтування магнітних силових ліній поля в екран із феромагнітних матеріалів (з $\mu >> 1$), обумовленого суттєво меншим магнітним опором матеріалу екрана, ніж навколишнього повітря;

2. 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. 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.

2.3.1 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. 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. 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). 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.

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.).

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

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.

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. 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).

2.4 Захист електронних компонентів від ЕМП

Захист електронних компонентів від електромагнітних пульсів (ЕМП) є важливою складовою заходів забезпечення безпеки технічних засобів обробки інформації. ЕМП є потужними електромагнітними випромінюваннями, які можуть спричинити непередбачувані руйнівні наслідки для електронних пристроїв.

Основна мета захисту електронних компонентів від ЕМП полягає у запобіганні їх пошкодженню або втраті функціональності під час впливу електромагнітних пульсів. Для досягнення цієї мети використовуються різні способи і технології. Один з основних способів захисту від ЕМП - це екранування. Екранування включає використання спеціальних матеріалів або покриттів, які здатні відбивати або поглинати електромагнітні хвилі, що надходять від ЕМП. Електронні компоненти можуть бути поміщені у екрановані контейнери або упаковки для забезпечення їх захищеності.

Інший спосіб - використання фільтрів. Фільтри є електричними пристроями, які здатні приглушувати або відфільтровувати небажані електромагнітні сигнали. Вони можуть бути встановлені на вхідних або вихідних лініях електронних компонентів для зниження рівня електромагнітних перешкод. Також, для захисту від ЕМП використовуються спеціальні захисні пристрої, такі як газорозрядні клапани, діоди з дієлектричною стійкістю, феритові обмотки тощо. Ці пристрої мають властивості захищати електронні компоненти від надлишкового електромагнітного впливу.

Незважаючи на ефективність цих способів захисту, вони також мають деякі недоліки і вразливості. Наприклад, екранування може бути недостатньо ефективним при дуже високих рівнях ЕМП. Фільтри можуть мати обмежену ширину смуги пропускання і не здатні відфільтрувати всі типи електромагнітних сигналів. Захисні пристрої можуть бути дорогими або вимагати додаткового обладнання для їх встановлення. Оцінка вразливостей цих способів захисту повинна враховувати специфічні потреби і характеристики системи. Вирішення вразливостей може включати пошук більш ефективних рішень, розробку комбінованих захисних методів або застосування додаткових заходів забезпечення безпеки, таких як резервне копіювання даних та контроль доступу.

2.4.1 . Засоби безперебійного живлення

Безперебійники (UPS) можуть бути використані як один із способів захисту від ЕМП. У наш час ПК або будь яка інша електронна апаратура інформаційнообчислювальних 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.

Джерело безперебійного живлення 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 – фільтр» ("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 .

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/OnLine і назад, що привело б до значних спотворень струму навантаження і можливого виходу його з ладу або до збою в його роботі.

По 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.

У разі ЕМП, безперебійники можуть виконувати декілька функцій захисту:

1.Згладжування напругових перешкод: ЕМП можуть спричиняти коливання напруги в електричних системах, що може пошкодити електронні компоненти. Безперебійники використовують свої внутрішні регулятори напруги, щоб згладити і стабілізувати вихідну напругу, що надходить до пристроїв.

2.Ізоляція від основної мережі: Безперебійники можуть забезпечувати електричну ізоляцію між електронними компонентами та основною електричною мережею. Це допомагає уникнути проникнення ЕМП через мережеві з'єднання.

3.Фільтрація електромагнітних шумів: Деякі безперебійники можуть мати вбудовані фільтри для приглушення шумів і перешкод, включаючи електромагнітні сигнали. Це може допомогти знизити ризик впливу ЕМП на електронні компоненти.

Однак, варто зазначити, що безперебійники не є спеціалізованими пристроями для захисту від ЕМП і не забезпечують повний захист від усіх типів

ЕМП. Вони можуть бути корисними у разі локальних впливів ЕМП, але не здатні забезпечити захист від масштабних ЕМП подій, таких як ядерний вибух. Для повного захисту від ЕМП рекомендується використовувати комбінацію різних захисних методів і пристроїв, включаючи електромагнітне екранування, фільтри, захист від електромагнітних пульсів та інші спеціалізовані рішення.

Розділ 3

Розробка рекомендацій щодо забезпечення електромагнітного захисту від впливу електромагнітних завад об’єктів інформаційної діяльності

3.1 Огляд потенційних загроз

Потенційні загрози, пов'язані з електромагнітними завадами, можуть бути різноманітними. Ось кілька типових загроз, які варто враховувати:

1.Електромагнітні пульси (ЕМП): Це короткочасні, інтенсивні електромагнітні події, які можуть спричинити серйозні пошкодження електронним компонентам. Найпоширеніші джерела ЕМП - ядерні вибухи, мігреньовані ЕМП-генератори тощо.

2.Електромагнітні перешкоди: Це включає шуми, інтерференцію та перешкоди в електромагнітному спектрі, які можуть завадити нормальному функціонуванню технічних засобів обробки інформації. Ці загрози можуть бути призводити до спотворення сигналів, помилкових даних чи втрати зв'язку.

3.Радіочастотні впливи: Включають нелегальне перехоплення радіочастотних сигналів або зловживання радіочастотними комунікаційними системами. Це може призвести до несанкціонованого доступу до інформації, перехоплення конфіденційних даних або зміни комунікаційних потоків.

4.Електромагнітне шпигунство: Це включає використання електромагнітних методів для нелегального збору інформації. Шпигуни можуть використовувати пристрої для перехоплення електромагнітних сигналів, включаючи електромагнітні випромінювачі та пристрої зчитування електромагнітних випромінювань зі скануючими антенами.

Я би хотів більше роз’яснити за ці загрози

3.1.1 Електромагнітний імпульс (EMI)

Електромагнітний імпульс (EMI) - це короткочасна високоінтенсивна електромагнітна подія, яка може мати широкий спектр частот і високу енергію. Імпульс може виникати внаслідок різних факторів, таких як ядерний вибух, мігреньовані EMI-генератори, блискавка або техногенні джерела.

EMI може мати негативний вплив на електронні компоненти, системи зв'язку, електронні пристрої та інфраструктуру. Імпульс може викликати різноманітні проблеми, включаючи:

1.Пошкодження електронних компонентів: EMI може призвести до виникнення високих напруг і струмів в електронних компонентах, що перевищують їх допустимі значення. Це може призвести до перегоряння, знищення або необоротного пошкодження компонентів.

2.Втрата або порушення даних: EMI може спричинити помилки в передачі даних або втрату інформації, особливо якщо вона зберігається на магнітних носіях або електронних пристроях. Імпульс може впливати на чутливі елементи пам'яті, які зберігають дані, і призвести до їх втрати або пошкодження.

3.Переривання роботи систем: EMI може впливати на нормальну роботу систем зв'язку, електронних пристроїв та інфраструктури. Імпульс може призводити до збоїв, переривання постачання електроенергії, зупинки пристроїв або системного збою.

4.Порушення безпеки: EMI може створювати потенційні загрози для безпеки, особливо в критичних системах. Імпульс може спричинити помилкові сигнали, перехоплення комунікацій, зміну параметрів систем або зловживання радіочастотними пристроями.

Щодо вразливостей EMI, вони можуть включати недостатню захищеність електронних компонентів, використання недостатньо екранированих кабелів та пристроїв, недостатнє захищення інфраструктури від потенційних EMI-джерел, а також недостатній рівень захисту від радіочастотних перешкод та шпигунства. Ці вразливості можуть призвести до небезпеки для систем та інфраструктури, і потребують відповідних заходів захисту та екранування для забезпечення електромагнітної стійкості і безпеки.

3.1.2 Електромагнітні перешкоди (ЕМП)

Електромагнітні перешкоди (ЕМП) - це навмисні електромагнітні сигнали, які використовуються для спотворення, перехоплення або перешкоджання нормальному функціонуванню електронних пристроїв, систем зв'язку або інфраструктури. Їх використання може бути спрямоване на шпигунство, дезінформацію, перешкоджання комунікації або навмисне пошкодження технічних засобів.

ЕМП можуть бути вироблені різними способами, включаючи генерацію імпульсних електромагнітних полів, використання радіочастотних сигналів, розповсюдження шуму або спектральних перехресних сигналів. Вони можуть бути передані з використанням антен, кабелів, пристроїв передачі сигналів або спеціально побудованих пристроїв.

ЕМП можуть мати наступні наслідки:

1.Перешкоджання комунікації: ЕМП можуть спричинити порушення передачі сигналів і комунікаційних зв'язків. Вони можуть спотворювати сигнали, викликати інтерференцію та призводити до втрати чи переривання зв'язку.

2.Зміна чутливості електронних пристроїв: ЕМП можуть впливати на чутливість електронних пристроїв, змінюючи їх робочі параметри або спричиняючи помилкову роботу. Це може призвести до некоректної обробки даних, втрати інформації або пошкодження пристроїв.

3.Збій систем: ЕМП можуть спричинити збої в роботі систем, зокрема в електронних пристроях, автоматичних системах керування, мережах зв'язку та електропостачанні. Це може призвести до відмови систем, недоступності послуг або неправильної роботи.

4.Шпигунство і перехоплення інформації: ЕМП можуть використовуватись для незаконного отримання конфіденційної інформації шляхом перехоплення радіосигналів або зламу захисту систем зв'язку. Це може створювати загрозу для безпеки даних та конфіденційності.

Вразливість до ЕМП залежить від рівня захисту, який забезпечується в електронних пристроях та системах. Вразливість може виникати внаслідок недостатньої екранування, недоліків в конструкції, використання недостатньо захищених компонентів або слабкого захисту від перешкод. Оцінка вразливостей і розробка заходів захисту від ЕМП є важливими завданнями для забезпечення електромагнітної стійкості систем та забезпечення безпеки інформації.

3.1.3 Радіочастотні впливи

Радіочастотні впливи відносяться до навмисних електромагнітних завад, які використовуються для спотворення або перешкоджання роботі радіочастотних систем. Ці впливи можуть включати передачу неправдивих сигналів, генерацію шуму, зміну частоти або спектра сигналу, а також перехоплення і перерозподіл сигналів.

Радіочастотні впливи можуть бути використані для різних цілей, включаючи шпигунство, перешкоджання комунікації, перехоплення інформації, навмисне впливання на пристрої та системи, а також генерацію сигналів з метою заміни або спотворення правильних сигналів.

Основні методи радіочастотних впливів включають:

1. Інтерференція: Це процес генерації навмисних радіочастотних сигналів, які спотворюють або перекривають правильні сигнали. Інтерференція може бути викликана намаганням перешкодити зв'язку або спотворити передачу даних.

2. Спектральне перехресне засмічування: Цей метод включає генерацію радіочастотних сигналів, які знаходяться в тому ж спектральному діапазоні, що й цільові сигнали. Це може призводити до перекриття та втрати сигналів, зниження якості комунікації і збільшення помилок передачі даних.

3. Перехоплення сигналів: Цей метод включає перехоплення радіочастотних сигналів, які передаються між пристроями або системами. Перехоплені сигнали можуть бути використані для розуміння або викрадення конфіденційної інформації.

4. Генерація шуму: Шум може бути намаганням завадити комунікації шляхом заповнення радіочастотного спектра навмисними сигналами низької сигнальної сили. Це може знизити якість сигналу, призвести до помилок передачі даних і знизити надійність зв'язку.

Щодо вразливостей радіочастотних систем, вони зазвичай пов'язані з недостатньою захищеністю від радіочастотних впливів. Вразливості можуть включати недостатню екранування, слабку автентифікацію та шифрування, недостатню відмовостійкість, а також використання незахищених протоколів із зв'язку. Відповідні заходи захисту, такі як використання сильних алгоритмів шифрування, захист від перехоплення та інтерференції, екранування пристроїв і застосування безпеки на рівні фізичних і логічних шарів, можуть допомогти зменшити вразливість до радіочастотних впливів.

3.1.4 Електромагнітне шпигунство

Електромагнітне шпигунство, також відоме як TEMPEST (Transient Electromagnetic Pulse Emanation Standard), є методом отримання конфіденційної інформації шляхом використання електромагнітних випромінювань, що випромінюються електронними пристроями. Цей метод шпигунства заснований на спостереженні, захопленні і аналізі випромінювань, які виникають від пристроїв під час їх роботи.

Електромагнітне шпигунство використовується для отримання різних видів інформації, включаючи звук, відео, текстові повідомлення та дані, що передаються через пристрої. За допомогою спеціального обладнання і технік, шпигуни можуть перехоплювати та аналізувати електромагнітні сигнали, що випромінюються пристроями, такими як комп'ютери, мобільні телефони, роутери, пристрої з Wi-Fi і т.д.

Одна з основних причин успішності електромагнітного шпигунства полягає в тому, що електромагнітні випромінювання від пристроїв можуть віддавати чутливу інформацію про їхню роботу, таку як секретні ключі шифрування, процесорні операції, акустичні сигнали тощо. Шпигуни можуть

використовувати цю інформацію для розшифрування захищених даних або для отримання доступу до конфіденційної інформації.

Щоб запобігти електромагнітному шпигунству, можна використовувати різні техніки і заходи захисту. Деякі з них включають екранування пристроїв, захист від електромагнітних перешкод, захист від радіочастотних випромінювань, використання захищених алгоритмів шифрування та криптографічних протоколів, а також фізичний контроль доступу до пристроїв.

Проте, електромагнітне шпигунство залишається потенційною загрозою, оскільки шпигуни можуть вдосконалювати свої методи та обладнання для перехоплення і аналізу електромагнітних сигналів. Крім того, нові технології, такі як бездротові мережі, Internet of Things (IoT) і розширена реальність (AR), створюють нові можливості для електромагнітного шпигунства. Тому, постійне вдосконалення технологій захисту та свідоме врахування потенційних загроз є важливими аспектами боротьби з цим типом шпигунства.

3.2 Аналіз існуючих методів захисту

В аналізі існуючих методів захисту від впливу навмисних електромагнітних завад повинні бути враховані наступні методи:

1.Електромагнітне екранування: Використання спеціальних матеріалів та конструкцій для створення фізичного бар'єру, який захищає електронні компоненти від зовнішніх електромагнітних сигналів.

2.Фільтри та супресори електромагнітних завад: Використання спеціальних фільтрів та супресорів для зменшення або приглушення електромагнітних завад на різних частотах.

3.Криптографічні методи: Використання шифрування та криптографічних алгоритмів для захисту конфіденційності та цілісності даних під час їх передачі та зберігання.

4.Методи обмеження електромагнітних пульсів: Використання спеціальних методів та пристроїв для обмеження впливу електромагнітних пульсів, таких як феритові обмотки, блокувальні дроселі, захисні екрани тощо.

Кожен з цих методів має свої переваги і обмеження. Проаналізував ефективність та обмеження кожного методу дозволить визначити їх придатність для захисту технічних засобів обробки інформації з обмеженим доступом.

3.2.1Електромагнітне екранування

Використання електромагнітного екранування має свої переваги і обмеження, і його ефективність може варіюватися залежно від конкретних умов та вимог безпеки. Давайте розглянемо переваги, обмеження і придатність електромагнітного екранування для захисту технічних засобів обробки інформації з обмеженим доступом:

Переваги електромагнітного екранування:

1.Захист від зовнішніх електромагнітних завад: Електромагнітне екранування може ефективно блокувати або значно зменшити вплив зовнішніх електромагнітних сигналів на електронні компоненти. Це дозволяє запобігати небажаним ефектам, таким як перешкоди, спотворення сигналу, переривання роботи системи та можливе пошкодження. (Рис 1.4)

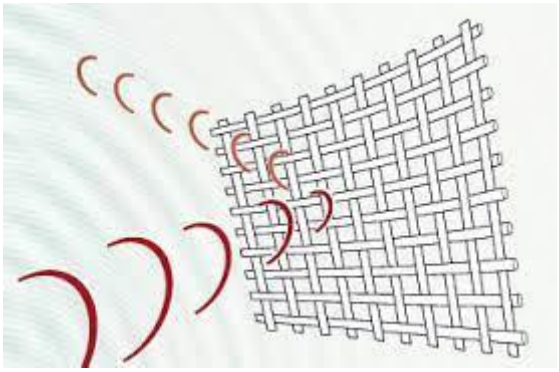


Рис.1.4

2.Фізичний бар'єр: Електромагнітне екранування використовує спеціальні матеріали, що мають високу провідність або магнітну проникність, для створення фізичного бар'єру навколо компонентів. Цей бар'єр блокує проникнення електромагнітних сигналів, що дозволяє забезпечити високий рівень захисту. (Рис1.5)

Рис.1.5

3.Гнучкість у використанні: Електромагнітне екранування може бути використано на різних рівнях - від індивідуальних компонентів до всієї системи. Це дозволяє забезпечити захист від електромагнітних завад на різних рівнях архітектури системи. (Рис.1.6)

Рис 1.6

Обмеження електромагнітного екранування:

1.Вартість: Електромагнітне екранування може бути витратним процесом, особливо якщо потрібно екранувати велику кількість компонентів або складних систем. Вартість матеріалів, виробництва та установки екранування може бути високою, що може ставити обмеження на його використання.

2.Вага та об'єм: Додавання екранування може збільшити вагу та об'єм системи. Це може бути проблемою, особливо для портативних пристроїв або деяких спеціалізованих додатків, де вага та розміри є важливими факторами.

3.Ефективність на різних частотах: Ефективність електромагнітного екранування може варіюватися в залежності від частоти електромагнітних сигналів. Відповідність екранування на різних діапазонах частот може бути різною, і це слід враховувати при виборі методу захисту.

Придатність електромагнітного екранування для захисту технічних засобів обробки інформації з обмеженим доступом залежить від конкретного контексту, потреб безпеки та вимог системи. У деяких випадках, де важливо забезпечити максимальний рівень захисту від електромагнітних завад, електромагнітне екранування може бути вигідним і ефективним рішенням. Однак, у випадках, де вартість, вага та об'єм є важливими факторами або де ефективність на певних частотах є проблемою, інші методи захисту можуть бути більш придатними. Оцінка потреб безпеки, обмежень та вимог системи допоможе визначити, наскільки вигідно і ефективно використовувати електромагнітне екранування у конкретному випадку.

3.2.2 Фільтри та супресори від електромагнітних завад

Аналізуючи використання фільтрів та супресорів електромагнітних завад для захисту технічних засобів обробки інформації з обмеженим доступом, можна виокремити наступні переваги та обмеження:

Переваги:

1.Ефективність у підборі діапазону: Фільтри та супресори можуть бути спроектовані для ефективного підбору та фільтрації конкретного діапазону електромагнітних сигналів. Це дозволяє ефективно усувати небажані електромагнітні завади, забезпечуючи захист технічних засобів обробки інформації.

2.Підвищення якості сигналу: Використання фільтрів та супресорів дозволяє покращити якість сигналу, усуваючи небажані шуми та завади. Це може сприяти кращій роботі технічних засобів обробки інформації та забезпечити надійність передачі даних.(рис 1.7)

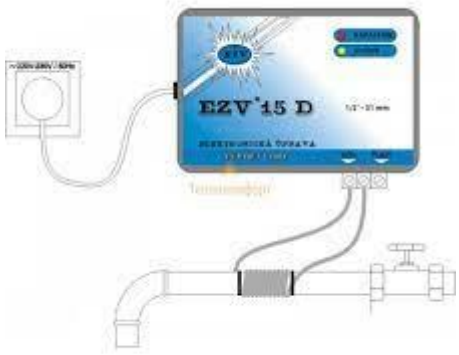


Рис1.7

3.Гнучкість у використанні: Фільтри та супресори можуть бути встановлені на різних етапах системи обробки інформації, від вхідних до вихідних інтерфейсів. Це дозволяє гнучко впливати на захист системи та адаптуватися до конкретних потреб та вимог.

Обмеження:

1.Вплив на швидкість передачі даних: Використання фільтрів та супресорів може вплинути на швидкість передачі даних. При виборі та налаштуванні фільтрів необхідно враховувати цей фактор, щоб забезпечити оптимальну балансу між захистом від електромагнітних завад та продуктивністю системи.

2.Обмеження частотного діапазону: Кожен фільтр або супресор має певний частотний діапазон, в якому він працює ефективно. Якщо електромагнітні завади

виникають за межами цього діапазону, їх може бути складніше усунути за допомогою цих засобів.

3.Витрати та складність впровадження: Використання фільтрів та супресорів вимагає додаткових витрат на придбання та встановлення цих засобів. Також може знадобитися експертний аналіз та налаштування для досягнення оптимальних результатів. Це може збільшити загальні витрати та складність процесу впровадження.

Оцінка:

Використання фільтрів та супресорів електромагнітних завад є ефективним способом захисту технічних засобів обробки інформації з обмеженим доступом. Вони можуть забезпечити ефективне приглушення небажаних сигналів та електромагнітних завад, що сприяє збереженню цілісності та конфіденційності інформації. Однак, необхідно враховувати обмеження, такі як вплив на швидкість передачі даних, обмеження частотного діапазону та додаткові витрати та складність впровадження. Рекомендується провести детальний аналіз вимог системи та добре збалансувати ефективність захисту та продуктивність системи при використанні фільтрів та супресорів електромагнітних завад.

3.2.3 Криптографічні методи

Аналізуючи використання криптографічних методів для захисту технічних засобів обробки інформації з обмеженим доступом, можна виділити наступні переваги та обмеження:

Переваги:

1.Конфіденційність даних: Криптографічні методи дозволяють зашифрувати дані та забезпечити їх конфіденційність. Це забезпечує захист від несанкціонованого доступу до інформації, що передається або зберігається на технічних засобах обробки інформації.

2.Цілісність даних: Криптографічні методи дозволяють перевірити цілісність даних, що означає виявлення будь-яких змін або модифікацій в переданих або збережених даних. Це допомагає виявити можливі вторгнення або зловживання.

3.Аутентифікація та авторизація: Криптографічні методи можуть забезпечити аутентифікацію користувачів та перевірку їх прав доступу до системи. Це дозволяє контролювати доступ до технічних засобів обробки інформації та забезпечувати лише санкціонованим користувачам використовувати систему.

Обмеження:

1.Обчислювальна складність: Деякі криптографічні алгоритми можуть бути обчислювально складними, особливо при роботі з великими обсягами даних. Це може вплинути на продуктивність системи та час обробки.

2.Ключовий обмін: Використання криптографічних методів вимагає безпечного обміну ключами між відправником і отримувачем. Неналежне керування ключами або можливість перехоплення ключів можуть вразити систему на ризик компрометації.

3.Соціальні інженерні атаки: Криптографічні методи можуть бути вразливі до соціальних інженерних атак, де зловмисники використовують маніпуляції та обман, щоб отримати доступ до ключів або навіть перехопити розшифровані дані в момент їх використання.

Оцінка:

Використання криптографічних методів є вигідним та ефективним способом захисту технічних засобів обробки інформації з обмеженим доступом. Вони забезпечують конфіденційність, цілісність та аутентифікацію даних, що є критичними аспектами безпеки інформації. Однак, необхідно враховувати обмеження, такі як обчислювальна складність, ключовий обмін та ризик соціальних інженерних атак. Для досягнення максимальної ефективності та безпеки рекомендується використовувати сильні криптографічні алгоритми, правильно керувати ключами та постійно оновлювати систему з огляду на нові загрози та атаки.

3.2.4 Методи обмеження електромагнітних пульсів

Аналізуючи використання методів обмеження електромагнітних пульсів для захисту технічних засобів обробки інформації з обмеженим доступом, можна виділити наступні переваги та обмеження:

Переваги:

Захист від ЕМП: Методи обмеження електромагнітних пульсів спрямовані на запобігання негативним впливам ЕМП на технічні засоби обробки інформації. Це дозволяє зберегти їх функціональність та недопущення втрати або пошкодження даних.

Ефективність: Відповідні методи обмеження електромагнітних пульсів можуть бути ефективними у зменшенні впливу ЕМП шляхом використання екранування, захисних оболонок, фільтрів та інших заходів. Вони можуть знизити рівень електромагнітних перешкод та захистити технічні засоби обробки інформації від небажаних впливів.

Гнучкість: Методи обмеження електромагнітних пульсів можуть бути застосовані до різних типів технічних засобів обробки інформації, незалежно від їх конкретного призначення або архітектури. Це дозволяє їх використання в різних сферах, включаючи військову, комерційну та громадську сфери.

Обмеження:

Вартість: Реалізація методів обмеження електромагнітних пульсів може бути витратною, особливо при застосуванні до складних систем або великих масштабів. Вона може включати в себе витрати на придбання та встановлення спеціалізованого обладнання, проведення тестувань та оцінку відповідності.

Технічні обмеження: Деякі методи обмеження електромагнітних пульсів можуть мати обмеження з точки зору технічної реалізації або можливості їх застосування до певних типів технічних засобів обробки інформації. Наприклад, можуть бути обмеження з точки зору розміру, ваги або споживання енергії, що може ускладнити їх застосування у певних сценаріях.

Вразливості: Деякі методи обмеження електромагнітних пульсів можуть бути вразливі до розробки нових технологій або розширення спектра ЕМП. Зловмисники можуть шукати способи обходу або подолання захисних заходів, що може призвести до несанкціонованого доступу до технічних засобів обробки інформації.

Оцінка:

Використання методів обмеження електромагнітних пульсів може бути вигідним і ефективним для захисту технічних засобів обробки інформації з обмеженим доступом. Вони забезпечують можливість зменшення впливу ЕМП на пристрої та системи, що дозволяє зберегти їх функціональність та інтерактивність даних. Однак, необхідно враховувати витрати на впровадження та обмеження, що можуть виникати при застосуванні конкретних методів. Також варто враховувати потенційні вразливості та можливість розвитку нових технологій або атак, які можуть вплинути на ефективність застосованих заходів захисту.

4.Розділ
Результати та обговорення отриманої інформації

4.1 Ефективність застосованих методів

4.1.1. Електромагнітне екранування

Воно базується на використанні спеціальних матеріалів і конструкцій, які здатні блокувати або відбивати електромагнітні сигнали, що можуть завдати шкоди технічним засобам обробки інформації з обмеженим доступом. Ефективність електромагнітного екранування полягає у здатності матеріалів екранування відбивати або поглинати електромагнітні сигнали, що потенційно можуть створити навмисні завади.

Отже, електромагнітне екранування може бути ефективним методом захисту від навмисних електромагнітних завад, проте його ефективність залежить від використовуваних матеріалів, конструкцій та інших факторів. Його використання вимагає ретельного проектування, налагодження та впровадження для досягнення оптимальних результатів.

4.1.2 Фільтри та супресори електромагнітних завад

Вони працюють на принципі фільтрації і приглушення небажаних електромагнітних сигналів, що дозволяє зменшити їх вплив на технічні засоби обробки інформації з обмеженим доступом.

Основна ефективність фільтрів та супресорів електромагнітних завад полягає в їх здатності блокувати або приглушувати небажані електромагнітні сигнали на певних частотах. Вони можуть бути використані для фільтрації шумів, інтерференції та інших навмисних сигналів, що можуть завадити нормальному функціонуванню технічних засобів обробки інформації. Вони можуть бути налаштовані або програмовані для фільтрації конкретних частот або широкого діапазону частот. Це дає можливість ефективно захистити технічні засоби обробки інформації від різноманітних електромагнітних завад .Окрім ефективності, важливо враховувати обмеження та вразливості фільтрів та супресорів електромагнітних завад. Деякі з них вимагають правильної настройки та налагодження для досягнення оптимальної ефективності. Крім того, вони можуть мати обмежену пропускну здатність, що може впливати на швидкість передачі даних або роботу системи. Деякі сигнали можуть бути складнішими для фільтрації, особливо якщо вони мають подібні характеристики до корисних сигналів . Також, варто враховувати, що фільтри та супресори електромагнітних

завад не є універсальними методами захисту. Вони можуть бути ефективні проти певних типів завад, але не забезпечувати повного захисту від всіх можливих електромагнітних завад. Тому рекомендується комбінувати їх використання з іншими методами захисту, такими як криптографічне шифрування та фізичні заходи безпеки, для створення комплексної системи захисту.

Узагальнено , фільтри та супресори електромагнітних завад є ефективними методами захисту від навмисних електромагнітних завад. Вони можуть блокувати або приглушувати небажані сигнали, забезпечуючи надійний рівень захисту технічних засобів обробки інформації з обмеженим доступом. Однак, їх використання повинно бути ретельно промислово налаштоване і поєднане з іншими методами захисту для досягнення максимального ефекту.

4.1.3 Криптографічні методи є , я би сказав ефективнішим за інші засобом захисту від навмисних електромагнітних завад. Вони забезпечують конфіденційність, цілісність та аутентичність передачі інформації шляхом застосування різних алгоритмів шифрування та підпису.

Однією з основних переваг криптографічних методів є їх здатність до захисту інформації навіть у випадку, коли навмисні електромагнітні завади спричиняють зміни в передаваному сигналі. Шифрування дозволяє перетворювати дані у такий спосіб, що вони стають незрозумілими для несанкціонованого отримувача, навіть якщо завади спричиняють втрату, спотворення або перехват частини інформації . Криптографічні методи також забезпечують цілісність інформації шляхом використання алгоритмів підпису. Це дозволяє переконатись, що отримані дані не були змінені під час передачі, оскільки будь-яка незначна зміна в даних призведе до недійсного підпису.

Окрім того, криптографічні методи дозволяють забезпечити аутентичність інформації, тобто переконатись у тому, що відправник і отримувач є вірними ідентифікованими сторонами. Це досягається за допомогою електронного підпису, який підтверджує автентичність відправника і неможливість підробки даних.

Важливо відзначити, що криптографічні методи мають свої обмеження і вразливості. Вони можуть бути піддані крипто аналізу, який застосовується для розкриття ключів або порушення інших аспектів криптографічного протоколу. Тому важливо використовувати надійні алгоритми шифрування, ключі достатньої довжини і дотримуватись сучасних стандартів криптографії.

Узагальнено , криптографічні методи є вигідними і ефективними для захисту технічних засобів обробки інформації з обмеженим доступом від навмисних електромагнітних завад. Вони забезпечують конфіденційність, цілісність та аутентичність передачі даних, що робить їх незрозумілими та недоступними для несанкціонованих осіб. Однак, необхідно обирати надійні

алгоритми і ключі, а також поєднувати криптографічні методи з іншими заходами безпеки для створення комплексної системи захисту.

4.1.4 Методи обмеження електромагнітних імпульсів (EMI)

Це є ефективні засоби захисту . Вони спрямовані на запобігання або мінімізацію впливу електромагнітних імпульсів на технічні засоби обробки інформації з обмеженим доступом.

Ефективність методів обмеження електромагнітних імпульсів полягає в їх здатності запобігти або мінімізувати вплив навмисних EMI на технічні засоби обробки інформації. Вони допомагають забезпечити стійкість та надійність роботи систем, зменшити можливість витоку конфіденційної інформації та забезпечити захист від навмисного перехоплення даних. Проте, слід враховувати, що ефективність цих методів може залежати від різних факторів, таких як потужність та характеристики навмисних EMI , технічні особливості системи та вимоги безпеки . Для досягнення максимальної ефективності рекомендується поєднувати кілька методів захисту та використовувати комплексну стратегію захисту від навмисних електромагнітних завад.

4.2 Оцінка вразливостей

4.2.1 Вразливості електромагнітного екранування

Воно також має свої вразливості, які потрібно враховувати при розгляді його ефективності.

Дизайн та якість екранування: Однією з ключових вразливостей є правильний дизайн та якість екранування. Якщо екранування не виконано належним чином, можуть виникати прогалини або слабі місця, через які можуть проникати електромагнітні сигнали. Недостатнє екранування може знизити ефективність методу захисту.

Електромагнітні щілини: Наявність щілин, розривів або інших просторів у структурі екранування може створювати можливість для проникнення електромагнітних сигналів. Навмисні особи можуть використовувати ці щілини для введення шуму або завад до системи.

Заземлення: Відповідне заземлення екранування є важливим аспектом ефективного екранування. Недостатнє заземлення може створювати можливість для проникнення електромагнітних сигналів через екранування. Недостатній контакт землі або відсутність надійного заземлення може знизити ефективність методу.

Частотні характеристики: Ефективність екранування може залежати від частоти електромагнітних сигналів. Деякі екранування можуть бути більш ефективними на певних діапазонах частот, але менш ефективними на інших.

Варто враховувати цей аспект при розробці екранування для конкретних потреб і застосувань.

Фізичний доступ: Хоча екранування може ефективно захищати від електромагнітних завад, фізичний доступ до системи може становити загрозу. Якщо навмисна особа має фізичний доступ до обладнання, вона може обійти екранування або використовувати інші методи для впливу на систему.

Оцінюючи вразливості електромагнітного екранування повинен зазначити що потрібно враховувати конкретні умови застосування та вимоги безпеки. Недоліки екранування можуть бути компенсовані додатковими заходами захисту, такими як криптографічні методи, контроль доступу або системи виявлення та запобігання вторгнень. Розумна комбінація різних методів захисту може забезпечити більш високий рівень безпеки для технічних засобів обробки інформації з обмеженим доступом.

4.2.2 Вразливості фільтрів та супресорів електромагнітних завад

Вони також мають свої вразливості, які потрібно враховувати при оцінці їх ефективності.

Фільтри та супресори ефективні на певних діапазонах частот. Однак, вони можуть бути менш ефективними або навіть неспроможними піддавити електромагнітні завади у інших діапазонах частот. Важливо правильно вибирати і налаштовувати фільтри та супресори для конкретного діапазону, щоб забезпечити найкращий рівень захисту. Існує можливість, що електромагнітні сигнали можуть проходити через паралельні шляхи, які обходять фільтри та супресори, особливо у випадку неправильної інсталяції або недостатньої екранування. Це може створити можливість для проникнення електромагнітних завад у систему. Якщо потужність електромагнітних сигналів дуже велика, фільтри та супресори можуть виявитися неспроможними ефективно піддавити ці завади. В таких випадках може знадобитися використання додаткових методів захисту або потужніших фільтрів та супресорів. Правильне позиціонування та розташування фільтрів та супресорів є важливим аспектом для їх ефективності. Недостатнє розташування або неправильне підключення може призвести до втрати ефективності цих методів захисту. Фільтри та супресори мають обмежену ширину смуги, в якій вони ефективно працюють. Якщо сигнали або завади виходять за межі цієї ширини смуги, ефективність методу може значно знизитися.

Оцінюючи вразливості фільтрів та супресорів повинен сказати що має базуватися на конкретних характеристиках системи, діапазонах частот, потужності сигналів та вимог безпеки. Важливо планувати і реалізовувати правильну конфігурацію та налаштування фільтрів та супресорів, а також

поєднувати їх з іншими методами захисту, щоб забезпечити надійний рівень захисту технічних засобів обробки інформації з обмеженим доступом.

4.2.3 Вразливості криптографічного методу

Криптографічні методи часто вимагають обміну ключами між комунікуючими сторонами. Цей процес може бути вразливим до атак перехоплення або підробки ключів. Якщо ключі потрапляють у руки зловмисника, це може ставити під загрозу безпеку системи.

Криптографічні алгоритми можуть бути піддані розгадуванню або відновленню шляхом криптоаналізу. Якщо алгоритм виявляється слабким або його вразливість вдається використати, це може знизити ефективність захисту.

Криптографічні методи передбачають зберігання ключів в секреті. Однак, якщо ключі стають доступними зловмисникам, це може дозволити їм розшифрувати зашифровану інформацію. Важливо забезпечити надійне зберігання ключів і використання відповідних методів для їх обміну та управління.

Криптографічні методи можуть бути компрометовані через соціальний інжиніринг, коли зловмисники використовують маніпуляцію або переконання людей для отримання доступу до ключів або зашифрованої інформації. Сильні криптографічні методи можуть бути безпечними тільки в тому разі, якщо ключі та інші параметри захищені від таких атак.

Криптографічні операції можуть бути вимогливими до обчислювальних ресурсів. У випадку обмежених пристроїв обробки інформації, які мають обмежену потужність або ресурси, використання складних криптографічних методів може стати проблемою.

Оцінюючи вразливості криптографічних методів повинен зазначити що воно має базуватися на конкретних реаліях і вимогах системи, а також на використовуваних алгоритмах і ключових матеріалах. Важливо проводити оцінку ризиків, враховувати рекомендації відповідних стандартів безпеки та забезпечувати належне впровадження та керування криптографічними методами для досягнення ефективного рівня захисту технічних засобів обробки інформації з обмеженим доступом.

4.2.4 Вразливості методів обмеження електромагнітних імпульсів

Методи обмеження електромагнітних імпульсів (EMI) використовуються для захисту технічних засобів обробки інформації від саме навмисних електромагнітних завад. Проте, вони також мають свої вразливості, які можуть впливати на їх ефективність.

Методи обмеження EMI можуть бути недостатньо ефективними у випадку дуже сильних або спеціально налаштованих електромагнітних імпульсів. Деякі засоби захисту можуть бути не здатні впоратися зі значними рівнями електромагнітної енергії або широким спектром частот, що може допустити проникнення завад в систему.

Деякі методи обмеження EMI можуть мати вплив на працездатність самої системи. Наприклад, застосування фільтрів або супресорів може призводити до зниження якості сигналу або затримки передачі даних. Це може бути неприйнятним для деяких систем, де низька затримка і висока якість сигналу є критичними.

Також деякі методи обмеження EMI можуть вимагати правильного встановлення та налаштування для досягнення оптимальної ефективності. Якщо ці вимоги не дотримуються, метод може бути менш ефективним або навіть неспроможним надати достатнього рівня захисту.

Залежно від швидкого розвитку технологій і комунікаційних стандартів, методи обмеження EMI можуть стати застарілими або неефективними проти нових видів електромагнітних завад. Поява нових способів генерації електромагнітних імпульсів може потребувати постійного оновлення та модернізації методів захисту.

Оцінюючи вразливості методів обмеження EMI повинно враховувати контекст використання, особливості системи, потенційні загрози та ризики. Критичність інформації, яку необхідно захистити, і можливі наслідки вразливостей повинні бути оцінені при виборі методів захисту. Крім того, рекомендації стандартів безпеки та експертний аналіз можуть допомогти визначити ефективність та обмеження методів обмеження EMI.

4.3 Визначення капітальних витрат

Розбір економічної ефективності для вище перерахованих методів захисту від впливу навмисних електромагнітних завад допомагає оцінити витрати та користь, пов'язані з впровадженням і застосуванням цих методів.

1. Електромагнітне екранування:

- Витрати: Вартість електромагнітного екранування може бути значною, оскільки вимагається встановлення спеціальних екранів та матеріалів, що забезпечують електромагнітну ізоляцію. Витрати також пов'язані з проектуванням, монтажем та перевіркою ефективності екранування.

-Користь: Електромагнітне екранування може забезпечити високий рівень захисту від електромагнітних завад, дозволяючи знизити ризик витоку чутливої інформації та забезпечити надійну роботу технічних засобів обробки інформації.

-Оцінка вразливостей: Електромагнітне екранування може бути вразливим до недоліків у проектуванні та монтажі, таких як неправильне прилягання екранів, просічки або слабкі місця у конструкції. Такі недоліки можуть знизити ефективність екранування і дозволити проникнення електромагнітних завад.

2.Фільтри та супресори електромагнітних завад:

- Витрати: Вартість фільтрів та супресорів може бути помірною, але вона залежить від потужності, ширини смуги і інших технічних характеристик. Додаткові витрати можуть виникнути від установки, налаштування та технічної підтримки.

- Користь: Фільтри та супресори дозволяють зменшити рівень електромагнітних завад і забезпечити нормальну роботу технічних засобів обробки інформації. Вони можуть бути ефективними в захисті від широкого спектру електромагнітних завад.

- Оцінка вразливостей: Фільтри та супресори можуть бути вразливими до високовольтних або широкосмугових електромагнітних завад, які можуть впливати на їхню ефективність. Крім того, недостатнє налаштування або неправильний вибір фільтрів може обмежити їхню ефективність.

3.Криптографічні методи:

- Витрати: Впровадження криптографічних методів може вимагати значних витрат на розробку алгоритмів, реалізацію систем шифрування та криптографічну інфраструктуру. Крім того, витрати пов'язані з підтримкою та оновленням криптографічних систем.

- Користь: Криптографічні методи забезпечують захист інформації шляхом шифрування даних, підпису та інших криптографічних механізмів. Вони можуть забезпечити конфіденційність, цілісність та автентичність даних.

- Оцінка вразливостей: Криптографічні методи можуть бути вразливими до атак, таких як підбір ключа, атаки на протоколи аутентифікації або аналіз секретного ключа. Крім того, недоліки у реалізації алгоритмів шифрування або неправильне управління ключами можуть підірвати безпеку криптографічних систем.

4.Методи обмеження електромагнітних пульсів:

- Витрати: Витрати на застосування методів обмеження електромагнітних пульсів можуть бути високими, оскільки вони вимагають встановлення спеціального обладнання та інфраструктури, такого як фільтри, гальванічна ізоляція, захистний обв'язок тощо. Крім того, витрати пов'язані з впровадженням стандартів та регуляторних вимог.

- Користь: Методи обмеження електромагнітних пульсів можуть забезпечити захист від потенційно шкідливих електромагнітних пульсів, що можуть порушити роботу технічних засобів обробки інформації. Вони можуть знизити ризик пошкодження або некоректної роботи техніки.

- Оцінка вразливостей: Методи обмеження електромагнітних пульсів можуть бути вразливими до нових типів електромагнітних загроз, які можуть вимагати постійного оновлення та підтримки обладнання. Крім того, неадекватне проектування або неправильне використання методів можуть знизити їхню ефективність.

Загальна оцінка економічної ефективності цих методів залежить від конкретних потреб, бюджету та характеристик системи захисту. Кожен метод має свої переваги та обмеження. І повинен бути розглянутий як початковий пункт для визначення найбільш підходящого методу для вашого конкретного випадку.

4.4 Висновки

На підставі проведеного аналізу і дослідження впливу навмисних електромагнітних завад на технічні засоби обробки інформації з обмеженим доступом, можна зробити наступні висновки:

-Навмисні електромагнітні завади є серйозною загрозою для безпеки надійності технічних засобів обробки інформації з обмеженим доступом. Вони можуть спричиняти порушення роботи, виток чутливої інформації, або навіть фізичне пошкодження пристроїв.

-Ефективний захист від навмисних електромагнітних завад вимагає комплексного підходу, включаючи різні методи і технології. Комбінація різних захисних заходів може забезпечити кращу захисту технічних засобів обробки інформації.

-Електромагнітне екранування є ефективним методом захисту від електромагнітних завад. Воно дозволяє зменшити рівень електромагнітного випромінювання та забезпечити нормальну роботу пристроїв. Проте, воно може бути вразливим до високовольтних або широкосмугових завад, і його ефективність залежить від якості і правильного встановлення екранів.

-Використання фільтрів та супресорів електромагнітних завад також може бути ефективним методом захисту. Вони допомагають знизити рівень електромагнітних завад і забезпечити нормальну роботу пристроїв. Однак, їх ефективність може бути обмежена неправильним вибором або налаштуванням фільтрів.

-Криптографічні методи є важливим компонентом захисту від навмисних електромагнітних завад. Вони дозволяють шифрувати передану інформацію, що забезпечує конфіденційність інформації навіть у випадку перехоплення. Проте, вони можуть бути вразливими до криптоаналітичних атак, і їх ефективність залежить від правильного вибору алгоритмів і реалізації.

-Методи обмеження електромагнітних пульсів можуть забезпечити ефективний захист від шкідливих впливів електромагнітних імпульсів. Вони можуть використовувати фільтри, гальванічну ізоляцію, захистний обв'язок та інші заходи для зменшення впливу електромагнітних пульсів на пристрої. Проте, їх ефективність може бути обмежена новими типами електромагнітних загроз, і вони вимагають постійного оновлення та підтримки.

Загалом, для забезпечення ефективного захисту технічних засобів обробки інформації з обмеженим доступом від навмисних електромагнітних завад, рекомендується комбінувати різні методи і технології. Оцінка ефективності кожного методу повинна враховувати його переваги, обмеження, вартість та вразливості. Крім того, регулярне оновлення та підтримка захисних заходів є важливими для забезпечення стійкості системи захисту у змінних умовах загроз.

Перелік літератури

1.David A. Weston, "Electromagnetic Compatibility: Principles and Applications" (2013)

2.Karl F. Warnick, "Principles of Electromagnetic Waves and Materials" (2013)

3.J. A. Brandão Faria, "Introduction to Electromagnetic Compatibility" (2016)

4.Oleg Wasynczuk, "Electromagnetic Compatibility in Power Systems" (2018)

5.S. M. Ghandour, "EMC for Power Electronics and Electric Drives" (2018)

6.George M. Kunkel, "Electromagnetic Compatibility Engineering: Principles, Measurements, Technologies, and Computer Models" (2017)

7.William G. Duff, "EMC for Systems and Installations" (2011)

8.Richard Standler, "Electromagnetic Compatibility: Methods, Analysis, Circuits, and Measurement" (2015)

9.Tim Williams, "EMC for Product Designers" (2011)

10.S. V. Hulicius, "EMC for Systems and Installations" (2013)

11.Gary L. Johnson, "Handbook of Electromagnetic Compatibility" (2017)

12.В.В. Андрійчук, "Електромагнітна сумісність. Загальні питання" (2005)

13. О.В. Лебедєв, "Електромагнітна сумісність систем радіоелектронного захисту" (2008)

14.В.О. Марченко, "Електромагнітна сумісність та якість електроенергії" (2013)

15.В.В. Ковальов, "Електромагнітна сумісність систем електропостачання" (2012)