МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **МЕТОДИКА ПАСИВНОГО ЗАХИСТУ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВІД ВИТОКУ ІНФОРМАЦІЇ КАНАЛАМИ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ**

Студент групи СЗД-41 Малашин Ілля Євгенович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н., доц. Г.В. Шуклін

«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Малашину Іллі Євгеновичу

1. Тема роботи: Система забезпечення захисту інформації в кімнаті нарад

Затверджена наказом по університету від «16» лютого 2022 р. № 22

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: є захист інформації від витоку за рахунок побічного електромагнітного випромінювання автоматизованих систем на об'єкті інформаційної діяльності.

4. Предмет дослідження: є методи та засоби захисту інформації автоматизованих систем на об'єкті інформаційної діяльності.

5. Мета роботи: розробка системи захисту інформації автоматизованих систем від витоку за рахунок побічного електромагнітного випромінювання на об'єкті інформаційної діяльності.

6. Перелік питань, які мають бути розроблені:

1. Аналіз існуючих підходів до захисту інформації автоматизованих систем від витоку за рахунок електромагнітного випромінювання .

2. Вимоги до захисту інформації автоматизованих систем на об'єкті інформаційної діяльності.

3. Засоби несанкціонованого отримання інформації в автоматизованих системах.

4. Методи захисту інформації автоматизованих систем з урахуванням побічного електромагнітного випромінювання.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Малашин І.Є.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз існуючих підходів до захисту інформації автоматизованих систем від витоку за рахунок електромагнітного випромінювання	До 04.04.2022	Виконано
2	Вимоги до захисту інформації автоматизованих систем на об'єкті інформаційної діяльності	До 25.04.2022	Виконано
3	Засоби несанкціонованого отримання інформації в автоматизованих системах	До 06.05.2022	Виконано
4	Методи захисту інформації автоматизованих систем з урахуванням побічного електромагнітного випромінювання	До 13.05.2022	Виконано
5	Перевірка роботи на плагіат + Передзахист	До 01.06.2022	
6	Захист роботи	З 13.06.22 по 21.06.22	
7	Випуск	30.06.2022	

Студент _____ Малашин І.Є.

(підпис) (прізвище тініціали)

Керівник бакалаврської роботи _____ Шуклін Г.В.

(підпис) (прізвище та ініціали)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЗІ	— захист інформації
ІБ	— інформаційна безпека
ІТ	— інформаційна технологія
КВІ	— канал витоку інформації
НСД	— несанкціонований доступ
НТІ	— науково-технічна інформація
АСУ	— автоматизована система управління
БД	— база даних (банк даних)
ІС	— інформаційна система
ІзОД	— інформація з обмеженим доступом
ОТЗС	основні засоби і системи
ТЗПІ	— технічні засоби пересилання, оброблення, зберігання, відображення інформації
ДТЗС	— допоміжні технічні засоби н системи
ПЕМВ	— канал побічних електромагнітних випромінювань
ПЕМВН	— канал побічних електромагнітних випромінювань та наводок
ТЗР	— технічні засоби розвідки
СТЗ	— спеціальні технічні засоби
ЕМС	— електромагнітна сумісность

ЗМІСТ

ВСТУП 8

РОЗДІЛ 1.ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ 9

1.1 Основні положення 6

Нормативні посилання 9

Терміни і визначення 10

Джерела небезпечних сигналів 11

Технічні засоби пересилання, оброблення, зберігання, відображення інформації (ТЗПІ) 13

Основні технічні засоби 13

Допоміжні технічні засоби і системи 14

Об'єкти інформатизації, що захищаються 15

1.2. Утворення технічних каналів витоку інформації 16

Електромагнітні канали витоку інформації. 17

Електричні канали витоку інформації (ЕКВІ) 20

1.3. Паразитні зв'язки і наведення. 22

Паразитні зв'язки 24

Випадкові антени 27

Зони небезпечних сигналів 28

Електричний канал витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах 29

Канал побічних електромагнітних випромінювань ОТЗС 30

Канал побічних електромагнітних випромінювань ДТЗС 32

Канал “паразитної” модуляції сигналів ВЧ генераторів 33

Основні параметри витоку інформації каналами ПЕМВН: 34

1.4. Перехоплення інформації 35

РОЗДІЛ°2. ДОСЛІДЖЕННЯ ПЕМВН 38

2.1. Загальна структура досліджень ПЕМВ 38

2.2. Механізм виникнення ПЕМВН засобів цифрової електронної техніки. 38

Види і джерела електромагнітних завад 39
Кондуктивні завади 40
Індуктивні завади 41
Методи зменшення випромінюваних завад 42
2.3. Оцінка рівня ПЕМВН. 45
Оцінка рівня ПЕМВ з точки зору електромагнітної сумісності 45
Оцінка рівня випромінювань при вирішенні задач захисту інформації 48
Метод оціночних розрахунків. 49
Метод примусової (штучної) активізації. 49
Метод еквівалентного приймача. 49
Аналіз можливості витоку інформації через ПЕМВ. 49
РОЗДІЛ°3. ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ 50
3.1 Загальні рекомендації з технічного захисту інформації 50
3.1.1. Організаційні заходи 51
3.1.2 Підготовчі технічні заходи 52
3.1.3 Технічні заходи 54
3.2. Способи і методи захисту інформації від витоку через ПЕМВ. 58
Електромагнітне екранування приміщень 58
Криптографічне закриття інформації 59
Активне радіотехнічне маскування 59
Енергетичні методи 59
Метод «синфазної завади» 60
Статистичний метод 60
Методи захисту обчислювальної техніки від ПЕМВН 60
3.3 Порядок контролю за станом технічного захисту інформації 62
ВИСНОВКИ 65
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 66

ВСТУП

Давній термін, який використовується - PEMVN - у зарубіжній літературі має синоніми TEMPEST та компрометуюча радіація.

Дослідження паразитного випромінювання почалися на початку 20 століття. Першою, мабуть, була робота Герберта Ядлі, який розробив способи виявлення та перехоплення симпатичної радіопередачі для армії США. У дослідженнях Ядлі звернув увагу на наявність випадкового випромінювання і припустив, що вони також можуть надати корисну інформацію.

Проте повномасштабні (але секретні) дослідження випадкового «компрометуючого» електромагнітного випромінювання почалися наприкінці 40-х – початку 50-х років.

Коли закінчилась Друга світова війна, прослухаючи секретні розмови радянських представництв у Німеччині (Берлін), спецслужби США помітили не звичайний шум у вигляді слабких клацань. Як виявилося пізніше, це був сигнал, випромінюваним електромагнітом друкувального пристрою телетайпної машинки, що відтворює відкритий текст. Відновлення цього сигналу та передачі його на телетайп, співробітники ЦРУ змогли отримати той самий відкритий текст.

В книзі Spycatcher колишній співробітник MI5 Пітер Райт розповідає про початок атак Tempest на криптографічні машини.

1960 року Лондон вів перемовини щодо вступу до Європейського економічного співтовариства, і прем'єр-міністр був стурбований тим, що саме французький лідер де Голль виступав проти цього рішення..

Через це розвідці доручили визначати позицію французів на майбутніх переговорах. Спроба порушити французький дипломатичний кодекс провалилася. Однак Райт і його помічник Тоні Сайл помітили, що зашифрований трафік несе слабкий сторонній сигнал. Райт і Сайл розробили обладнання для його відновлення і прийшли до висновку, що сигнал був відкритим повідомленням, яке чомусь «витік» через машину для шифрування.

Сьогодні державні системи (в даному випадку більшість систем, які раніше використовувалися і досі використовувалися в державних установах США) використовують дороге металеве екранування окремих пристроїв, об’єктів, а іноді

й окремих будівель. Однак навіть для закритих броньованих приміщень існує принцип поділу техніки на так звані «червоні» і «чорні». «Червоне» обладнання, яке використовується для обробки конфіденційної інформації (наприклад, монітори), повинно бути ізольоване фільтрами та екранами від «чорного» обладнання (наприклад, радіомодемів), яке передає несекретні дані. Обладнання, яке має обидва типи з'єднань («червоне», «чорне»), наприклад, шифрувальні машини або захищені робочі станції, повинно бути спеціально перевірено.

Усі дослідження TEMPEST та переселення раніше трималися в таємниці, і перший публічний опис TEMPEST з'явився у шведській доповіді Крістіана Бекмана на початку 1980-х рр. Однак стаття голландця Віма ван Ейка, опублікована в 1985 р., привертає більшу увагу до проблеми.

Стаття («Електромагнітне випромінювання від модулів відеодисплея: ризик перехоплення інформації»). Автор показав, що вміст екрану монітора можна відновити дистанційно за допомогою дешевої побутової техніки — телевізора, в якому синхронізатори замінили генератори, налаштовані вручну.

Лютого 1985 року ван Ейк спільно з British Broadcasting Corporation провели експеримент з «підслуховування» з позитивним результатом.

Результати, отримані Ван Ейком, пізніше були підтверджені Мюллером, Бернштейном і Кольбергом, які розробили різні техніки екранування обладнання.

В 1987 році, Садерс продемонстрував, що екрановані кабелі RS-232 можна транспортувати отруєними.

Переломною можна назвати середину 80-х, після якої кількість відкритих дописів на цю тему з кожним роком почала неухильно зростати. Проблему витоку інформації через ПЕМВН почали вивчати не тільки на закритих військових кафедрах, а й у громадських організаціях.

РОЗДІЛ 1. ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ

1.1 Основні положення

Нормативні посилання

Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 09.09.94 № 632.

ТР ТЗІ - ПЕМВН-95. Документ системи технічного захисту інформації. Рекомендації технічного захисту інформації від витоків через радіаційні канали та випадкових електромагнітних перешкод.

Цей нормативний документ призначений для організації захисту інформації з обмеженим доступом (далі - інформація - ІСО) від витоку через канали випромінювання та паразитних електромагнітних перешкод (ПЕМВН).

Положення цього документа є тимчасовими та поширюються на центральні та місцеві органи виконавчої влади, органи виконавчої влади Республіки Крим, місцеві Ради народних депутатів та їх органи, військові частини всіх військових формувань, підприємств, установ та організацій усіх форм власності, представництва України за кордоном та громадяни, які володіють, користуються та розпоряджаються інформацією з обмеженим доступом.

Технічному захисту підлягає ІСО, носіями якого є поля та сигнали, що утворюються в результаті технічних засобів передачі, обробки, зберігання, відображення інформації (ТЗПІ), а також допоміжних технічних засобів і систем (ДТЗС). ТЗПІ та ДТЗС можуть бути захищеними та незахищеними.

Терміни і визначення

1. **конфіденційність** - властивість, яка не підлягає розголосові; довірливість, секретність, суто приватність.;

- **цілісність** - внутрішня єдність, пов'язаність усіх частин чого-небудь, єдине ціле;

- **доступність** - властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу;

- **технічний захист інформації** (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

- **інформаційна система** - автоматизована система, комп'ютерна мережа або система зв'язку;
- **дозвіл** - документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;
- **комплекс технічного захисту інформації** - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Джерела небезпечних сигналів

Сигнал (в теорії інформації та зв'язку) - носій інформації, що використовується для передачі повідомлень у системі зв'язку. Маркер може бути згенерований, але його отримання не є обов'язковим, на відміну від повідомлення, яке призначене для отримання стороною, яка отримує, інакше це не повідомлення. Сигналом може бути будь-який фізичний процес, параметри якого змінюються (або змінюються) відповідно до переданого повідомлення.

Концепція сигналу дозволяє абстрагуватися від певної фізичної величини, такої як струм, напруга, акустична хвиля, і розглядати поза фізичного контексту явище, пов'язане з кодуванням інформації та отриманням її із сигналів.

Часто сигнал є функцією часу, параметри якого можуть нести необхідну інформацію. Спосіб запису цієї функції, так само як і спосіб запису інтерференційного шуму, називають математичною моделлю сигналу. Сигнали можуть викликати зміни властивостей фізичних тіл. Це явище називається реєстрацією сигналу. Сигнали, записані на матеріальний носій, називаються даними.

Для отримання інформації з даними необхідно застосовувати до них методи, що перетворюють дані в поняття, що сприймаються людською свідомістю.

Об’єкти, які випромінюють сигнали, містять джерела сигналу**.**

Джерела маркерів, які створюються та використовуються для забезпечення зв’язку між авторизованими абонентами, називаються функціональними джерелами маркерів.

До основних джерел функціональних сигналів відносяться:

- джерела систем зв'язку;

- передавачі радіотехнічних систем;
- випромінювачі акустичних сигналів;
- люди.

Якщо сигнали становлять загрозу інформаційній безпеці, їх умовно називають небезпечними.

Функціональні сигнали стають небезпечними, якщо не вжити заходів інформаційної безпеки.

Існує велика група джерел, з яких можуть поширюватися несанкціоновані сигнали від захищеного і які виникають випадково або створюються зловмисниками. Випадкові червоні прапори виникають незалежно від бажання власника інформації, і часто без спеціального розслідування виявити їх практично неможливо.

Для забезпечення свідомого захисту інформації необхідно враховувати сутність джерел сигналу. Загроза викрадення інформації через її витік створюється сигналами, що виникають випадково в результаті випадкового випромінювання та наведення. Якщо ці сигнали містять захищену інформацію, то вони небезпечні. Джерелами небезпечних сигналів є радіо- та електричні елементи та пристрої в принципі будь-яких електронних та електричних пристроїв та апаратів. Деякі засоби запису, опитування та передачі інформації забезпечують додаткові заходи інформаційної безпеки для запобігання появі небезпечних сигналів. Однак технічні заходи щодо захисту інформації значно підвищують вартість цих електронних пристроїв і роблять їх неконкурентоспроможними на ринку. Тому основною тенденцією запобігання витоку інформації із незахищених електронних носіїв є використання додаткових засобів захисту інформації.

Незважаючи на різноманітність типів носіїв, джерело небезпечних сигналів можна класифікувати на основі їх фізичної природи наступним чином:

- акустоелектричні перетворювачі;
- випромінювачі низькочастотних сигналів;
- випромінювачі високочастотних сигналів;
- паразитні зв'язки і наведення.

Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля та сигнали, що формуються технічними засобами передачі, обробки, зберігання, відображення інформації (ТЗПІ), а також допоміжними технічними засобами та системами (ДТЗС).

Технічні засоби пересилання, оброблення, зберігання, відображення інформації (ТЗПІ)

Радіоелектронні та електричні пристрої та системи, що містять потенційні джерела небезпечних сигналів, поділяються на основні та допоміжні. Основні засоби та системи (ОСЗ) забезпечують обробку, зберігання та передачу захищеної інформації, технічні допоміжні засоби до системи (ОСС) - іншу інформацію.

Основні технічні засоби

ТЗПІ, застосовувані для оброблення інформації з обмеженим доступом, називаються **основними технічними засобами** (ОТЗ).

До основних засобів масової інформації та технічних систем належать засоби масової інформації (системи) та їх комунікації (лінії зв'язку).

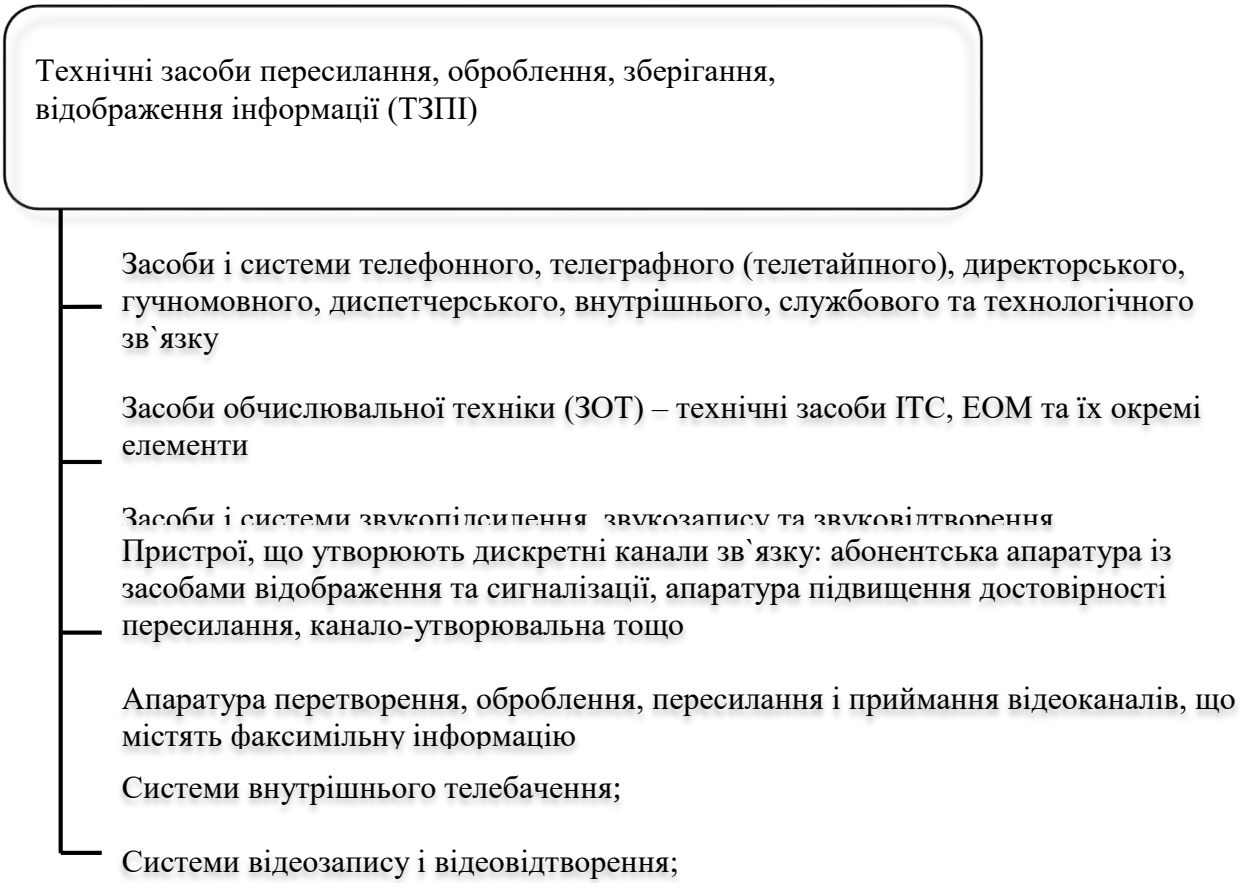

Рис. 1.1. Технічні засоби пересилання, оброблення, зберігання, відображення інформації.

З точки зору захисту ці технічні засоби та системи називають основними технічними засобами (ОТЗ). ТЗПІ може бути захищеним і незахищеним.

Допоміжні технічні засоби та системи (АТС) не призначені для обробки захищеної інформації, але можуть бути розміщені разом із ЗБС у контрольованій зоні.

Останнє спостереження має принципове значення, оскільки саме близькість місця аварії до НТС змушує нас розглядати засоби та системи як потенційні джерела небезпечних сигналів, які потребують захисту разом із HTS.

Допоміжні технічні засоби і системи

Допоміжні технічні засоби і системи (ДТЗС)

- ❖ Засоби і системи спеціальної охоронної сигналізації, пожежної сигналізації.
- ❖ Система дзвінкової сигналізації.
- ❖ Контрольно-вимірювальна апаратура (КВА).
- ❖ Засоби і системи кондиціонування.
- ❖ Засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення.
- ❖ Засоби і системи годинофікації

Рис. 1.2. Допоміжні технічні засоби і системи

ДТЗС можуть бути захищеними і незахищеними.

Слід зазначити, що багато ОТЗС і ДТЗС схрещуються. Дійсно, в одній кімнаті можна розмістити інструменти, наприклад, однотипні комп'ютери, одні з яких є основними, інші – допоміжними. До Інтернету можна підключити допоміжний комп'ютер, що неможливо зробити для комп'ютера, який є основним засобом обробки інформації.

Елементами ТЗПІ та ДТЗС можуть бути зосереджені випадкові антени (обладнання та його блоки) або розподілені випадкові антени (кабельні лінії та дроти).

Зазначеними елементами можуть бути:

- кінцеві технічні засоби і прилади;

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

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

- елементи заземлення та електроживлення.

Як джерело витоку інформації найцікавішими є аварії, що виходять за межі підконтрольної зони.

Об'єкти інформатизації, що захищаються

Об'єкт інформатизації (ОІ), що захищається, – це сукупність інформаційних ресурсів, що містять відомості обмеженого доступу, ТЗОІ обмеженого доступу, ДТЗС, приміщень або об'єктів (будівель, споруд), в яких вони встановлені.

Виділені приміщення (ВП) – приміщення, призначені для ведення закритих переговорів, що містять відомості з обмеженим доступом.

Приміщення, що захищаються, – приміщення, призначені для ведення конфіденційних переговорів.

Захищені інформаційні об’єкти, спеціалізовані засоби та захищені об’єкти мають бути сертифіковані відповідно до вимог інформаційної безпеки.

Об'єкти засобів обчислювальної техники (ЗОТ) – об'єкти інформатизації, на яких обробка інформації здійснюється з використанням комп’ютерної техніки.

Об’єкт інформатизації, як об’єкт розвідки з боку порушника, включає ряд джерел (рис. 1.3), що дозволяють дістати доступ до закритих відомостей через перехоплення каналов витоку інформації.

Рис. 1.3 Об’єкт інформатизації, як об’єкт розвідки

Як об’єкт захисту, інформаційні об’єкти (ІО), які захищаються, не можна описати без поняття контрольованої території.

Контрольована зона (КЗ) - це територія, на якій виключено неконтрольоване перебування осіб і транспортних засобів, які не мають допуску.

Межа контрольованої зони – периметр території організації, що охороняється, а також конструкції охороняємої будівлі або частини будівлі, якщо вони розміщені на території, що не охороняється.

Контрольована зона визначається керівництвом організації, виходячи з конкретних обставин розташування об'єкта та можливості використання технічних засобів перехоплення.

Крім з’єднувальних ліній ОТЗС і ДТЗС, поза контролем можуть простягатися дроти та кабелі, які їм не належать, але проходять через приміщення, де встановлено технічне обладнання, а також металеві труби опалення, водопостачання та інші електропровідні металеві конструкції. площа. Такі дроти, кабелі та провідні елементи називаються зовнішніми провідниками.

Незважаючи на різноманітність типів носіїв, джерело небезпечних сигналів можна класифікувати на основі їх фізичної природи наступним чином:

- акустоелектричні перетворювачі;
- випромінювачі побічних низькочастотних сигналів;
- випромінювачі побічних високочастотних сигналів;
- паразитні зв'язки і наведення.

1.2. Утворення технічних каналів витоку інформації

Розглянемо сутність та форми (фізичні основи, принципи та порядок) формування технічних каналів витоку інформації, яка обробляється основними технічними засобами та системами.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела інформативного сигналу (наприклад, ТЗОІ), технічного засобу, що здійснює перехоплення інформації, і фізичного середовища, в якому поширюється інформативний сигнал (рис. 1.4).

Рис. 1.4 Схема технічного каналу витоку інформації в ТЗОІ

Класифікація технічних каналів витоку інформації приведена на рис. 1.5.

Рис. 1.5 Класифікація технічних каналів витоку інформації в ІТС

Електромагнітні канали витоку інформації.

В електромагнітних каналах витоку інформації (ЕМКВІ) носієм небезпечної інформації є *електромагнітні випромінювання* (ЕМВ), що виникають при обробці інформації ТЗОІ. Причини виникнення цих каналів показані на рис. 1.6.

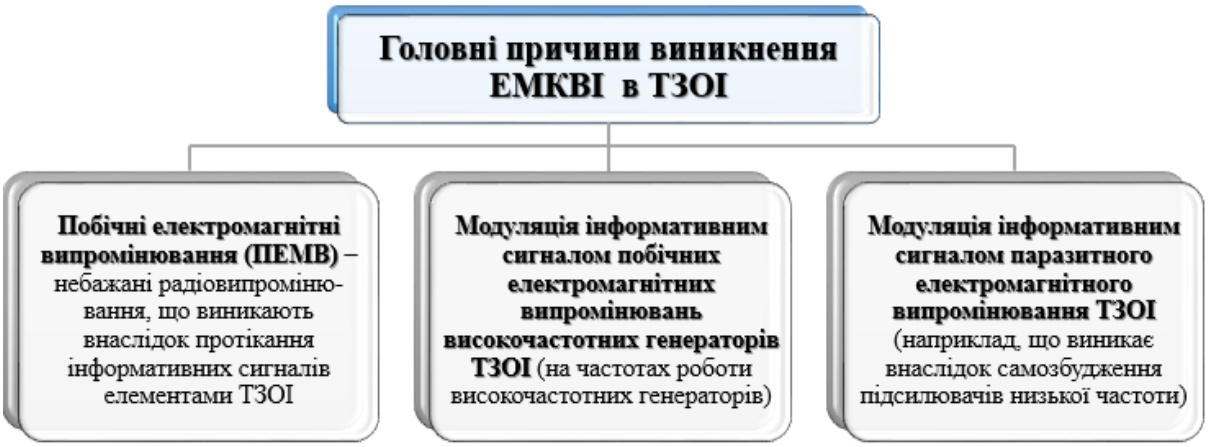

Рис. 1.6 Причини виникнення електромагнітних каналів витоку інформації

У деяких ТЗОІ (наприклад, системах підсилення звуку) носієм інформації є електричний струм, параметри якого (струм, напруга, частота і фаза) змінюються за законом зміни інформаційного голосового сигналу. При протіканні електричного струму через струмопровідні елементи ТЗОІ та їх сполучні лінії в навколишньому просторі виникає змінне електричне та магнітне поле. Отже, елементи ТЗОІ є випромінювачами електромагнітного поля, яке модулюється законом зміни інформаційного сигналу.

Найбільш небезпечними для витоку інформації, що обробляється в ОТЗС, є канали орієнтації та паразитне електромагнітне випромінювання (канали PEMVN).

Ініціаторами виникнення ПЕМВ можуть бути різного роду високочастотні генератори:

- задаючі генератори;
- генератори тактової частоти;
- генератори стирання і підмагнічивання магнітофонів;
- гетеродини радіоприймальних і телевізійних пристроїв;
- генератори вимірювальних приладів і т.д.

Рис. 1.7 ілюструє можливі режими роботи обчислювальної техніки, в яких виникають ПЕМВ. Діапазон можливих частот ПЕМВ ЗОТ може складати 10 кГц – 2 ГГц.

Рис. 1.7 Режими оброблення інформації в ЗОТ, в яких виникають ПЕМВ

Розсіяне електромагнітне випромінювання ТЗОІ - це випадкове радіовипромінювання, яке виникає в результаті самозбудження генеруючих або підсилювальних блоків ТЗОІ через розсіяні з'єднання. У більшості випадків такі з'єднання виникають за рахунок випадкових перетворень негативного зворотного зв'язку (індуктивного чи ємнісного) в паразитний позитивний, що призводить до переходу підсилювача з режиму посилення в режим автоматичного формування сигналу. Частота самогенерації (самозабудження) знаходиться в межах робочих частот нелінійних елементів у підсилювачах (наприклад, напівпровідникові прилади, вакуумні лампи тощо).

У деяких випадках розсіяне електромагнітне випромінювання модулюється інформаційним сигналом відповідно до змін параметрів інформаційного сигналу, що впливають на нього.

Умови для виникнення електромагнітного каналу витоку інформації

Простір навколо ТЗОІ, на межі і за межами якого напруженість електричної (***E***) або магнітної (***H***) складової електромагнітного поля не перевищує допустимого (нормованого) значення ($\boldsymbol{E \le E_н; H \le H_н}$) називається **небезпечною зоною 2** (*R*2).

Зона *R*2 для кожного ТЗОІ визначається інструментально-розрахунковим методом при проведенні спеціальних досліджень ТЗОІ на ПЕМВ і вказується в приписі на їх експлуатацію або сертифікаті відповідності.

Умови для виникнення електромагнітного каналу витоку інформації (рис. 1.9):

1) відстань від ТЗОІ до межі контрольованої зони має бути менш зони $R2$ ($R < R2$);
2) в межах зони $R2$ можливе розміщення стаціонарних або перевозимих (переносимих) засобів розвідки ПЕМВН

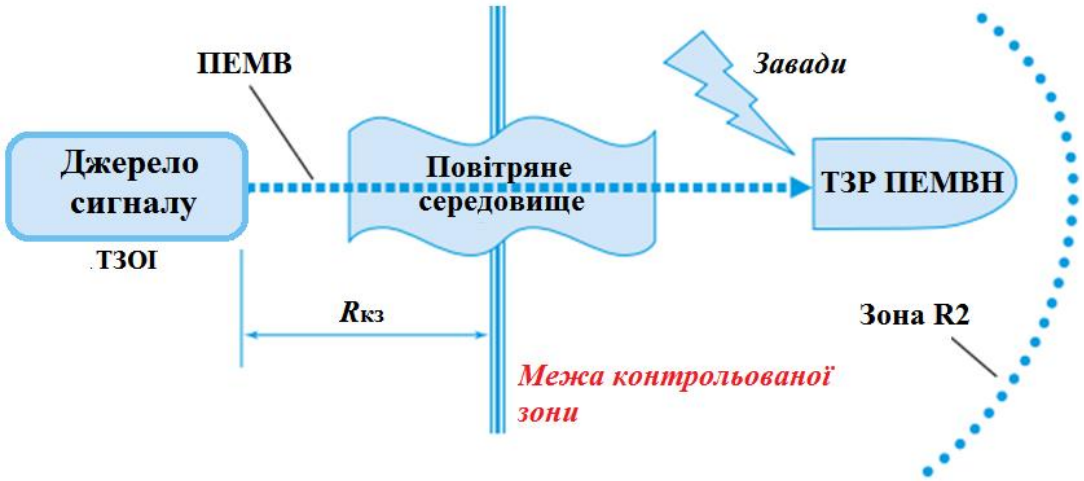

Рис. 1.9 Умови для виникнення електромагнітного каналу витоку інформації

Електричні канали витоку інформації (ЕКВІ)

Причинами виникнення ЕКВІ є наведення інформативних сигналів.

Довідником інформаційних сигналів є струми та напруги в струмопровідних елементах, викликані падаючим електромагнітним випромінюванням, ємнісними та індуктивними з'єднаннями електричних елементів.

Наведені інформативні сигнал виникають:

- у лініях електроживлення ТЗОІ;
- у лініях електроживлення і сполучних лініях ДТЗС;
- у ланцюгах заземлення ТЗОІ і ДТЗС;
- у сторонніх провідниках (металевих трубах систем опалювання, водопостачання, металоконструкціях і т.д.).

Поява інформаційних сигналів у ланцюзі живлення ТЗОІ можлива як за рахунок ПЕМВ, так і за наявності внутрішніх паразитних ємнісних та (або) індуктивних з’єднань випрямного пристрою блоку живлення ТЗОІ. Наприклад, в

підсилювачі низької частоти струми посиленого сигналу замикаються накоротко через джерело живлення, створюючи падіння напруги на його внутрішньому опорі, яке при недостатньому загасання в фільтрі випрямляча може бути виявлено на лінії живлення.

На додаток до заземлюючих провідників, які використовуються для прямого підключення TZOI до заземлювального ланцюга, гальванічне заземлення може мати кілька провідників, що виходять за межі контрольованої зони. До них належать нульовий провід електромережі, екрани (металеві оболонки) з'єднувальних кабелів, металеві труби систем водопостачання та опалення, металева арматура залізобетонних конструкцій тощо. Усі ці провідники разом із заземлюючим пристроєм утворюють розгалужену систему заземлення, на яку можна подавати інформаційні сигнали.

Крім того, навколо заземлюючого пристрою в землі з’являється електромагнітне поле, яке також є джерелом інформації.

Різні технічні засоби, лінії їх з'єднання, а також лінії електропередачі, зовнішні провідники та заземлення відіграють роль випадкових антен, з прямим підключенням (через струмоприймач або індукційний датчик), до яких засоби розвідки PEMVN можуть перехоплювати інформаційні сигнали.

Залежно від причин виникнення наведення інформативних сигналів можна розділити на:

- наведення в електричних ланцюгах ТЗОІ, викликані інформативними побічними і (або) паразитними електромагнітними випромінюваннями ТЗОІ;
- наведення в сполучних лініях ДТЗС і сторонніх провідниках, викликані інформативними побічними і (чи) паразитними електромагнітними випромінюваннями ТЗОІ;
- наведення в електричних ланцюгах ТЗОІ, викликані внутрішніми ємнісними і (або) індуктивними зв'язками («просочування» інформативних сигналів в ланцюзі електроживлення через блоки живлення ТЗОІ);
- наведення в ланцюгах заземлення ТЗОІ, викликані інформативними ПЕМВ ТЗОІ, а також гальванічним зв'язком схемної (робочої) землі і блоків ТЗОІ.

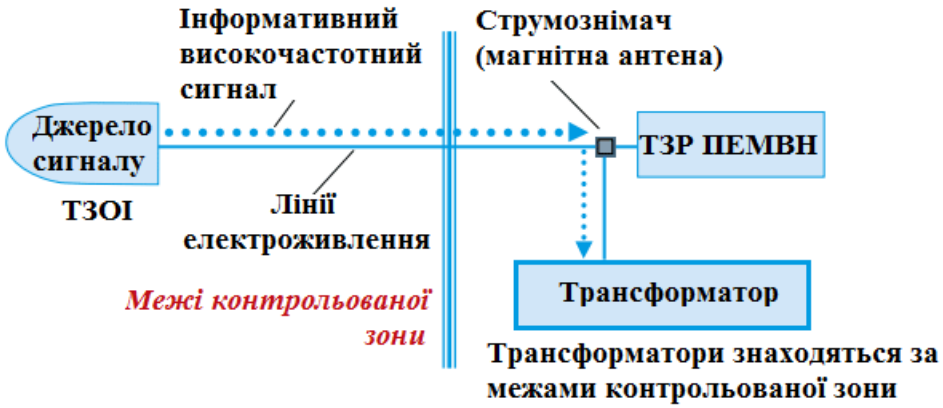

Рис. 1.10 Схема технічного каналу витоку інформації, що виникає за рахунок наведень інформативних сигналів в лініях електроживлення ТЗОІ

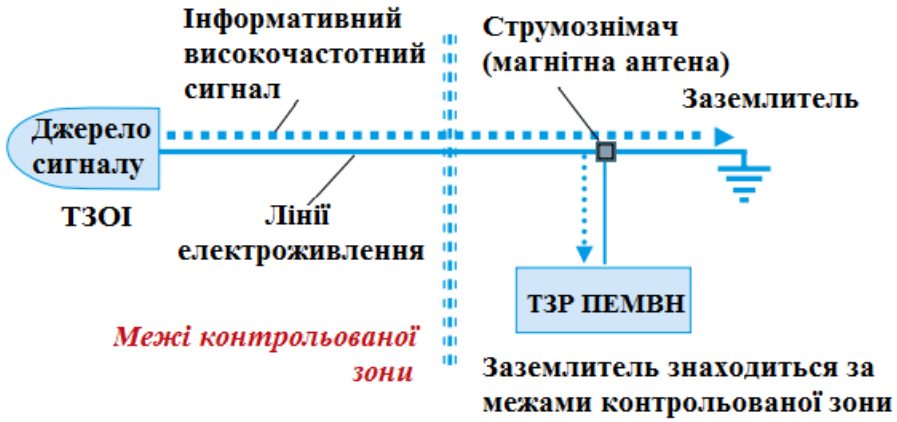

Рис. 1.11 Схема технічного каналу витоку інформації, що виникає за рахунок наведень інформативних сигналів в ланцюгах заземлення ТЗОІ

1.3. Паразитні зв'язки і наведення.

Фізичною основою випадкових небезпечних сигналів, що виникають при роботі в приміщенні, відведеному для радіо та електроприладів, є вторинне та направляюче електромагнітне випромінювання (СЕМВН). Під паразитними перешкодами розуміють передачу напруги від одного радіоелемента до іншого, не передбаченого його схемою та конструкцією. Така порада виникає через наявність паразитного зв’язку між цими елементами, з’єднання електричних ланцюгів, яке з’явиться незалежно від бажання дизайнера.

Паразитний напрямний призводить до появи на виході елемента напруг і струмів, які не відповідають його основному призначенню. У ряді випадків паразитні напрямні на вході підсилювача напруги, які утворюються на його виході,

можуть викликати самозбудження підсилювача або змінювати його характеристики.

При розгляді паразитних наведень доводиться завжди мати справу з трьома елементами:

1. джерелом напруги. що наводиться;

2. приймачем напруги. що наводиться;

3. паразитним зв'язком між ними.

При розгляді будь-якої проблеми, пов’язаної з паразитними перешкодами, необхідно мати на увазі, що наведені вище напруги та струми підпорядковуються загальним законам електротехніки без будь-яких відхилень.

Усунення паразитарних інвазій в основному зводиться до виявлення цих трьох елементів, що часто є дуже складним завданням. Це ускладнюється ще й тим, що в багатьох випадках паразитичне керівництво надходить з кількох джерел і кількох паразитних комунікаційних ланцюгів. За цих умов виявлення слабкіших джерел і з’єднань можливе лише після видалення сильніших джерел і напрямних з’єднань.

У будь-якому електронному пристрої або електричному пристрої, поряд з провідниками струму (проводами, провідниками друкованих плат), передбаченими його ланцюгами, є численні бічні шляхи, по яких поширюються електричні сигнали, в тому числі небезпечні сигнали акустико-електричних перетворювачів. Ці шляхи створюються в результаті паразитних зв'язків і втручання. Основною причиною є поля, створювані електричними зарядами і струмами в ланцюгах електронних носіїв і пристроїв.

Постійні електричні заряди і електричний струм в елементах і ланцюгах радіоприймачів і електроприладів створюють відповідні електричні та магнітні поля, а заряди і струм змінної частоти - електромагнітні поля. Поля поширюються в просторі і впливають на елементи та схеми інших середовищ і технічних систем. Крім того, для роботи інструментів і систем необхідно передбачити гальванічне з'єднання їх елементів. Через гальванічні з'єднання існують додаткові шляхи для поширення сигналів від одних вузлів і блоків по колах від інших. В результаті впливу бічних полів і впливу через провідники і опори сигналів одних вузлів і

блоків на сигнали інших блоків і вузлів виникають паразитні та керовані зв'язки як всередині електронних середовищ, так і між суміжними носіями. Ці з’єднання та напрямні погіршують роботу компонентів, агрегатів та інструментів загалом. Тому при проектуванні електронних носіїв рівні цих паразитних зв’язків і перешкод знижуються до прийнятних значень. Чим вищі вимоги до характеристик медіа, тим більше зусиль і, як наслідок, витрати на нейтралізацію паразитних зв’язків і перешкод. Більшість високої ціни на високоточні вимірювальні прилади припадає на заходи щодо зменшення паразитних зв'язків і перешкод.

Паразитарні з'єднання та наведення характерні для будь-якого електронного середовища та кабелів, які з'єднують їх кабелі. Тому будь-який електронний пристрій чи електричний пристрій слід розглядати як потенційне джерело загрози інформаційної безпеки з точки зору інформаційної безпеки.

Паразитні зв'язки

Розрізняють три види паразитних зв'язків:

- ємкісні;
- індуктивні;
- гальванічні.

Паразитні ємнісні зв'язки

Ємнісний зв'язок утворюється в результаті впливу електричного поля, індуктивний - впливу магнітного поля, гальванічний зв'язок - через загальний активний опір.

Паразитні ємнісні зв'язку обумовлені електричною ємністю, що утворюється між елементами, деталями і провідниками схем, які несуть потенціал сигналу.

Так як опір ємності, що створює паразитне ємнісний зв'язок, падає з ростом частоти ($Xc = 1/\omega C$), енергія що проходить через неї з підвищенням частоти збільшується. Тому паразитний ємнісний зв'язок може привести до самозбудження підсилювача на частотах, що перевищують його вищу робочу частоту.

Якщо ОТЗС і ДТЗС розташовуються поруч, то, внаслідок наявності ємнісного паразитного зв'язку, можлива передача інформації, що захищається від ОТЗС до ДТЗС.

Для визначення величини такої наводки треба знати власну ємність радіоелектронного засобу або електричного приладу, яку в загальному випадку можна отримати тільки експериментальним шляхом.

Модель ємнісного паразитного зв'язку представлена на рис. 1.12

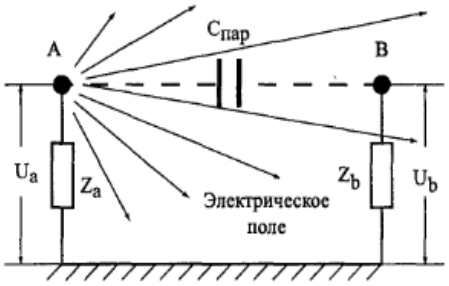

Рис. 1.12. Паразитний ємнісний зв'язок

На цьому рисунку ***Ua*** - потенціал заряду точки ***A*** відносно корпусу, що створює електричне поле. В результаті впливу цього поля в точці ***B*** виникає заряд протилежного знаку. Величина потенціалу заряду (наведеної напруги) ***Ub*** точки ***B*** відносно корпусу визначається співвідношенням ємнісного опору ***Cn***, і опорів ***Zb***:

де $Z = 1/j\omega C$ - ємнісний опір між точками ***A*** і ***B***, ω - кругова частота зміни потенціалу заряду точки ***A***. Ємність ***Cn*** є паразитною і створює ємнісний паразитний зв'язок між точками ***A*** і ***B***.

Паразитні індуктивні зв'язки

Паразитні індуктивні з'єднання обумовлені наявністю взаємної індукції між провідниками частин ланцюга, переважно між трансформаторами.

Паразитний індуктивний зворотний зв'язок, наприклад між вхідним і вихідним трансформаторами, може викликати самозбудження в області робочих частот і гармонік.

Для підсилювачів з низькою вхідною напругою індуктивне з'єднання вхідного трансформатора з джерелами змінних магнітних полів (силовими трансформаторами) є дуже небезпечним. При розташуванні такого джерела на відстані кількох десятків сантиметрів від вхідного трансформатора ЕРС, що

подається на вторинну обмотку трансформатора середнього розміру, може досягати кількох мілівольт, що в сотні разів перевищує допустиме значення.

Паразитний індуктивний зв'язок послаблюється при зменшенні розмірів трансформаторів.

Паразитний індуктивний зв'язок ілюструється рис. 1.13.

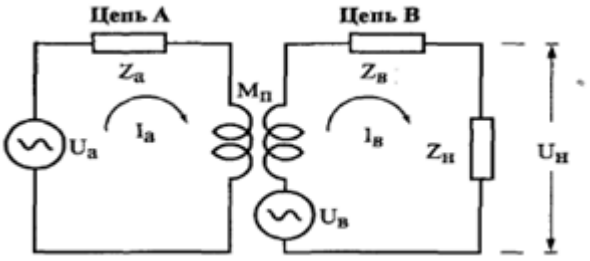

Рис. 1.13. Паразитний індуктивний зв'язок

Змінний струм, що протікає по ланцюгу А, створює магнітне поле, силові лінії якого досягають провідників другого ланцюга В і наводять в ній ЕРС

Взаємна індуктивність замкнутих ланцюгів залежить від розташування та взаємної конфігурації провідників. Тим більше, що більша частина магнітного поля струму в одному колі проникає через провідники іншого кола.

Гальванічні паразитні зв'язки

Гальванічним паразитним зв'язком ще називають зв'язком через загальний опір, що входить до складу декількох ланцюгів. Такими поширеними опорами можуть бути опори з'єднувальних кабелів і пристроїв живлення та управління. Наприклад, компоненти та блоки комп’ютера, що обробляють інформацію, підключені до напруги живлення +5 В. Щоб встановити тригери «0» дискретних пристроїв на відповідні входи, одночасно подається відповідний

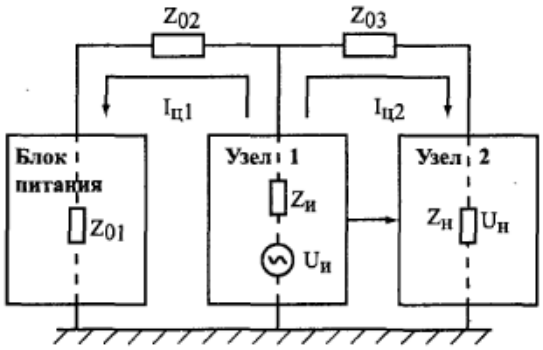

Рис.1.14. Модель гальванічного паразитного зв'язку

керуючий сигнал. На рис. 1.14 показана спрощена схема, що ілюструє походження гальванічного зв'язку.

Відповідно до нього до блоку живлення через загальні опору Z01, Z02 і Z03 підключені вузол 1 і вузол 2 радіоелектронного засобу. Сигнал напругою Ui 1-го вузла створює струми Iц1 і Iц2 в результаті яких на еквівалентному опорі Zн 2-го вузла виникає напруга наводки Uh. Відношення $\beta = U_н / U_i$ називається коефіцієнтом паразитного гальванічного зв'язку.

Випадкові антени

Якщо бічні поля та електричні струми є носіями захищеної інформації, то паразитне наведення та з’єднання можуть викликати витік інформації.

Тому паразитні зв’язки та орієнтація є вторинними фізичними процесами та явищами, які можуть призвести до витоку захищеної інформації. Можливість витоку інформації через паразитні проводи та з’єднання залежить від багатьох факторів, включаючи конфігурацію, розмір і взаємне розташування передавальних і приймаючих провідних елементів носія. На відміну від передбачених для зв'язку функціональних антен, конструкція та характеристики яких визначаються при створенні радіопередавальної та приймальної апаратури, ці елементи можна назвати випадковими антенами. Довільні антени можуть бути монтажними проводами, патч-кордами, друкованими платами, радіокомпонентами, металевими корпусами та іншими компонентами. Параметри випадкових антен значно гірші за функціональні. Однак через невеликі відстані між передачею та прийомом випадкових антен (на електронному пристрої чи в приміщенні) вони становлять загрозу витоку інформації.

Випадкові антени мають складну і часто апріорно невизначену конфігурацію, дуже важко точно розрахувати значення їх електричних параметрів, які збігаються з виміряними. Тому справжню випадкову антену замінюють її моделі у вигляді дротяної антени: шматок дроту (вібратора) і каркас.

Випадкові антени можуть бути зосередженими і розподіленими.

Концентрована випадкова антена є компактним технічним пристроєм (наприклад, телефоном, гучномовцем мережі мовлення, датчиком пожежної сигналізації тощо), підключеним до лінії за межами контрольованої зони.

До розподілених випадкових антен належать випадкові антени з розподіленими параметрами: кабелі, дроти, металеві труби та інші струмопровідні комунікації, що виходять за межі контрольованої зони.

Рівень сигналів, що наводяться в них в значній мірі залежить не тільки від потужності випромінюваних сигналів, але і відстані від ліній ТЗПІ до ліній ДТЗС або сторонніх провідників, а також довжини їх спільного пробігу.

Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації, як наведено на рис 1.15.

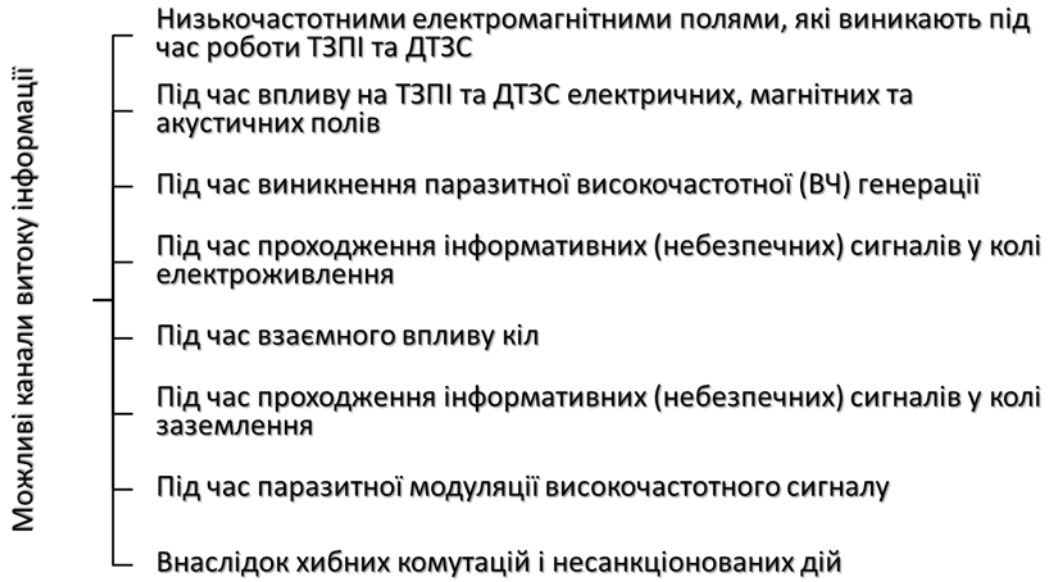

Рис 1.15. Можливі сигнали утворення каналів витоку інформації.

Зони небезпечних сигналів

Простір навколо ТЗОІ, на межі і за межами якого рівень напруги наведеного від ТЗОІ інформативного сигналу в зосереджених антенах не перевищує допустимого (нормованого) значення ($\boldsymbol{U} = \boldsymbol{U}_{\text{н}}$), називається **небезпечною зоною 1** ($r1$), а в розподілених антенах – **небезпечною зоною 1'** ($r1'$).

Розмір зони $r1$ ($r1'$) залежить не лише від рівня ПЕМВ ТЗОІ, але і від довжини випадкової антени (від приміщення, в якому встановлене ТЗОІ до місця можливого підключення до неї засобів розвідки).

Зони $r1$ ($r1'$) для кожного ТЗОІ визначаються інструментально-розрахунковим методом без урахування затухання сигналів у випадкових антенах при проведенні спеціальних досліджень технічних засобів на ПЕМВН і вказується в приписі на їх експлуатацію або сертифікаті відповідності, а з урахуванням реального затухання сигналів у випадкових антенах – при атестації об'єкту інформатизації.

Електричний канал витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах

Схема електричного каналу витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах приведена на рис. 1.16.

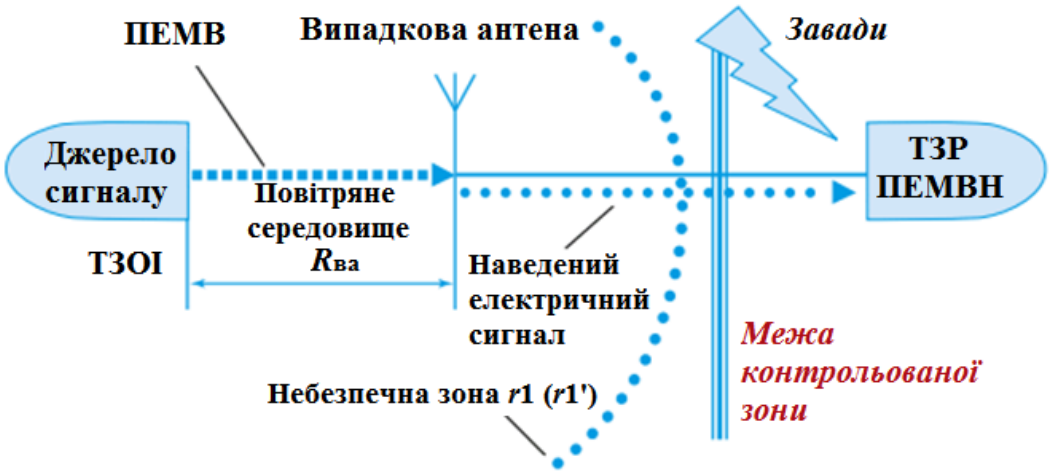

Рис. 1.16 Схема електричного каналу витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах

Умови виникнення електричного каналу витоку інформації

Для виникнення електричного каналу витоку інформації необхідно, щоб:

1) сполучні лінії ДТЗС, лінії електроживлення, сторонні провідники і т.д., що виконують роль випадкових антен, виходили за межі контрольованої зони об'єкту;
2) відстань від ТЗОІ до випадкової зосередженої антени була менш $r1$, а відстань до випадкової розподіленої антени була менш $r1'$;

3) була можливість безпосереднього підключення до випадкової антени за межами контрольованої зони об'єкту засобів розвідки ПЕМВН;
4) за межами контрольованої зони повинна існувати можливість безпосереднього підключення до ліній електроживлення і заземлення ТЗОІ, до сполучних ліній ДТЗС або до сторонніх провідників портативних засобів розвідки ПЕМВН.

Канал побічних електромагнітних випромінювань ОТЗС

Бічний канал електромагнітного випромінювання ОТЗС (PEMV channel of ОТЗС) утворюється шляхом перехоплення приймачами технічної розвідки вторинних електромагнітних полів, які утворюються навколо електронних і провідних елементів (шлейфів) ОТЗС при пропусканні інформаційних сигналів і поширенні цих полів назовні. контрольна зона.

Інформаційними сигналами у даному випадку з електричні струми, що несуть інформацію.

Обробка та передача інформації в ОТЗС здійснюється за допомогою струмів електричної провідності, які являють собою спрямований потік заряджених частинок – електронів. Як відомо з фізики, навколо нерухомих електронів або груп електронів завжди існує електростатичне поле. Якщо цей заряд змусити рухатися, у полі з’являється магнітна складова, яка стає електромагнітною. Електромагнітне поле поширюється в просторі.

Навколо ОТЗС, як системи електронних елементів та провідників (шлейфів), в яких відповідно з принципом основної дії ОТЗС циркулюють електричні струми, що несуть інформацію, завжди присутні поля випромінювання. Оскільки ці випромінювання небажані та носять паразитний (побічний) характер, їх називають побічними електромагнітними випромінюваннями (ПЕМВ). Побічні електромагнітні випромінювання поширюються у вільному просторі і можуть бути перехоплені за межами КЗ приймачами засобів технічної розвідки противника, таким чином утворюється канал ПЕМВ ОТЗС (Рис. 1.17).

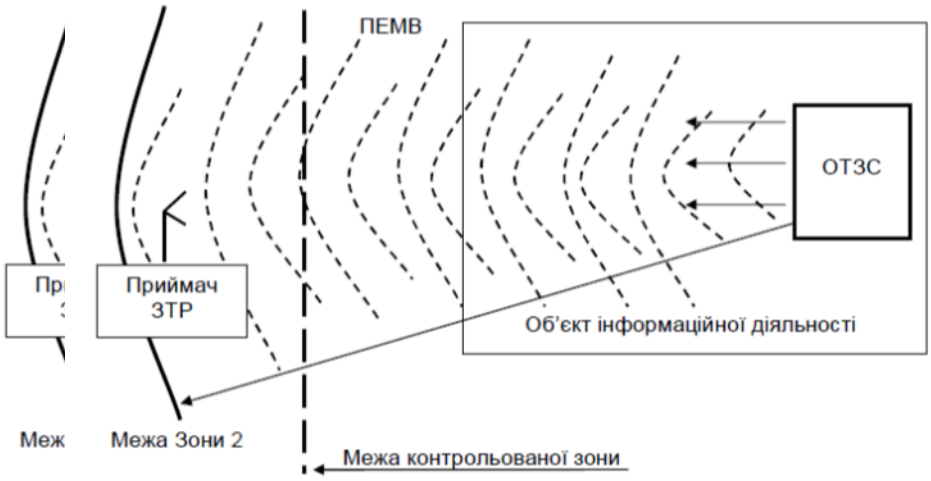

Рис. 1.17. Схематична можливість витоку інформації.

З фізики також відомо, що при поширенні електромагнітного поля воно загасає. Тому є така відстань від джерела випромінювання – ОТЗС, на якій поле випромінювання згасне до рівня, при якому стає неможливим його приймання (виявлення та вимірювання його параметрів). При цьому небезпечний сигнал, що переноситься цим полем, буде, практично, зруйнованим звичайними завадами та шумами. Як вже відмічалося раніше, простір, за межами якого відношення сигналу до завади не перевершує допустиму норму, з Зоною 2 даного ОТЗС.

Розташування приймачів ЗТР противника за межами Зони 2 не дасть можливості перехоплення інформації.

Запобігання витоку інформації каналом ПЕМВ ОТЗС (унеможливлення створення такого ТКВІ) досягається шляхом:

- створення КЗ не меншої за Зону 2 та організація режиму доступу до КЗ та на ОІД;
- екранування ОТЗС або локального екранування електронних елементів та провідників (шлейфів) ОТЗС, зменшення довжини провідників (шлейфів) ОТЗС;
- просторового електромагнітного замулення на об'єкті ЕОТ.

Канал побічних електромагнітних випромінювань ДТЗС

Канал побічних електромагнітних випромінювань ДТЗС, як різновид Каналів , утворюється шляхом перехоплення приймачами засобів технічної розвідки за межами КЗ небезпечних сигналів у вигляді побічних електромагнітних полів ОТЗС, які перевипромінюються допоміжними технічними засобами та системами, а також сторонніми провідниками (рис. 1.18).

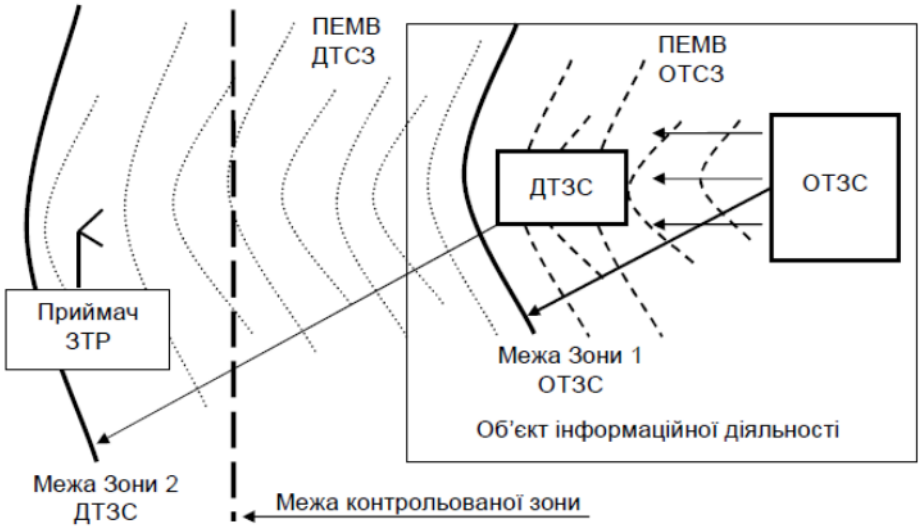

Рис. 1.18. Канал побічних електромагнітних випромінювань ДТЗС.

Допоміжні технічні засоби та системи, а також сторонні провідники, якщо вони знаходяться в зоні 1 ОТЗС або мають спільні пробіги з лініями, якими поширюються небезпечні сигнали (в тому числі сигнали побічних електромагнітних наведень) ОТЗС, з випадковими антенами і можуть привести до витоку інформації небезпечними сигналами, наведеними на них побічними електромагнітними випромінюваннями основних технічних засобів та систем.

Запобігання витоку інформації Каналом побічних електромагнітних випромінювань ДТЗС (унеможливлення створ1ення такого ТКВІ) досягається шляхом:

- • створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗ на ОІД;
- • розташування ДТЗС та сторонніх провідників поза Зоною 1 ОТЗС;
- • екранування ОТЗС;
- • екранування ДТЗС;

- • просторового електромагнітного зашумлення на об’єкті ЕОТ.

Канал “паразитної” модуляції сигналів ВЧ генераторів

Канал “паразитної” модуляції сигналів ВЧ генераторів, як різновид Каналів ПЕМВ, утворюється шляхом модуляції небезпечним сигналом високочастотних сигналів ВЧ генераторів ОТЗС, випромінювання модульованих ВЧ коливань у вільний простір та перехоплення таких коливань радіоприймальними пристроями засобів технічної розвідки за межами КЗ (рис. 1.19).

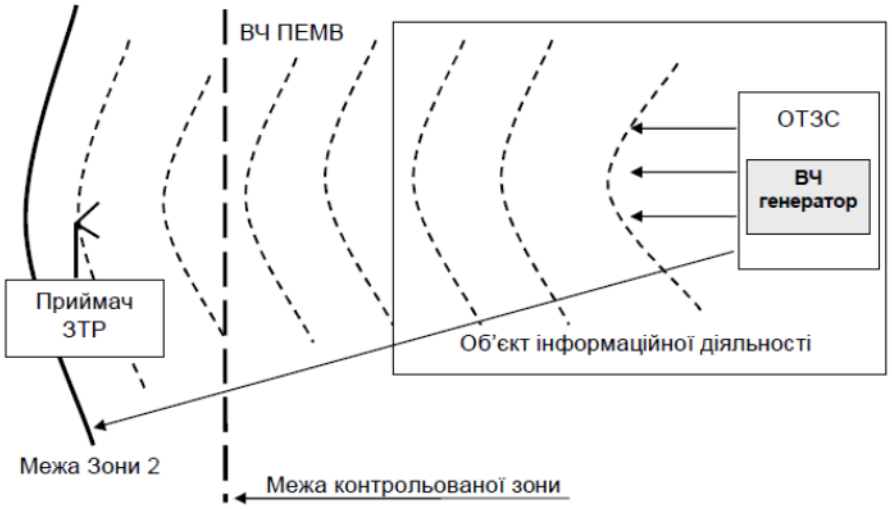

Рис. 1.19. Канал “паразитної” модуляції сигналів ВЧ генераторів.

Основні технічні засоби та системи в своєму складі мають генератори високих частот (ВЧ генератори). Практично всі засоби ЕОТ в своєму складі мають генератори тактових частот, гетеродини та інші ВЧ генератори. Високочастотний сигнал ВЧ генератора модулюється низькочастотними небезпечними сигналами, що циркулюють в ОТЗС, та випромінюється у вигляді електромагнітного поля у вільний простір. Оскільки згасання електромагнітного поля на високих частотах менше ніж на низьких, то поле розповсюджується дальше. А це, в свою чергу, дає можливість перехоплення інформації засобами технічної розвідки за межами 3они 2, розрахованої для сигналу баз модуляції. Слід відмітити, що модуляція розширює спектр частот сигналу, підвищує його потужність і завадостійкість. Тому 3она 2 має розраховуватись з врахуванням модульованого випромінювання на частотах ВЧ генераторів ОТЗС.

Запобігання витоку інформації Каналом “паразитної” модуляції сигналів ВЧ генераторів (унеможливлення створення такого ТКВІ) досягається шляхом:

- створення КЗ не меншої за 3ону 2, яка розрахована з врахуванням паразитної модуляції небезпечним сигналом коливань ВЧ генераторів ОТЗС, та організації режиму доступу до КЗ та на ОІД;
- екранування ОТЗС або унеможливлення “паразитної” модуляції сигналів ВЧ генераторів ОТЗС (локальне екранування ВЧ генераторів, оцінювання випромінювань та блокування роботи ОТЗС у разі виявлення “паразитної” модуляції тощо);
- просторового електромагнітного зашумлення на об’єкті ЕОТ.

Основні параметри витоку інформації каналами ПЕМВН:

- напруженість електричного поля інформативного (небезпечного) сигналу;
- напруженість магнітного поля інформативного (небезпечного) сигналу;
- величина звукового тиску;
- величина напруги інформативного (небезпечного) сигналу;
- величина напруги наведеного інформативного (небезпечного) сигналу;
- величина напруги шумів (завад);
- величина струму інформативного (небезпечного) сигналу;
- величина чутливості до впливу магнітних полів для точкового джерела;
- величина чутливості апаратури до впливу електричних полів (власна ємкість апаратури);
- величина чутливості до впливу акустичних полів;
- відношення "інформативний сигнал/шум";
- відношення напруги небезпечного сигналу до напруги шумів (завад) у діапазоні частот інформативного сигналу.

Зазначені параметри визначаються і розраховуються за результатами вимірювань у заданих точках.

Гранично допустимі значення основних параметрів є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахункових (**виміряних**) значень основних параметрів до гранично допустимих (**нормованих**) значень **визначають необхідні умови захисту інформації**.

1.4. Перехоплення інформації

Для перехоплення інформації правопорушники використовують засоби технічної розвідки. Інші зацікавлені особи (юридичні особи, групи фізичних осіб, фізичні особи) використовують спеціальні технічні засоби (СТЗ) для перехоплення інформації, адаптованої або модифікованої для негласного одержання інформації..

Рис. 1.20 Способи перехоплення інформації в ТЗОІ

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

Типовий комплекс розвідки ПЕМВ включає спеціальний приймальний пристрій, ПЕОМ (або монітор), спеціальне програмне забезпечення і широкодіапазонну спрямовану антену (рис. 1.29).

Рис. 1.21 Комплекс перехоплення ПЕМВ ТЗОІ

(включає спеціальне приймальне облаштування PKI 2715 (дальність перехоплення ПЕМВ від 10 до 50 м) і широкосмугова спрямована антена R&SHЬ 007 (діапазон частот від 80 МГц до 1,3 ГГц, коефіцієнт посилення 5 – 7 дБ)

Перехоплення побічних електромагнітних випромінювань ТЗОІ технічними засобами розвідки показано на рис. 1.22.

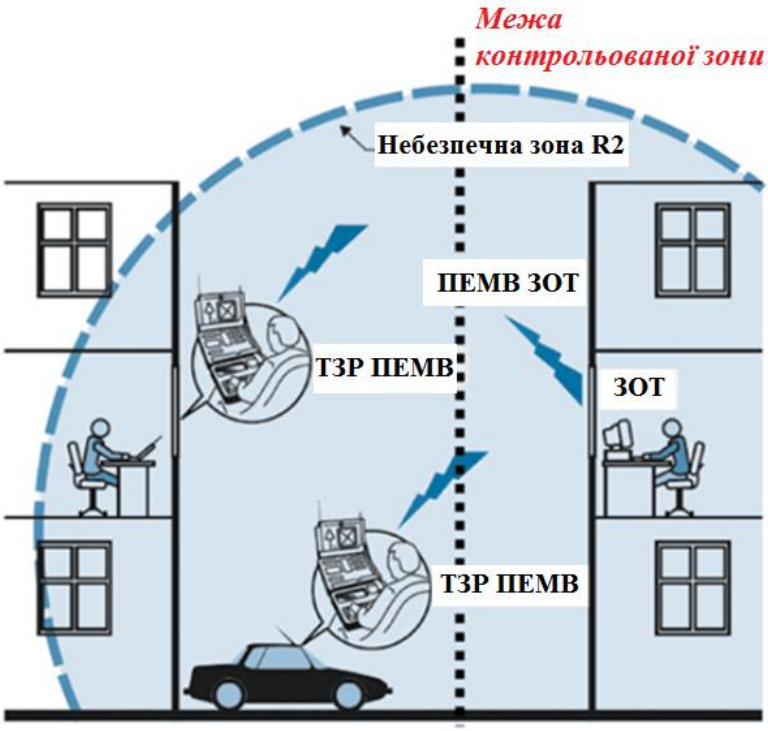

Рис. 1.22 Приклади перехоплення ПЕМВ технічними засобами розвідки

Перехоплення інформативних сигналів з електричного каналу витоку інформації

Приклад перехоплення наведень інформативних сигналів з інженерних комунікацій технічним засобом розвідки ПЕМВН показан на рис. 1.23.

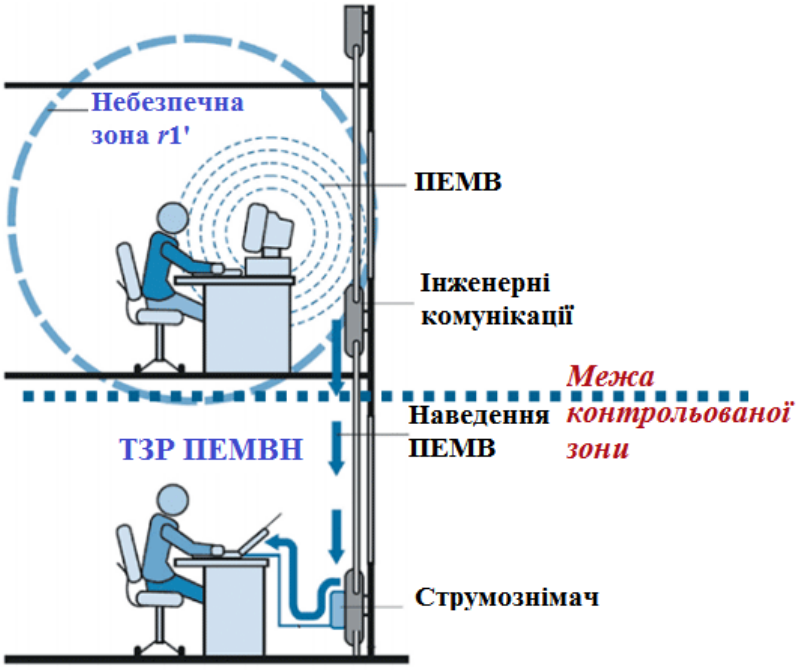

Рис. 1.23 Перехоплення наведень інформативних сигналів з інженерних комунікацій

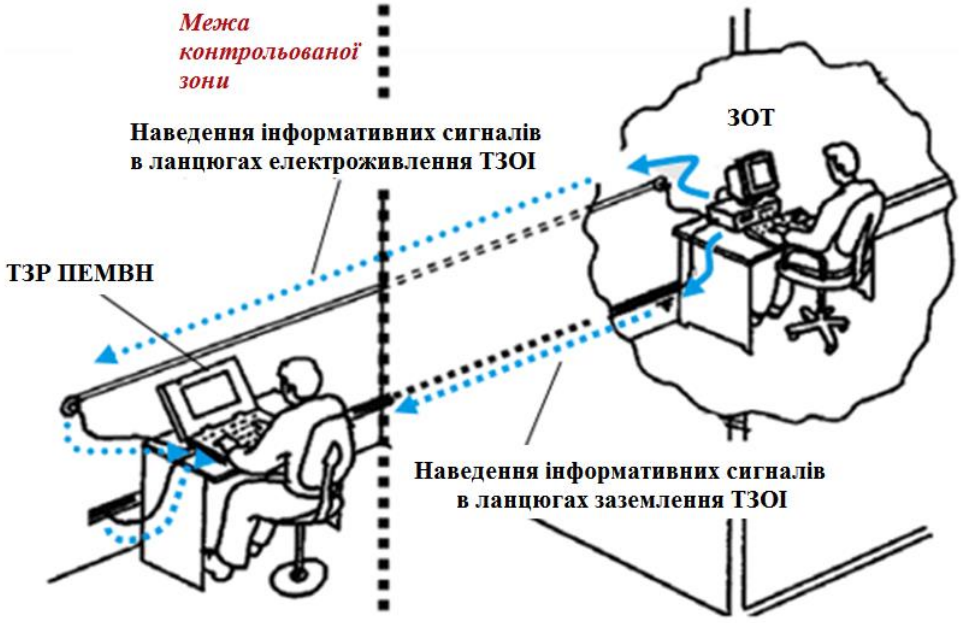

Рис. 1.24 Приклад перехоплення інформативних сигналів при підключенні засобів розвідки ПЕМВН до ліній електроживлення і заземлення ТЗОІ

РОЗДІЛ°2. ДОСЛІДЖЕННЯ ПЕМВН

2.1. Загальна структура досліджень ПЕМВ

ПЕМВ - одна із головних причин існування проблеми електромагнітної сумісності технічних засобів. Тому виявлення і інструментальний контроль ПЕМВ завжди входили в число важливих завдань органів радіоконтролю і осіб, пов'язаних з розробкою і експлуатацією цих засобів.

У випадках, коли для обробки інформації з обмеженим доступом використовуються технічні засоби, найбільш актуальними є теми, що стосуються інформативного PEMV та наведення інформаційних сигналів у провідних колах. Під ними розуміють PEMV і орієнтацію, які містять інформацію про оброблювану інформацію і можуть бути перехоплені зацікавленими сторонами.

Порівняльна простота і скритність добування інформації за рахунок перехоплення інформативних ПЕМВ і наведень, постійне вдосконалення техніки перехоплення і алгоритмів виділення інформативних сигналів змушує фахівців проводити спеціальні дослідження технічних засобів для виявлення і інструментального контролю інформативних ПЕМВ і наведень. Загальна структура досліджень ПЕМВН приведена на рисунку 2.1.

2.2. Механізм виникнення ПЕМВН засобів цифрової електронної техніки.

Низький рівень паразитних перешкод не забезпечується схемою і конструкцією передачі сигналу від одного елемента радіостанції до іншого. Такі перешкоди виникають через наявність паразитного зв'язку між цими елементами, з'єднання електричних ланцюгів.

Високий ступінь стандартизації методу вимірювання рівня електромагнітного випромінювання при вирішенні задач оцінки електромагнітної сумісності дозволяє (з урахуванням деяких характеристик) використовувати його при вирішенні задач захисту інформації від витоку через канали PAMVN.

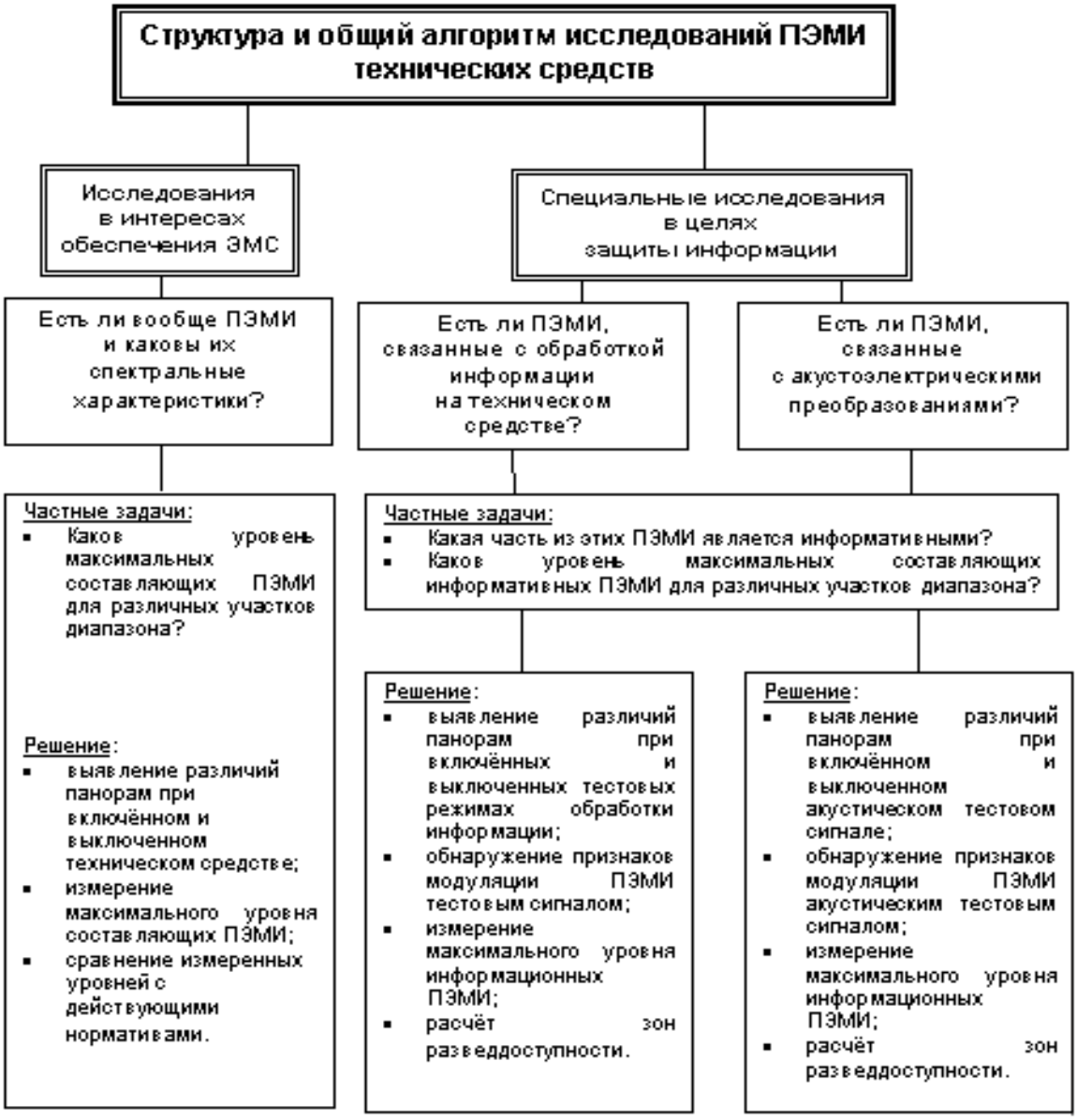

Рис. 2.1. Загальна структура досліджень ПЕМВН

Т.ч. дослідження питань паразитних зв'язків і наводок небезпечних сигналів в **якісному** плані можна звести до вирішення завдань оцінки електромагнітної сумісності.

Види і джерела електромагнітних завад

Залежно від середовища поширення електромагнітні завади можуть розділятися на індуктивні і кондуктивні.

Кондуктивні завади являють собою струми, що течуть по дротовим конструкціям і землі, і вимірюються в діапазоні частот до 30 МГц.

Індуктивними називають завади, що поширюються в вигляді електромагнітних полів в непровідних середовищах.

Кондуктивні завади

Кондуктивні завади прийнято ділити на синфазні (струми частотою **вище 5 МГц**) і диференціальні (струми частотою **нижче 5 МГц**).

Диференціальні завади виникають через диференційні струми в парі дротів: струм залишає джерело по одній лінії і повертається по зворотній лінії диференціальної пари (рис. 2.2). Диференційні струми протікають між імпульсним джерелом живлення і його джерелом або навантаженням через висновки живлення. На земляній шині диференціальні струми відсутні.

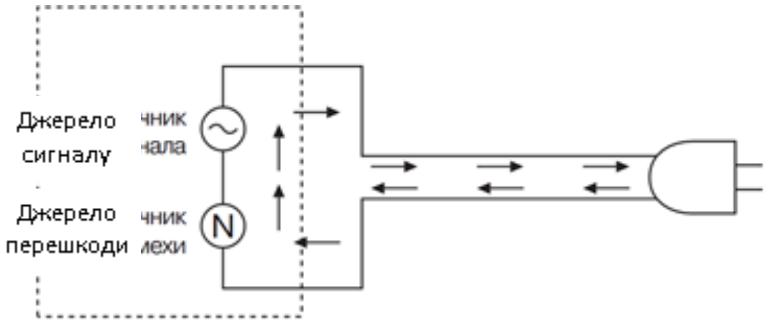

Рис. 2.2. Диференційна завада

Синфазні завади викликаються синфазними струмами. Струм синфазної завади протікає по всіх лініях в одному напрямку, потрапляє через паразитні ланцюги на системну земляну шину і повертається назад до джерела по землі (рис. 2.3). У багатьох випадках **джерелами синфазних завад є паразитні ємності** в схемі. Крім того, синфазні струми можуть передаватися через ємність між корпусом і землею.

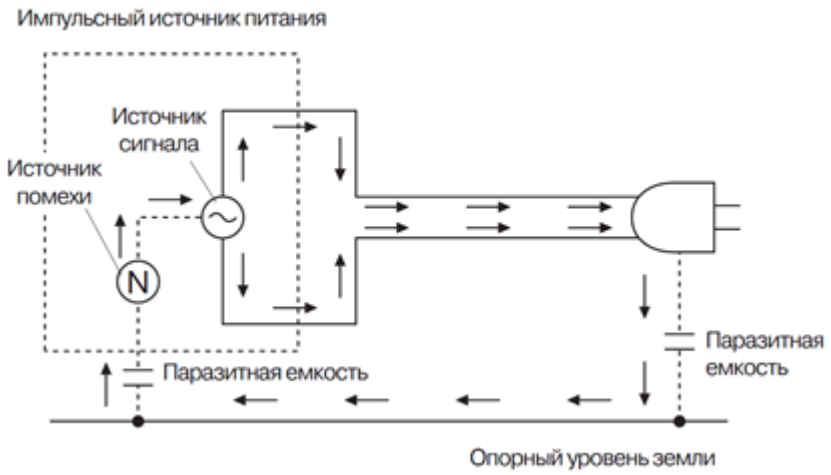

Рис. 2.3. Синфазна завада

Коли паразитна ємність замикає диференційний або синфазних контур, струм стає функцією частоти. У міру зростання частоти або збільшення

довжини дроту ємнісний опір зменшується. На низьких частотах опір ємності дорівнює $Xc = 1/j\omega C$. Відповідно, повний опір контуру буде великим, а струм зміщення малим. Наприклад, при частоті 10 кГц опір ємністю 1000 пФ становить $Xc=15$**923 Ом**, а при частоті 1 ГГц – всього 159 мОм.

При тому, чім більший струм, тим сильніше радіочастотне випромінювання.

Хоча **синфазний струм, як правило, менший диференційного**, площа його контуру настільки більше, що він має більше значення, ніж диференційний. Оскільки синфазний струм може виникати одночасно в декількох ланцюгах і на шині землі, з ним важко боротися. При проектуванні схеми необхідно вживати заходи для попередження виникнення синфазних струмів.

Індуктивні завади

Індуктивні перешкоди виникають, коли джерело і приймач знаходяться на невеликій відстані один від одного. Індуктивне сполучення може бути викликано електричною або магнітною індукцією. Електрична індукція обумовлена ємнісним зв’язком, а магнітна – індуктивною. Ємнісне з’єднання виникає, коли між двома сусідніми провідниками виникає змінне електричне поле, що викликає зміну напруги в сусідньому провіднику. Магнітне з’єднання виникає, коли між двома паралельними провідниками виникає змінне магнітне поле, викликаючи зміну струму вздовж випромінюваного поля, що приймає провідник. Наявність магнітного зв’язку між провідниками виявляється в тому, що при кожній зміні струму в одному з провідників з’являється ЕРС індукції в іншому.

Способи зменшення кондуктивних завад

Щоб ефективно зменшити негативний вплив провідних перешкод, необхідно окремо розглядати диференціальний і синфазний шум, оскільки методи усунення несправностей для кожного типу шумів різні. Реалізовані рішення для диференціальних шумів не виключають синфазних шумів у схемі і навпаки.

Диференціальні перешкоди зазвичай пригнічують шляхом включення байпасного конденсатора безпосередньо між живильною і зворотною лініями імпульсного джерела живлення. Лінії електропередачі, які потребують фільтрації,

можуть бути розташовані на вході або виході імпульсного джерела живлення. Для найкращої ефективності байпасні конденсатори на цих лініях повинні розташовуватися близько до виходів джерела перешкод. Розташування байпасного конденсатора дуже важливо для ефективного ослаблення диференціальних струмів на високих частотах. Для ослаблення диференціальних струмів на нижчих частотах поблизу основної частоти перемикання перешкоди може знадобитися використання шунтирующего конденсатора значно більшої ємності, що не дозволяє використовувати керамічний конденсатор.

Керамічні конденсатори ємністю до 22 мкФ можуть підійти для фільтрації диференціальних завад на низьковольтних виходах імпульсних джерел живлення, але їх може бути недостатньо для застосування на входах імпульсних джерел живлення, де можуть спостерігатися 100 В викиди напруги. У таких випадках використовуються електролітичні конденсатори зважаючи на їх високу ємність і робочу напругу.

Диференціальний вхідний фільтр зазвичай складається з комбінації електролітичного і керамічного конденсатора, що дозволяє ефективно послаблювати диференційний струм як на нижчій основній частоті перемикання, так і на частотах вищих гармонік. Додаткового придушення диференційних струмів можна досягти за допомогою, включеної послідовно з мережевим входом котушки індуктивності, утворюючи спільно з шунтувальним конденсатором однокаскадний диференційний LC-фільтр нижніх частот.

Синфазні провідні перешкоди ефективно пригнічуються шляхом включення байпасного конденсатора між кожною лінією живлення імпульсного джерела живлення та землею. Ці лінії електропередачі можуть бути на вході та/або виході імпульсного джерела живлення. Додаткове придушення синфазних струмів може бути досягнуто за допомогою пари з’єднаних дроселів індуктивності, з’єднаних послідовно з кожним мережевим входом. Високий імпеданс індуктивностей, підключених до фазних струмів, забезпечує передачу цих струмів через байпасний конденсатор.

Методи зменшення випромінюваних завад

Випромінювані завади можна придушити шляхом зменшення високочастотного імпедансу і скорочення площі антенної петлі, що забезпечується шляхом мінімізації площі замкнутої антенної петлі, яка утворюється силовою лінією і її зворотним каналом (рис. 2.4). Роблячи ширину друкованої плати якомога більше і прокладаючи її паралельно зворотному каналу можна значно знизити значення імпедансу провідника даної плати. Зменшення площі між силовий лінією і її зворотним каналом забезпечує зниження її імпедансу. В межах друкованої плати ця область може бути скорочена шляхом розміщення силової та зворотної лінії - однієї під інший - на сусідніх шарах плати. Розташування земляного шару, розташованого на відкритих поверхнях друкованої плати (особливо якщо плата розташована прямо під джерелом генерації завад) значно зменшує випромінювані електромагнітні завади.

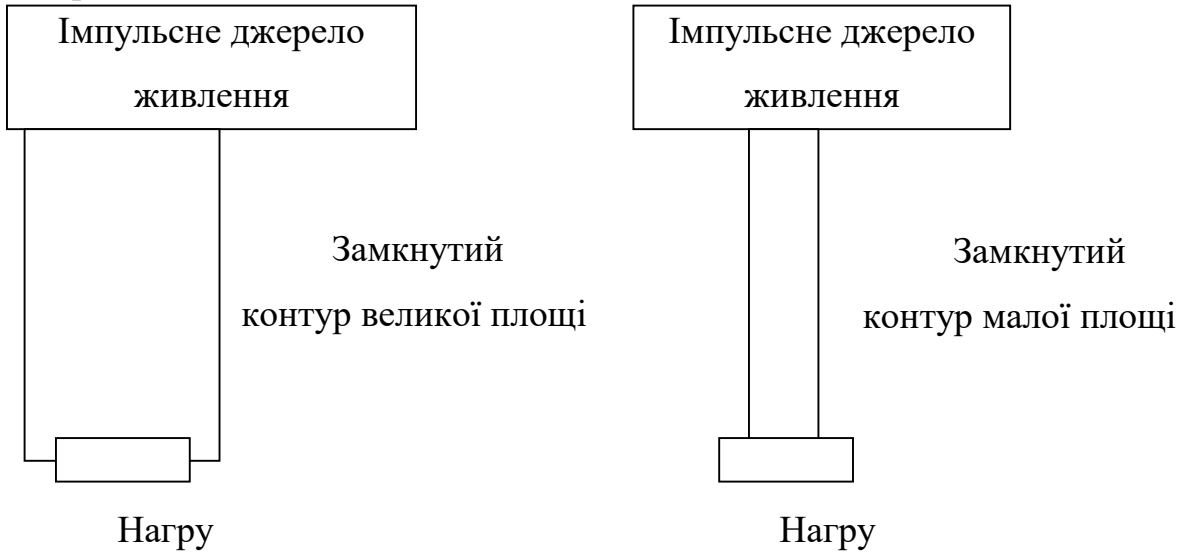

Рис. 2.4. Зниження випромінюваних завад за рахунок зменшення площі петлевої антени

Також, використання металевих екранів (каналізуючи випромінювання), сприяє додатковому зменшенню випромінюваних завад. Це досягається шляхом розміщення джерела генерації завад всередині заземленого провідного корпусу. Інтерфейс із зовнішнім середовищем здійснюється через прохідні фільтри. Більш того, необхідно розмістити синфазні шунтуючі конденсатори між провідним корпусом і земляною шиною.

Отже, ПЕМВ, що генеруються електронними пристроями, обумовлені протіканням диференціальних і синфазних струмів.

У напівпровідникових приладах випромінюване електромагнітне поле формується синхронним протіканням диференціальних струмів у ланцюгах двох типів.

Один тип схем складається з провідників друкованої плати або шин, які живлять напівпровідникові прилади. Площа ланцюга системи живлення приблизно дорівнює добутку відстані між шинами на відстань найближчої логічної схеми до її розв'язувального конденсатора.

Інший тип схеми формується шляхом передачі логічних сигналів від одного пристрою до іншого за допомогою шини живлення як зворотного дроту. Провідники даних разом з силовими шинами утворюють динамічно функціонуючі схеми, що з'єднують передавальні та приймальні пристрої.

Випромінювання, викликане синфазними струмами, викликається падінням напруги на пристрої, що створює синфазну напругу відносно землі. Як правило, в цифровій електронній апаратурі виконується синхронна робота логічних пристроїв. В результаті, коли кожен логічний пристрій перемикається, концентрація енергії зосереджується на компоненти вузьких імпульсів, які збігаються за часом, перекриваються, і загальний рівень випромінювання може бути вищим, ніж будь-який з окремих пристроїв може створити.

У багатьох випадках основними джерелами випромінювання є кабелі, по яких інформація передається в цифровому вигляді. Ці кабелі можна розмістити всередині пристрою або з’єднати один з одним.

Використання заземлювальних перемичок для кабелів або дротяних оплеток, які характеризуються високою індуктивністю і активним опором високочастотних перешкод і не забезпечують хорошого заземлення екрана, призводить до того, що кабель починає виконувати роль передавальної антени.

2.3. Оцінка рівня ПЕМВН.

Оцінка рівня ПЕМВ засобів цифрової електронної техніки може проводитися з точки зору відповідності цих рівнів наступним нормам і вимогам:

• санітарно-гігієнічні норми;

• норми електромагнітної сумісності (ЕМС);

• норми і вимоги по захисту інформації від витоку через ПЕМВ.

Залежно від того, відповідність яким нормам потрібно встановити, використовуються ті чи інші прилади, методи та методики проведення вимірювань.

Слід зауважити, що норми на рівні електромагнітних випромінювань з точки зору ЕМС істотно (на кілька порядків) суворіше санітарно-гігієнічних норм. Очевидно, що норми, методики та прилади, які використовуються в системі забезпечення безпеки життєдіяльності, не можуть бути використані при вирішенні задач захисту інформації.

Оцінка рівня ПЕМВ з точки зору електромагнітної сумісності

Рівні ПЕМВ цифрової електронної техніки з точки зору електромагнітної сумісності (ЕМС) регламентовані цілим рядом міжнародних та вітчизняних стандартів. Так, наприклад, Публікація № 22 CISPR (Спеціальний міжнародний комітет з радіозавад) встановлює такі норми напруженості поля радіозавад від устаткування інформаційної техніки:

Полоса частот, МГц	Квазипиковые нормы, дБ·мкВ/м (мкВ/м)
30-230	30 (31,6)
230-1000	37 (70,8)

- Рівні напруженості поля випромінюваних завад нормуються на відстані 10 або 30 м від джерела завад в залежності від того, де буде експлуатуватися обладнання (в житлових приміщеннях або в умовах промислових підприємств).

Очевидно, що наведені допустимі рівні випромінювання достатні для перехоплення електромагнітних випромінювань на значній відстані. Крім того, в діапазоні частот 0,15-30 МГц нормуються тільки рівні напруги завад на

мережевих зажимах обладнання і не нормується напруженість поля радіозавад. Не буде зайвим згадати, що дані норми при серійному випуску виконуються з якоюсь ймовірністю.

Таким чином, відповідність ПЕМВ засобів цифрової електронної техніки нормам на ЕМС не може бути гарантією збереження конфіденційності інформації, що обробляється за допомогою цих засобів.

Однак висока ступінь стандартизації методик і апаратури вимірювання рівня електромагнітних випромінювань при вирішенні задач оцінки електромагнітної сумісності уможливлює (з урахуванням деяких особливостей) використання їх і при вирішенні задач захисту інформації. Докладно зупинятися на характеристиках використовуваної вимірювальної апаратури не будемо, наведемо лише деякі з них:

• діапазон робочих частот 9 кГц - 1000 МГц;

• можливість зміни смуги пропускання;

• наявність детекторів квазіпікового, пікового, середнього і середньоквадратичного значень;

• можливість слухового контролю сигналу, що має амплітудну і частотну модуляцію;

• наявність виходу проміжної частоти і виходу на осцилограф;

• наявність комплекта стандартних каліброваних антен.

Приклади приладів, які використовуються на практиці вирішення задач ЕМС, наведені в табл. 1.

Таблица 1

Прибор	Диапазон рабочих частот, МГц	Производитель
SMV-8	26–1000	«Messelektronik», Германия
SMV-11	0,009–30	«Messelektronik», Германия
SMV-41	0,009–1000	«Messelektronik», Германия
«Элмас»	30–1300	ПО «Вектор», Санкт-Петербург
ESH-2	0,009–30	«ROHDE&SCHWARZ», Германия
ESV	20–1000	«ROHDE&SCHWARZ», Германия
ESH-3	0,009–30	«ROHDE&SCHWARZ», Германия
ESVP	20–1300	«ROHDE&SCHWARZ», Германия

Сучасні вимірювальні приймачі («Елмас», ESH-3, ESVP, SMV-41) автоматизовані і оснащені інтерфейсами за стандартом IEEE-488, що надає можливість управління режимами роботи приймача за допомогою зовнішньої ЕОМ, а також передачи виміряних значень на зовнішню ЕОМ для їх обробки.

Крім перерахованих приладів, для виміру побічних електромагнітних випромінювань засобів цифрової електронної техніки можуть бути використані аналізатори спектра в комплекті з вимірювальними антенами.

Сучасні аналізатори спектра (АС) з вбудованими мікропроцесорами дозволяють аналізувати різні параметри сигналів. Є можливість об'єднання АС за допомогою інтерфейсу за стандартом IEEE-488 з іншими вимірювальними приладами і зовнішніми ЕОМ в автоматизовані вимірювальні системи [8].

В процесі обробки можуть виконуватися такі функції:

пошук екстремальних значень сигналу;

відбір сигналів, рівень яких перевищує заданий;

зсув по осі частот для оптимальної реєстрації сигналу.

Вбудований мікропроцесор забезпечує обробку амплітудно-частотних спектрів, а також оптимізацію часу вимірювання і роздільної здатності для розглянутого інтервалу частот. Приклади сучасних аналізаторів спектра наведені в табл. 2.

Таблица 2

Прибор	Диапазон рабочих частот, МГц	Диапазон измерения	Производитель
С4-82	$3 \cdot 10^{-4}$–1500	1 мкВ – 3 В	СНГ
СК4-84	$3 \cdot 10^{-5}$–110	70 нВ – 2,2 В	СНГ
С4-85	$1 \cdot 10^{-4}$–$39{,}6 \cdot 10^{3}$	1 мкВ – 3 В, 10^{-16}–10^{-2} Вт	СНГ
РСК4-86	25–1500	40 нВ –2,8 В, $3 \cdot 10^{-17}$–1 Вт	СНГ
РСК4-87	1000–4000	10^{-12}–0,1 Вт	СНГ
РСК4-90	1000–17440	10^{-12}–0,1 Вт	СНГ
HP8568 B	$1 \cdot 10^{-4}$–1500	10^{-16}–1 Вт	«Hewlett-Packard», США
HP71100 A	$1 \cdot 10^{-4}$–2900	10^{-16}–1 Вт	«Hewlett-Packard», США
HP8566 B	$1 \cdot 10^{-4}$–22000	10^{-16}–1 Вт	«Hewlett-Packard», США
2756 P	$1 \cdot 10^{-2}$–$325 \cdot 10^{3}$	10^{-16}–1 Вт	«Tektronix», США
2380+2383	$1 \cdot 10^{-4}$–4200	10^{-18}–1 Вт	«Marconi Instruments», Великобритания
FSA	$1 \cdot 10^{-4}$–2000	10^{-17}–1 Вт	«ROHDE&SCHWARZ», Германия
FSB	$1 \cdot 10^{-4}$–5000	10^{-17}–1 Вт	«ROHDE&SCHWARZ», Германия

Необхідно відзначити, що аналізатори спектра виробництва СНД мають більш скромні можливості в порівнянні з виробами західних фірм.

Оцінка рівня випромінювань при вирішенні задач захисту інформації

На відміну від завдань ЕМС, де потрібно визначити максимальний рівень випромінювання в заданому діапазоні частот, при вирішенні задач інформаційної безпеки необхідно визначити рівень випромінювання в широкому діапазоні частот, що відповідає інформаційному сигналу. Тому оцінку рівня радіації при вирішенні задач захисту інформації необхідно починати з аналізу технічної документації та вибору електричних ланцюгів, по яких може передаватися конфіденційна інформація.. Необхідно провести аналіз і визначити характеристики небезпечних сигналів:

- використаний код: послідовний, паралельний;
- періодичне повторення сигналу: є, немає;
- часові характеристики сигналу;

• спектральні характеристики сигналу.

Після цього можна приступати безпосередньо до визначення рівнів інформативних ПЕМВ. Тут можуть бути запропоновані наступні методи.

Метод оціночних розрахунків.

Визначаються елементи конструкції обладнання, в яких циркулюють небезпечні сигнали, складаються моделі, проводиться оцінний розрахунок рівня випромінювань. Цей метод найкращим чином може бути реалізований при наявності програмного забезпечення для ЕОМ у вигляді експертної системи, що містить банк моделей випромінювачів.

Метод примусової (штучної) активізації.

Небезпечний ланцюг (програмне або апаратне забезпечення) активується опорним сигналом, який дозволяє ідентифікувати випромінювання, і виміряти рівні PEMV. Описані вище прилади можна використовувати для вимірювань у цьому методі.

Метод еквівалентного приймача.

Синтезується приймач для відновлення інформації, що міститься в ПЕМВ. Після калібрування такий приймач може бути використаний для вимірювання рівнів інформативних випромінювань.

Кожен із запропонованих методів має свої переваги та недоліки. На даний момент найбільш прийнятним методом оцінки інформаційних рівнів PEMV є метод примусової активації.

Аналіз можливості витоку інформації через ПЕМВ.

При проведенні такого аналізу необхідно враховувати такі особливості радіотехнічного каналу витоку інформації із засобів цифрової електронної техніки:

• для відновлення інформації мало знати рівень ПЕМВ, потрібно ще знати їх структуру;

•оскільки інформація в цифрових засобах електронної техніки переноситься послідовностями прямокутних імпульсів, то оптимальним

приймачем для перехоплення ПЕМВ є виявник (важливий сам факт наявності сигналу, а відновити сигнал просто, так як форма його відома);

•не всі ПЕМВ є небезпечними з точки зору реальної витоку інформації. Як правило, найбільший рівень відповідає неінформативним випромінюванням (так, в персональних комп'ютерах найбільший рівень мають випромінювання, породжувані системою синхронізації);

•наявність великої кількості паралельно працюючих електричних ланцюгів призводить до того, що інформативні та неінформативні випромінювання можуть перекриватися за діапазоном (взаємна завада);

•для відновлення інформації смуга пропускання розвідприймача повинна відповідати смузі частот перехоплюваних сигналів. Імпульсний характер інформативних сигналів призводить до різкого збільшення смуги пропускання приймача та, як наслідок, до збільшення рівня власних і наведених шумів;

• періодичне повторення сигналу приводить до збільшення можливої дальності перехвату;

• використання параллельного коду в більшості випадків робить практично неможливим відновлення інформації при перехваті ПЕМВ.

РОЗДІЛ°3. ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ

3.1 Загальні рекомендації з технічного захисту інформації

Роботи із захисту інформації з обмеженим доступом від витоку каналами ПЕМВН складаються з **організаційних**, **підготовчих технічних**, **технічних** заходів і контролю за виконанням заходів технічного захисту інформації (ТЗІ) та за ефективністю цього захисту.

Організаційні і **підготовчі** заходи щодо технічного захисту інформації проводяться одночасно і є **першим** етапом робіт, технічні заходи - **наступним** етапом робіт.

Заходи щодо ТЗІ і контролю за його ефективністю можуть виконуватись організаціями, що мають ліцензію Державної служби України з питань технічного захисту інформації (ДСТЗІ) на право надання послуг у галузі ТЗІ.

3.1.1. Організаційні заходи

На етапі проведення організаційних заходів потрібно:

- визначити перелік відомостей з обмеженим доступом, що підлягають технічному захисту (визначає власник інформації згідно з чинним законодавством України);

- обґрунтувати необхідність розроблення і реалізації захисних заходів з урахуванням матеріальної або іншої шкоди, яка може бути завдана внаслідок можливого порушення цілісності ІзОД чи її витоку технічними каналами;

- установити перелік виділених приміщень, в яких не допускається реалізація загроз та витік інформації з обмеженим доступом;

- визначити перелік технічних засобів, що повинні використовуватися як ОТЗ;

- визначити технічні засоби, застосування яких не обґрунтовано службовою та виробничою необхідністю та які підлягають демонтажу;

- визначити наявність задіяних і незадіяних повітряних, наземних, настінних та закладених у приховану каналізацію кабелів, кіл і проводів, що уходять за межі виділених приміщень;

- визначити системи, що підлягають демонтажу, потребують переобладнання кабельних мереж, кіл живлення, заземлення або установлення в них захисних пристроїв.

За результатами обстеження складається акт довільної форми з переліком виконаних заходів і прикладанням (за необхідністю):

- переліку ОТЗ, розміщених у виділених приміщеннях;

- плану виділених приміщень із зазначенням місць установлення ОТЗ, а також схем прокладання кабелів, проводів, кіл;

- переліку технічних засобів, кабелів, кіл, проводів, що підлягають демонтажу.

Акт підписується виконавцем робіт і затверджується керівником організації (підприємства).

3.1.2 Підготовчі технічні заходи

Підготовчі технічні заходи включають первинні заходи з блокування електроакустичних перетворювачів і ліній зв'язку, що виходять за межі призначених об'єктів.

Блокування ліній зв`язку може виконуватися такими способами:

- відключенням ліній зв`язку ТЗПІ та ДТЗС або встановленням найпростіших схем захисту;

- демонтажем технічних засобів, кабелів, кіл, проводів, що уходять за межі виділених приміщень;

- видаленням за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

Блокування каналів можливого витоку ІзОД у системах міського та відомчого телефонного зв`язку може здійснюватися:

- відключенням дзвінкових (викличних) ліній телефонного апарата;

- установленням у колі телефонного апарата безрозривної розетки для тимчасового відключення;

- установленням найпростіших пристроїв захисту.

Запобігання витоку ІзОД через діючі системи гучномовного диспетчерського та директорського зв`язку здійснюється застосуванням таких захисних заходів:

- установленням у викличних колах вимикачів для розриву кіл;

- установленням на вході гучномовців вимикачів (реле), які дають можливість розривати кола по двох проводах;

- забезпеченням можливості відключення живлення мікрофонних підсилювачів;

- установленням найпростіших пристроїв захисту.

Захист ІзОД від витоку через радіотрансляційну мережу, що виходить за межі виділеного приміщення, може бути забезпечений:

- відключенням гучномовців по двох проводах;

- вмиканням найпростіших пристроїв захисту.

Для послуги сповіщення необхідно призначити такі абонентські пристрої за межами закріпленого приміщення; ланцюги до цих пристроїв повинні підключатися за допомогою окремого кабелю.

Блокування каналів витоку ІзОД через кола вторинних електрогодинників системи електрогодинофікації здійснюється відключенням їх на період проведення закритих заходів.

Запобігання витоку ІзОД через системи пожежної та охоронної сигналізацій здійснюється відключенням датчиків пожежної та охоронної сигналізації на період проведення важливих заходів, що містять ІзОД, або застосуванням датчиків, які не потребують спеціальних заходів захисту.

З метою виключення можливості витоку ІзОД під час роботи незахищених технічними засобами телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури необхідно на період проведення важливих заходів зазначені пристрої відключати від мережі електроживлення по двох проводах.

Блокування витоку ІзОД через системи електронної оргтехніки та кондиціонування може бути забезпечене такими заходами:

- розташуванням зазначених систем усередині контрольованої території без винесення окремих компонентів за її межі;

- електроживленням систем від трансформаторної підстанції, що знаходиться всередині контрольованої території.

При невиконанні зазначених вище умов системи повинні відключатися від мережі електроживлення по двох проводах.

Захист ІзОД від витоку через кола електроосвітлення та електроживлення побутової техніки повинен здійснюватися підключенням зазначених кіл до окремого фідера трансформаторної підстанції, до якого не допускається підключення сторонніх користувачів.

У разі невиконання цієї вимоги електроприлади повинні бути відключені від ланцюгів живлення на період закриття для діяльності.

3.1.3 Технічні заходи

Технічні заходи є основним етапом робіт з технічного захисту ІзОД і полягають у встановленні ОТЗ, забезпеченні ТЗПІ та ДТЗС пристроями ТЗІ.

При виборі, монтажі, заміні технічних засобів слід керуватися паспортами, технічними описами, інструкціями з експлуатації, рекомендаціями з монтажу, монтажу та експлуатації, які додаються до цих засобів.

ОТЗ повинні розміщуватися, по можливості, ближче до центру будинку або в бік найбільшої частини контрольованої території. Складові елементи ОТЗ повинні розміщуватися в одному приміщенні або в суміжних.

Якщо зазначені вимоги невиконувані, слід вжити додаткових заходів захисту:

- установити високочастотні ОТЗ в екрановане приміщення (камеру);

- установити в незахищені канали зв`язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.

- прокласти проводи і кабелі в екранувальних конструкціях;

- зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;

- виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

До засобів технічного захисту відносяться:

- фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;

- пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;

- фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;

- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;

- генератори лінійного зашумлення;

- генератори просторового зашумлення;

- екрановані камери спеціальної розробки.

Для телефонного зв`язку, не призначеного для пересилання ІзОД, рекомендується застосовувати апарати вітчизняного виробництва, сумісні з пристроями захисту. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку компетентних організацій системи ТЗІ про їх сумісність з пристроями захисту.

Вибір методів і способів захисту елементів ТЗПІ та ДТЗС, що мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1 кГц.

Елементи з вхідним опором менше 600 Ом (головки гучномовців, електродвигуни вентиляторів, трансформатори тощо) рекомендується відключати по двох проводах або встановлювати у розрив кіл пристрої захисту з високим вихідним опором для зниження до мінімальної величини інформативної складової струму.

Елементи з високим вхідним опором (електричні дзвінки, телефонні капсулі, електромагнітні реле) рекомендується не тільки відключати від кіл, а й замикати на низький опір або закорочувати, щоб зменшити електричне поле від цих елементів, зумовлене напругою, наведеною під час впливу акустичного поля. При цьому слід враховувати, що обраний спосіб захисту не повинен порушувати працездатність технічного засобу і погіршувати його технічні параметри.

Високочастотні автогенератори, підсилювачі (мікрофонні, приймання, пересилання, гучномовного зв`язку) та інші пристрої, що містять активні елементи, рекомендується відключати від ліній електроживлення у "черговому режимі" або "режимі чекання виклику".

Підключення пристроїв захисту слід проводити без порушення або зміни електричної схеми і ТЗПІ, і ДТЗС.

Захист ІзОД від витоку кабелями та проводами рекомендується здійснювати шляхом:

- застосування екранувальних конструкцій;

- роздільного прокладання кабелів ОТЗ, ТЗПІ та ДТЗС.

При неможливості виконання вимог щодо рознесення кабелів електроживлення ОТЗ, ТЗПІ та ДТЗС електроживлення останніх слід здійснювати або екранованими кабелями, або від розділових систем, або через мережеві фільтри.

Не допускається утворення петель та контурів кабельними лініями. Перехрещення кабельних трас різного призначення рекомендується здійснювати під прямим кутом одна до одної.

Електроживлення ОТЗ повинно бути стабілізованим за напругою та струмом для нормальних умов функціонування ОТЗ і забезпечення норм захищеності.

У колах випрямного пристрою джерела живлення необхідно встановлювати фільтри нижніх частот. Фільтри повинні мати фільтрацію по симетричних і несиметричних шляхах поширення.

Необхідно передбачити відключення електромережі від джерела живлення ОТЗ під час зникнення напруги в мережі, під час відхилення параметрів електроживлення від норм, заданих в ТУ, та під час появи несправностей у колах електроживлення.

Усі металеві конструкції ОТЗ (шафи, пульти, корпуси роз-подільних пристроїв та металеві оболонки кабелів) повинні бути заземлені.

Заземлення ОТЗ слід здійснювати від загального контуру заземлення, розміщеного в межах контрольованої території, з опором заземлення за постійним струмом відповідно до вимог стандартів.

Система заземлення повинна бути єдиною для всіх елементів ОТЗ і будуватися за радіальною схемою.

Утворення петель і контурів у системі заземлення не допускається.

Екрани кабельних ліній ТЗПІ, що виходять за межі контрольованої території, повинні заземлятися в кросах від загального контуру заземлення в одній точці для виключення можливості утворення петель по екрану та корпусах.

У кожному пристрої повинна виконуватися умова безперервності екрана від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватися як другий провід сигнального кола або кола живлення.

Екрани кабелів не повинні мати електричного контакту з металоконструкціями. Для монтажу слід застосовувати екрановані кабелі з ізоляцією або одягати на екрани ізоляційну трубку.

У довгих екранованих лініях (мікрофонних, лінійних, звукопідсилювальних) рекомендується ділити екран на ділянки для одержання малих опорів для високочастотних струмів і кожну ділянку заземляти тільки з одного боку.

Вихідні дані для здійснення ТЗІ наведені у додатку 1.

Результати виконання технічних заходів оформляються актом приймання робіт, складеним у довільній формі, підписуються виконавцем робіт і затверджуються керівником організації (підприємства).

3.2. Способи і методи захисту інформації від витоку через ПЕМВ.

Класифікація способів і методів захисту інформації, що обробляється засобами цифрової електронної техніки, від витоку через ПЕМВ приведена на схемі.

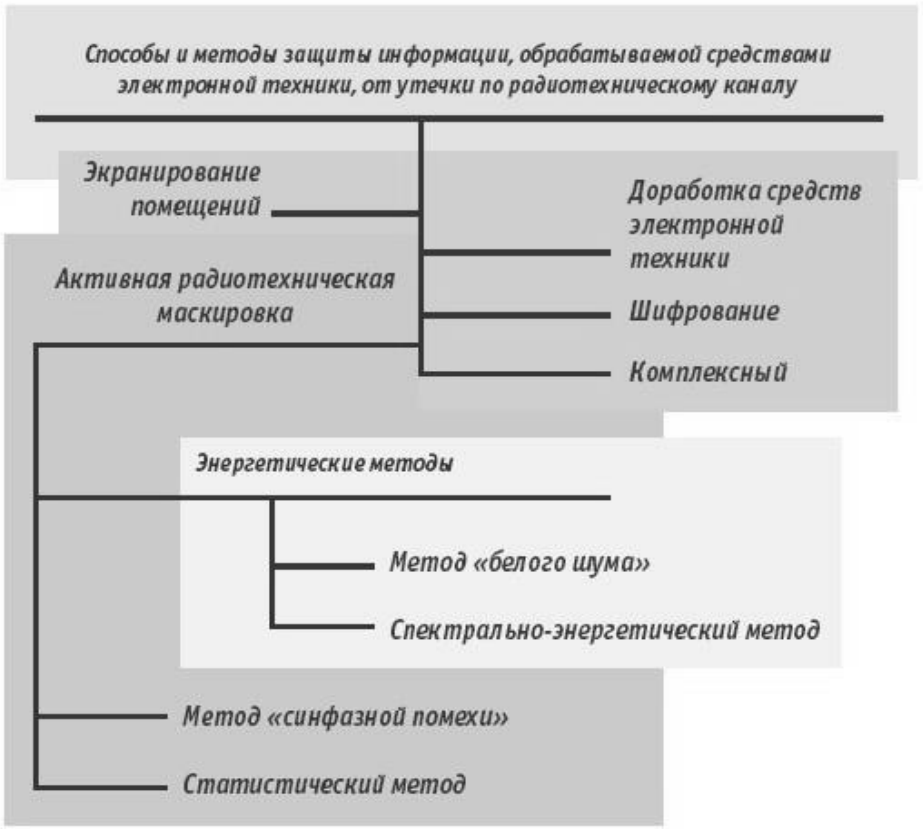

Рис. 2.5. Класифікація способів і методів захисту інформації

Коротко охарактеризуємо ці способи і методи.

Електромагнітне екранування приміщень

Електромагнітне екранування приміщень у широкому діапазоні частот є складною технічною задачею, вимагає значних капітальних витрат, постійного контролю і не завжди можливо з естетичних та ергономічних міркувань. Добудова електронного обладнання для зниження рівня ПЕМВ здійснюється уповноваженими організаціями. Використовуючи різні радіопоглинаючі матеріали та схемні рішення, можна значно знизити рівень радіації. Вартість таких модифікацій залежить від радіусу необхідної зони безпеки і, наприклад, для персонального комп'ютера становить від 20 до 70% його вартості.

Криптографічне закриття інформації

Криптографічне закриття інформації є радикальним способом її захисту. Шифрування здійснюється програмним або апаратним забезпеченням за допомогою вбудованих інструментів. Такий спосіб захисту виправданий при передачі інформації на великі відстані по лініях зв'язку. Наразі неможливо використовувати шифрування для захисту інформації, що міститься в сигналах цифрових електронних послуг.

Активне радіотехнічне маскування

Активне радіотехнічне маскування передбачає формування і випромінювання маскуючого сигналу в безпосередній близькості від електронної техніки, що захищається. Розрізняють декілька методів активного радіотехнічного маскування:

- енергетичні методи;
- метод «синфазної завади»;
- статистичний метод.

Енергетичні методи

Енергетична маскування «білого шуму» випромінює широкосмуговий шумовий сигнал з постійним енергетичним спектром, що значно перевищує максимальний рівень випромінювання електронного обладнання. В даний час найбільш поширені пристрої захисту інформації, що реалізують цей метод. До недоліків методу можна віднести створення неприпустимих перешкод радіоелектронним засобам, розташованим поблизу захищеного обладнання обробки інформації.

Спектральний енергетичний метод полягає у генерації шуму, енергетичний спектр якого визначається модулем спектральної щільності інформаційного випромінювання електронної апаратури та енергетичним спектром атмосферного шуму. Цей метод дозволяє визначити оптимальні перешкоди з обмеженою потужністю для досягнення бажаного співвідношення сигнал/шум на краю контрольованої зони.

Ці методи можна використовувати для захисту інформації як на аналоговому, так і на цифровому обладнанні. Як індикатор безпеки в цих методах

використовується співвідношення сигнал/шум. Наступні два методи призначені для захисту інформації в електронній техніці, яка працює з цифровими сигналами.

Метод «синфазної завади»

В методі **«синфазної завади»** в якості маскуючого сигналу використовуються імпульси випадкової амплітуди, що збігаються за формою і часу існування з корисним сигналом. У цьому випадку, як стверджують автори, завада повністю маскує сигнал, прийом сигналу втрачає сенс, тому що апостеріорні ймовірності наявності і відсутності сигналу залишаються рівними їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність помилки (ППВО) на кордоні мінімально допустимої зони безпеки. Однак через відсутність апаратури для безпосереднього вимірювання цієї величини автори методу припускають перерахувати ППВО в необхідне співвідношення сигнал-завада.

Статистичний метод

Статистичний метод захисту інформації полягає у зміні імовірнісної структури сигналу, що приймається приймачем розвідки, шляхом випромінювання маскуючого сигналу спеціальної форми. Матриці ймовірності зміни стану (МРТ) використовуються як характеристики контрольованого сигналу. У разі оптимального захисту від ПЕМВ МЗС вона відповідатиме еталонній матриці (всі елементи цієї матриці рівні між собою). До переваг цього методу можна віднести те, що рівень генерованого маскуючого сигналу не перевищує рівень інформативного паразитного електромагнітного випромінювання електронної апаратури. Проте статистичний метод має деякі особливості реалізації на практиці.

Методи захисту обчислювальної техніки від ПЕМВН

Найбільш небезпечними, з погляду несанкціонованого зняття за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН), є монітори комп'ютерів зі стандартами розгорнень телевізійних систем. В усіх зазначених випадках навіть використання могутніх криптографічних методів захисту інформації не приводить до бажаних результатів, і тільки застосування спеціальних методів і апаратури захисту від ПЕМВН здатне усунути виникаючий канал витоку інформації.

Такими методами є:

1. **Доробка пристроїв** обчислювальної техніки з метою мінімізації електромагнітних випромінювань (застосування малоенергетичних мікросхем, пристроїв відображення на рідкісних кристалах, локальне екранування окремих пристроїв персональних комп'ютерів, гальванічна розв'язка за ланцюгами електроживлення і т. д.).
2. **Електромагнітне екранування приміщень**, у яких розташована обчислювальна техніка, а також інше електронне устаткування, використовуване для обробки як аналогової, так і дискретної інформації.
3. **Активне радіотехнічне придушення** побічних електромагнітних випромінювань і радіотехнічне маскування працюючої апаратури.

Припинення роботи обчислювальних пристроїв може значно знизити рівень паразитного електромагнітного випромінювання, але не усуває його повністю. Слід також враховувати, що електромагнітне екранування створює певний дискомфорт у роботі користувачів та персоналу, а в деяких випадках таке екранування здійснити неможливо.

Активне радіотехнічне придушення і маскування ПЕМВН полягають у формуванні й випромінюванні в безпосередній близькості від пристроїв обчислювальної техніки широкосмугового шумового сигналу з рівнем випромінювання, що перевищує рівень інформаційних випромінювань у всьому частотному діапазоні, де є ці випромінювання, а також у здійсненні наведень, що придушують шумові коливання в ланцюги комутації, які відходять.

Для здійснення електромагнітного придушення ПЕМВН розроблено клас генераторів електромагнітних коливань **білого шуму**, що створює шумове електромагнітне поле від десятків кілогерц до одиниць ГГц зі спектральним рівнем випромінюваного сигналу, який істотно перевищує рівні природних шумів, випромінюваних засобами обчислювальної техніки.

Спектральна щільність електромагнітного поля, що випромінюється генераторами білого шуму, рівномірно розподіляється по діапазону частот шуму і

забезпечує необхідне перевищення маскуючого сигналу над фоновим електромагнітним випромінюванням у задану кількість разів.

Зараз різними організаціями розробляється, виготовляється та поширюється цілий клас таких приладів – широкосмугові генератори (передавачі) шумових електромагнітних коливань.

Існує два типи пристроїв електромагнітного зашумлення:

1) генератори **об'ємного** електромагнітного зашумлення;

2) генератори **локального** електромагнітного зашумлення.

3.3 Порядок контролю за станом технічного захисту інформації

Метою контролю є виявлення можливих технічних каналів витоку інформації (небезпечного) сигналу (спеціальне розслідування), розробка заходів щодо її приховування, оцінка адекватності та ефективності заходів захисту, оперативний контроль за технічним захистом витоку. канали інформаційного сигналу.

Технічний канал витоку вважається захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення "інформативний сигнал/шум".

Пристрої захисту та захищені технічні засоби вважаються корисними, якщо їх параметри відповідають вимогам експлуатаційних документів.

Контроль за виконанням організаційно-підготовчих технічних заходів із захисту інформації здійснюється шляхом візуального огляду прокладки проводів і кабелів, що виходять за межі об'єкта захисту, а також технічних засобів захисту та обладнання.захищених.

У ході перевірки визначаються:

- наявність електромагнітного зв`язку між лініями ОТЗ, ТЗПІ та ДТЗС (проходження в одному кабелі чи жгуті), між різними видами ТЗПІ та ДТЗС (спільний пробіг проводів систем пожежно-охоронної сигналізації, годинофікації, радіотрансляції);

- наявність виходів ліній зв`язку, сигналізації, годинофікації, радіотрансляції за межі виділених приміщень;

- наявність незадіяних ТЗПІ, ДТЗС, проводів, кабелів;

- можливість відключення ТЗПІ на період проведення конфіденційних переговорів або важливих нарад;

- рознесення джерел електромагнітних та акустичних полів на максимально можливу відстань у межах виділених приміщень;

- виконання заземлення апаратури, яке виключає можливість утворення петель з проводів та екранів;

- рознесення кабелів електроживлення ОТЗ, ТЗПІ та ДТЗС з метою виключення наводок небезпечних сигналів;

- виконання розведення кіл електроживлення екранованим або крученим кабелем;

- наявність можливості відключення електроживлення ОТЗ під час обезструмлення мережі; відхилення параметрів електроживлення від норм, заданих в ТУ, під час появи несправностей у колах живлення.

У процесі проведення спецдосліджень, перевірки ефективності технічних заходів захисту підлягають інструментальному контролю ОТЗ і лінії зв`язку.

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

Під час спецдосліджень визначається радіус, за межами якого відношення "інформативний сигнал/шум" менше гранично допустимої величини. Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витоку каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витоку, проводиться порівняння фактичних параметрів з нормованими.

У разі перевищення допустимих значень розробляються захисні заходи, застосовуються засоби захисту (екранування від джерел випромінювання, встановлення фільтрів, стабілізаторів, засобів активного захисту).

Після проведення спеціальних досліджень, розробки та впровадження засобів захисту здійснюється контроль ефективності застосовуваних технічних засобів захисту.

Під час роботи технічних засобів і захищеного устаткування, у міру необхідності, здійснюється оперативний контроль ефективності захисту каналів випуску інформаційного (небезпечного) сигналу.

Результати контролю (спеціального розслідування) оформлюються актом, складеним у довільній формі, підписаним інспектором і затвердженим керівником організації (підприємства).

ВИСНОВКИ

Технічному захисту підлягає інформація з обмеженим доступом, яка обробляється, поширюється, відображається в автоматизованих системах та обчислювальних засобах. Носіями цієї інформації є електричні та електромагнітні поля та сигнали, що утворюються в результаті роботи технологічного обладнання (основних технічних засобів) або впливу небезпечного сигналу на відкриті засоби обробки інформації, засоби та системи життєзабезпечення (засоби та допоміжні технічні системи).

Канали витоку інформаціє можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території. Інформативні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами КТ.

Роботи з технічного захисту інформації (ТЗІ) в АС і ЗОТ передбачають: категоріювання об'єктів електронно-обчислювальної техніки; включення до технічних завдань на монтаж АС і ЗОТ розділу з ТЗІ; монтаж АС і ЗОТ відповідно до рекомендацій НД ТЗІ; обстеження (в тому числі технічний контроль) об'єктів ЕОТ; установлення (при необхідності) атестованих засобів захисту; технічний контроль за ефективністю вжитих заходів.

В дипломній роботі розглянуто політику безпеки, основні її засади, загрози інформації, витоки інформації каналами ПЕМВ.

Розглянуто механізми побудови захисту від перехвату інформації по каналам ПЕМВ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок

2. ТР ТЗІ - ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок

3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу

5. Гребенніков В. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ. ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД / В. Гребенніков — «Издательские решения», 2019.

6. Андреев В.І. СТРАТЕГІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: підручник / В.І.Андреев, В.Д.Козюра, Л.М.Скачек, В.О.Хорошко. – К.: Вид. ДУІКТ, 2007. – 277 с.

7. Белов Е.Б. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шлепанов. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.

8. Блавацька Н.М. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.

9. Бузов Г.А. ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ: Учебное пособие для студентов высших учебных заведений / Г.А.Бузов, С.В.Калинин, А.В.Кондратьев. – М.: «Горячая линия – Телеком», 2005. – 416 с.

10. Гайворонський М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ / М.В.Гайворонський, О.М.Новиков. - К.: Видавнича група BHV, 2009. - 608 с.

11. Ленков С.В. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ТОМ II. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко; под ред. В.А.Хорошко. – К.: Арий, 2008. –344 с.

12. Малюк А.А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ: учеб. пособие для студентов высших учебных заведений. – М.: «Горячая линия – Телеком», 2004. – 280 с.

13. Мельников В.П. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ: учеб. пособие для студ. высш. учеб. заведений / В.П.Мельников, С.А.Клейменов, А.М.Петраков; под. ред. С.А.Клейменова. – 3-е изд., стер. – М.: Изд. центр «Академия», 2008. – 336 с.

14. Меньшаков Ю.К. ЗАЩИТА ОБЬЕКТОВ И ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКИХ СРЕДСТВ РАЗВЕДКИ: Учеб. пособие для студентов высших учебных заведений / Ю.К.Меньшаков. – М.: Росийский государственный гуманитарный университет, 2002. – 399 с.

15. Сёмкин С.Н. ОСНОВЫ ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ И НФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ: Учебное пособие / С.Н.Сёмкин, Э.В.Беляков, С.В.Гребенев, В.И.Козачок. – М.: Гелиос АРВ, 2005. – 192 с.

16. Торокин А.А. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Учебное пособие для студентов высших учебных заведений / А.А.Торокин. – М.: «Гелиос АРВ», 2005. – 960 с.

17. Хорев А.А. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ. ЧАСТЬ 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ: Учебное пособие. – М.: Гостехкомиссия России, 1998. – 320 с.

18. Хорошко В.А. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ / В.А.Хорошко, А.А.Чекатков; под ред. Ю.С.Ковтанюка. – К.: Изд-во «ЮНИОР», 2003. – 504 с.

19. Шаньгин В.Ф. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ / В.Ф.Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

20. Щеглов А.Ю. ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА / А.Ю.Щеглов. – СПб.: Изд-во Наука и Техника, 2004. – 384 с.

21. Ярочкин В.И. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебник для студентов вузов, 2 -е изд. / В.И.Ярочкин. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

22. Грайворонський М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ: Підручник / М.В.Грайворонський, О.М.Новіков. — К: Видавнича група BHV, 2009. — 608 с.

23. 26. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

24. Яремчук Ю.Є. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ/ Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін. Навчальний посібник, 2018. https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi

25. Остапов С. Е. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. Навчальний посібник. – Х. : Вид. ХНЕУ, 2013. – 476 с.

26. Лужецький В.А. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ / В.А. Лужецький, А.Д.Кожухівський, О.П. Войтович. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.

27. Пількевич І.А. ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ/І.А. Пількевич, Н.М. Лобанчикова, К.В.

Молодецька. Навчальний посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

28. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс] : навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.] К.: НТУУ «КПІ», 2016. – 104 с.

29. Біла книга Держспецзв'язку

http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941