

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ
до виконання курсового проекту з дисципліни
“ Фізико – технічні методи захисту інформації “
для студентів спеціальностей 7.160103
“Системи захисту від несанкціонованого доступу”
та 7.160105 «Захист інформації в комп’ютерних системах
та мережах»
всіх форм навчання

2008

Методичні вказівки до виконання курсового проекту з дисципліни "Фізико-технічні методи захисту інформації" для студентів спеціальностей 7.160103 "Системи захисту від несанкціонованого доступу" та 7.160105 «Захист інформації в комп'ютерних системах та мережах» всіх форм навчання /Укл.: Ключко В.В.- Запоріжжя: ЗНТУ, 2008. -56 с.

Укладач - ст.викладач Ключко В.В.

Рецензент – професор Карпуков Л.М.

Відповідальний
за випуск

Ключко В.В.

Затверджено
на засіданні кафедри
"Захист інформації"
Протокол № 10
від 05.07.2007р.

ЗМІСТ

ВСТУП	5
1 МЕТА І ЗАВДАННЯ КУРСОВОГО ПРОЕКТУ.....	5
2. ЗМІСТ КУРСОВОГО ПРОЕКТУ	6
2.1. Організація курсового проектування	6
2.2. Зміст пояснювальної записки	7
2.2.1 Реферат	7
2.2.2 Зміст	7
2.2.3 Основна частина	8
2.2.4. Заключення	8
2.2.5 Перелік посилань.....	9
2.2.6 Додатки	9
2.3 Порядок і зміст захисту курсової роботи	9
3 ЗРАЗКИ ТЕМ КУРСОВОГО ПРОЕКТУ	10
4 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З РОЗРАХУНКУ ДЕЯКИХ ПРИСТРОЇВ ЗАХИСТУ ІНФОРМАЦІЇ	12
4.1 Вибір і обґрунтування можливих варіантів побудови електричних схем шумових генераторів	12
4.1.1 Резистивний генератор шуму	12
4.1.2 Генератор шуму на напівпровідниковому діоді	13
4.1.3 Генератор шуму на лампі розжарювання	14
4.1.4 Генератор шуму на ламповому стабілітроні	15
4.1.5 Генератор шуму на ламповому шумовому діоді	16
4.1.6 Простий генератор шуму на напівпровідниковому стабілітроні	17
4.1.7 Генератор шуму на шумовому діоді.....	20
4.1.8 Генератори шуму на транзисторах	20
4.1.9 Простий пристрій придушення радіомікрофонів	23
4.1.10 Цифровий шумовий генератор	24
4.1.11 Потужний генератор завад	25
5 ЗАХИСТ АКУСТИЧНОГО ТА ВІБРОАКУСТИЧНОГО КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ	26
5.1 Критерії захисту мовних повідомлень	27

5.2 Випадок використання однорідної перегородки	28
5.3 Випадок використання неоднорідної перегородки	31
6 ЗАХИСТ ТЕЛЕФОННИХ ЛІНІЙ	32
6.1 Захист телефонних переговорів	32
6.2 Захист інформації на енергетичному рівні. Активні методи захисту телефонних каналів	33
6.3 Метод «синфазної» маскуючої низькочастотної завади.....	33
6.4 Метод високочастотної маскуючої завади	34
6.5 Метод «ультразвукової» маскуючої завади	35
6.6 Метод низькочастотної маскуючої завади	35
6.7 Метод підвищення напруги	35
6.8 Метод пониження напруги	35
6.9 Компенсаційний метод	36
6.10 Метод випалювання	36
6.11 Пасивні методи захисту телефонних ліній та пристроїв ..	37
7 ПЕРЕДАВАЧІ ПО МЕРЕЖІ ЕЛЕКТРОЖИВЛЕННЯ 220 В ...	40
8 ФІЛЬТРУВАННЯ НАПРУГИ ЕЛЕКТРОЖИВЛЕННЯ РЕА..	
БОРІТЬБА З ПЕВМІН	45
ЗАКЛЮЧЕННЯ	54
ЛІТЕРАТУРА	54
Додаток	56

ВСТУП

Дані методичні вказівки містять рекомендації щодо виконання курсового проекту з дисципліни "Фізико-технічні методи захисту інформації".

Метою виконання курсового проекту є поглиблення теоретичних та набуття практичних навичок з розрахунку та аналізу конкретних технічних каналів витоку інформації та засобів її захисту.

Під час організації технічного захисту інформації необхідно розглядати всю сукупність технічних засобів, за допомогою яких зберігають, обробляють та передають інформацію з обмеженим доступом. До таких пристроїв входить з'єднувальне, розподільче та комунікаційне обладнання, система електроживлення і заземлення, допоміжні технічні засоби такі як телефонний зв'язок, пожежна і охоронна сигналізація, проводи яких виходять за межі контрольованої зони.

У сучасному житті основні об'єми інформації обробляються і передаються електронними методами, завдяки чому ці процеси супроводжуються електромагнітними випромінюваннями. Тому існує реальна загроза несанкціонованого доступу до цієї інформації за допомогою засобів радіоперехватування або контактного підключення до комунікацій.

Наприклад, за даними АНБ США приблизно 80% розвідувальної інформації отримується технічними каналами витоку інформації за рахунок її радіоперехоплення.

1 МЕТА І ЗАВДАННЯ КУРСОВОГО ПРОЕКТУ

Курсовий проект являється складовою частиною навчального курсу «Фізико-технічні методи захисту інформації» і призначений для практичного закріплення і розширення отриманих теоретичних знань. Завданням курсового проекту являється придбання студентами навичок з проектування пристроїв захисту інформації або їх базових вузлів, а також поглиблення знань з питань сучасних методів розробки пристроїв для організації каналів витоку інформації.

Студент повинний здійснити огляд існуючих методів та засобів захисту інформації, притягти до складу комплексу захисного обладнання існуючі пристрої захисту. Під час проектування також перевіряються навички студентів з користування навчально-науковою

літературою, науковими сайтами з Інтернету.

2. ЗМІСТ КУРСОВОГО ПРОЕКТУ

2.1. Організація курсового проектування

Тривалість виконання курсового проекту – 14 неділь. Кожен студент виконує індивідуальне завдання, яке йому визначає викладач. Перелік тем курсових проектів наведено у розд.3 цих методичних вказівок.

За підсумками виконання проекту студент оформлює пояснювальну записку і один лист графічного матеріалу формату А3. Вимоги до оформлення записки викладено нижче. Потім студент здає записку на перевірку керівнику курсового проекту. Після перевірки записка повертається студенту для усунення виявлених недоліків або для захисту.

Календарний графік роботи над темою курсового проекту наведено у табл. 2.1.

Таблиця 2.1- Календарний графік виконання курсового проекту

№ етапу	Виконувана робота	Тиждень семестру
1	Отримання завдання на проектування	1
2	Аналіз технічного завдання	2
3	Пошук і огляд літературних джерел у відповідності до отриманого завдання	3-4
4	Аналіз факторів витоку інформації	5
5	Вибір первинних та вторинних демаскуючих ознак	6
6	Детальний опис каналу витоку інформації	7
7	Опис методів захисту інформації	8
8	Опис заходів, спрямованих на збереження і захист інформації	9-10
9	Оформлення курсового проекту	11
10	Здача готового проекту на перевірку	13
11	Захист курсового проекту	14

2.2. Зміст пояснювальної записки

Пояснювальна записка оформляється на аркушах формату А4 і повинна мати:

- 1) титульний лист;
- 2) завдання на курсовий проект;
- 3) реферат;
- 4) зміст;
- 5) вступ;
- 6) основну частину;
- 7) висновки (заключення);
- 8) перелік посилань;
- 9) додатки.

При цьому 1), 2), 3), 4), 5), 7), 8), 9) як розділи не нумеруються.

Допускається перед рефератом розміщати сторінку з прийнятими у подальшому тексті скороченнями.

2.2.1 Реферат

Реферат розташовується на третій сторінці пояснювальної записки і включає такі відомості:

- відомості про обсяг курсового проекту, кількість ілюстрацій, таблиць, використаних літературних джерел;
- текстова частина;
- перелік ключових слів.

Текст реферату відбиває наведену в курсовому проекті інформацію, як правило, у такій послідовності: об'єкт дослідження або розробки; мета роботи; використані методи; отримані результати. Реферат повинен мати обсяг не більший, як 500 слів.

Кількість ключових слів дорівнює від 5 до 15. Вони пишуться заголовними літерами в називному відміннику, в рядок через коми.

2.2.2 Зміст

Зміст вміщує назву усіх розділів та підрозділів (починаючи зі вступу) з позначенням номеру сторінки, на якій починає викладатися матеріал розділу (підрозділу). Назва розділів пишеться заголовними літерами, а підрозділів - малими з заголовної першої літери.

2.2.3 Вступ

У цьому розділі викладаються відомості про призначення та застосування пристрою, який розробляється. Тут же викладається сучасний стан і напрямки подальшого розвитку того класу пристроїв, який проектується, відзначаються їх переваги і недоліки.

Приблизний об'єм вступу – 1...2 сторінки.

2.2.4 Основна частина

У разі, коли завдання передбачає розробку пристрою, то спочатку здійснюється обґрунтування і вибір структурної або функціональної схеми системи або пристрою. На схемі може бути виділено той блок, який підлягає розробці. Потім надається деталізована функціональна схема блоку, який розробляється, з описанням принципу його роботи.

Огляд аналогічних рішень пишеться після вивчення спеціальної літератури за темою курсового проекту. Огляд повинен мати критичний характер: необхідно відзначати позитивні якості, а також недоліки розглянутих методів захисту інформації, вибраних засобів та пристроїв, які аналізуються.

Після цього виконуються необхідні електричні (акустичні) розрахунки, здійснюється вибір елементної бази. І як результат обґрунтовується схема електрична принципова, яка наводиться у додатку до пояснювальної записки на листі формату А3.

Якщо здійснюються розрахунки, наприклад, систем активного шумлення, або розробка методик, то в основній частині записки у першому підрозділі надаються теоретичні відомості, а в наступних – викладаються необхідні розрахунки.

Текст записки доповнюється рисунками, таблицями та графіками. Рисунки можуть містити необхідні для пояснень і розрахунків фрагменти загального каналу захисту.

Текст основної частини поділяється на розділи і підрозділи. Назви розділів пишуться жирним шрифтом заголовними літерами, а підрозділів – жирними, з першої заголовної літери.

Всі наведені формули і запозичені технічні рішення повинні мати посилання на їх джерело з указанням сторінок, наприклад [5] ст.24.

Оформлювати пояснювальну записку необхідно у

відповідності до стандарту підприємства (СТП ЗНТУ 15-96).
Максимальний обсяг ПЗ – повинен складати 30-40 сторінок.

2.2.5 Висновки (Заключення)

У цьому розділі ПЗ наводяться висновки з виконаної роботи з викладенням технічних характеристик системи (пристрою, вузла) які розроблялись і їх відповідність технічному завданню.

Обсяг цієї частини записки повинен складати не більше однієї сторінки.

2.2.6 Перелік посилань

Перелік літературних джерел допоможе студентам освоїти необхідний науковий матеріал і своєчасно виконати курсову роботу. Цей перелік є обов'язковою частиною курсової роботи і повинен додаватися у її кінці. Його обсяг показує наскільки глибоко обґрунтовані теоретичні та практичні положення, на яких будується курсова робота.

2.2.7 Додатки

У додатках наводиться принципова схема системи чи пристрою на аркуші формату А3 у згорнутому вигляді. Принципові електричні схеми супроводжуються специфікацією (переліком) елементів розрахованої схеми.

Графічний матеріал проекту виконується у відповідності до вимог ЕСКД.

Нумеруються додатки великими літерами українського алфавіту. Номер ставиться у правому верхньому куті аркушу, наприклад, Додаток А.

2.3 Порядок і зміст захисту курсової роботи

Призначення захисту - оцінити повноту, складність виконаної роботи, загальний рівень, кваліфікацію розробника і ступінь самостійності його роботи.

Захист відбувається за графіком у присутності комісії з двох викладачів, один з яких є керівником курсової роботи. На доповідь відводиться 6-7 хвилин. За цей час необхідно стисло викласти зміст поставленої задачі (одна хвилина), доповісти про власну роботу по

вибору методів та засобів захисту каналу передачі інформації (4-5 хвилини) і зробити висновки (одна хвилина). Необхідно розповідати про свою власну роботу, пояснювати, чому прийнято саме такі рішення, на основі яких міркувань були вибрані методи захисту каналу і обирались засоби його захисту.

Після закінчення доповіді учасники комісії задають питання, призначення яких — уточнити рівень кваліфікації і ступень самостійності доповідача під час виконання ним курсового проекту. На питання необхідно давати стислі прямі відповіді, при необхідності ілюструючи їх відповідними формулами, графіками, рисунками, діаграмами, які наведено у пояснювальній записці.

Захист є важливим етапом виконання курсової роботи. До нього треба готуватись і заздалегідь складати план доповіді з урахуванням відведеного для цього часу. Найбільш поширена помилка при захистах - докладні описи широко відомих речей, досконалий опис каналу витоку інформації, і внаслідок цього – відсутність часу на демонстрацію рівня власної кваліфікації доповідача. Доповідати необхідно про власну роботу над курсовим проектом і при цьому ефективно використовувати весь час, що його відведено для захисту.

3 ЗРАЗКИ ТЕМ КУРСОВОГО ПРОЕКТУ

1. Двоканальний генератор «білого акустичного шуму» для захисту акустики приміщень. Діапазон частот 200...5 000 Гц.

2. Генератор шуму для маскування ПЕМВІН працюючих ПЕОМ. Діапазон частот 0,1...1000 МГц. Нерівномірність спектральної потужності - не більше 40 дБ.

3. Генератор шуму для придушення радіозакладних пристроїв з ЧМ, що працюють у діапазоні частот 130...170 МГц.

4. Генератор шуму для придушення радіозакладних пристроїв з ЧМ, що працюють у діапазоні частот 200...250 МГц.

5. Генератор шуму для придушення радіозакладних пристроїв з ЧМ, що працюють на частоті 433,8 МГц.

6. Фільтри для захисту телефонних апаратів від з'єму інформації за рахунок ВЧ-нав'язування та мікрофонного ефекту дзвінка.

7. Мережевий фільтру електроживлення для засобів обчислювальної техніки та передавання інформації.

8. Електромагнітний та електричний екрани з ефектом

екранування -80 дБ.

9. Методика розрахунку комплексного захисту виділених приміщень від втрат мовної інформації.

10. Методика дослідження акустичної захищеності виділених приміщень.

11. Методика комплексного захисту від витоку інформації по провідних лініях.

12. Методика комплексної нейтралізації радіозакладних пристроїв з методикою пошуку радіозакладок.

13. Теоретичні основи виникнення ПЕМВІН і методика їх вимірювань.

14. Методика технічного забезпечення конфіденціальності переговорів, які проводяться у звичайних умовах.

15. Методика визначення місця установки радіозакладного пристрою у робочому приміщенні.

16. Комплексний метод захисту телефонних ліній.

17. Аналогові скремблери і огляд сучасного ринку скремблерів.

18. Комбіновані мовні скремблери і їх різновиди.

19. Фізико-технічні основи роботи нелінійних локаторів і методика робіт з цими приладами.

20. Техніко-економічний аналіз сучасного ринку нелінійних локаторів.

21. Структурна схема сучасного локатора нелінійностей і розрахунок частот для приймання 2-ї та 3-ї гармонік.

22. Система отримання мовної інформації за допомогою мережі електроживлення.

23. Сучасний стан використання мереж електроживлення для завдань передавання інформації.

24. Одинадцятисмутовий еквалайзер на транзисторах.

25. Одинадцятисмутовий еквалайзер на мікросхемах.

26. Автоматичний телефоний мікропередавач з ЧМ на 433,8 МГц.

27. Відео- та аудіопередавач середньої потужності на частоту 479,5 МГц.

28. Система захисту інформації у разі її витоку оптичним каналом.

29. Система охоронної сигналізації для виділеного об'єкту.

30. Автоматичний вмикач пристрою запису телефонних розмов.

31.Методика вимірювань спектру випромінювання монітору та відео карти комп'ютера за допомогою програмно-апаратного комплексу на базі скануючого приймача AR8200Mk3 та спеціалізованого програмного забезпечення DigiScan EX Standart.

32.Пристрій пошуку скритої проводки.

33.Детектор радіовипромінювань.

34.Захищена система електроживлення ПЕОМ.

35.Захист комп'ютера від несанкціонованого доступу.

36.Принципи побудови систем захисту від несанкціонованого захисту комп'ютерних мереж.

4 ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З РОЗРАХУНКУ ДЕЯКИХ АКТИВНИХ ПРИСТРОЇВ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Вибір і обґрунтування можливих варіантів побудови електронних схем шумових генераторів

Генератори шумових завад можна розділити на дві групи:

- 1) генератори на задаючих пасивних радіоелементах;
- 2) транзисторні і цифрові генератори.

Розглянемо основні практичні схеми генераторів шуму, які можливо використовувати як задаючі в складніших пристроях.

4.1.1 Резистивний генератор шуму

Цей генератор (рис. 4.1) дозволяє генерувати шум в діапазоні частот 140...1300 МГц. ЕРС шуму виникає в генераторі завдяки підвищенню температури струмопровідного шару резистора, який нагрівається постійним струмом.

На резистор R1 опором 50, 75, 300 Ом (залежно від необхідного вихідного опору генератору), постійна напруга поступає через фільтр, що складається з дроселю L1 і конденсатору C2.

Струм, що протікає через резистор R1, регулюють змінним резистором R2, а це призводить до зміни його температури. Перемикачем SA1 генератор можна підключити до вбудованого або зовнішнього джерела живлення з напругою 12...14 В.

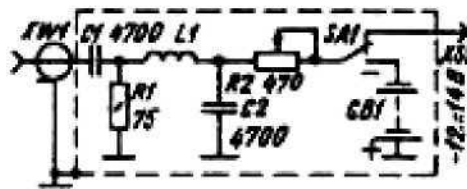


Рисунок 4.1 – Резистивний генератор шуму

Конструктивно генератор виконаний в прямокутному корпусі з фольгованого склотекстоліту завтовшки 1,5 мм (або у штампованому металевому корпусі) із знімною нижньою кришкою. На передню панель корпусу виведена ручка резистора R2 зі шкалою. Конденсатор C1 безкорпусний типу K10-9. Його припаюють безпосередньо до заздалегідь укороченого врівні з корпусом центрального виведення рознімання XW1. Резистор R1 типу МЛТ-0,125. Дросель L1 містить 15 витків емальованого дроту діаметром 0,6 мм, намотаних на об'ємовування діаметром 4 мм. Крок намотування змінний - від «виток до витку» на початку, до 3 мм у кінці, що присьднується до резистора R1.

4.1.2 Генератор шуму на напівпровідниковому діоді

Схема одного з «простих» генераторів шуму показана на рис.4.2. Роль джерела шумів грає замкнутий р-п-перехід кремнієвого діода VD1 (типу ДК-И1 або йому подібний). Регулювання зворотного струму, що протікає через діод, а отже, і регулювання вихідної потужності шумів здійснюється резистором R1. Струм вимірюється міліамперметром ИП1 із струмом повного відхилення 1 мА. Можна виключити з схеми міліамперметр, тоді слід забезпечити шкалою резистор R1, щоб по величині кута повороту його ручки судити про шумову потужність. Конденсатор C1 перешкоджає проходженню шумової складової в ланцюг джерела живлення. Джерелом живлення генератору може служити як батарея, так і блок живлення.

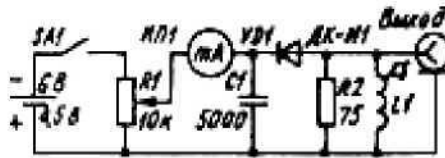


Рисунок 4.2 – Генератор шуму на напівпровідниковому діоді

Особливо слід розглянути роль резистору R2. Він є опором навантаження і, по суті, вихідним опором генератора. Як вже указувалося вище, його слід вибирати рівним входному опору приймачів, який звичайно дорівнює 50 або 75 Ом. Якщо входний опір приймача має іншу величину, наприклад, 300 Ом, то і опір резистора повинен бути рівний 300 Ом. Компенсуючу індуктивність L1 розраховують так, щоб спільно з ємністю діода і ємністями схеми вона забезпечувала резонанс в робочому діапазоні частот. Остаточна підгонка цієї індуктивності здійснюється у процесі настроювання. Під час цієї операції резистор R2 слід вибрати зі схеми, оскільки він вносить сильне загасання в утворений коливальний контур. Після настроювання резистор треба упаяти в схему. Підгонку індуктивності L1 можна проводити з невисокою точністю, оскільки у разі включеного резистору R2 резонансна характеристика коливального контуру стає площинною. У крайніх випадках взагалі можна не включати індуктивність L1.

Генератор можна зібрати у невеликій металевій коробці. Монтаж C1, VD1, R2, L1 слід проводити без застосування додаткових провідників, кінці на елементах повинні бути максимально укорочені. Особливе це відноситься до резистору R2.

Для зниження паразитних індуктивностей можна також рекомендувати паралельне включення двох або більш резисторів, результуючий опір яких повинен дорівнювати необхідній величині опору резистору R2.

4.1.3 Генератор шуму на лампі розжарювання

Шумовий генератор можна побудувати за схемою, яка наведена на рис.4.3. Джерелом шуму у цій схемі являється опір нагрітої до високої температури вольфрамової нитки лампочки розжарювання. Все сказане вище щодо створення шумового генератора на

напівпровідниковому діоді справедливо і для цієї схеми. З лампочкою розжарювання слід виконати наступну операцію: акуратно відокремити скляний балон від цоколя і відпаяти виводи від цоколя. У схему лампочку необхідно паяти без додаткових провідників.

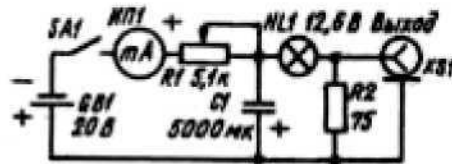


Рисунок 4.3 – Генератор шуму на лампі розжарювання

4.1.4 Генератор шуму на ламповому стабілітроні

У шумовому генераторі в епоху радіоламп використовувався газовий стабілітрон. Схема такого генератора зображена на рис. 4.4. Максимальний струм, що протікає через стабілітрон СГ2П, рівний 30 мА. Цей струм слід розраховувати з врахуванням опору фільтру випрямляча Rф. Напруга на конденсаторах фільтру C1, C2 повинна складати 220 В.

Потенціометр R2 являє собою дрітаний змінний резистор з хорошим контактом між движком і намотаним шаром дроту. Резистор R1, що підключається до схеми за допомогою вимикача SA1, покращує установку малих значень потужності шумів.

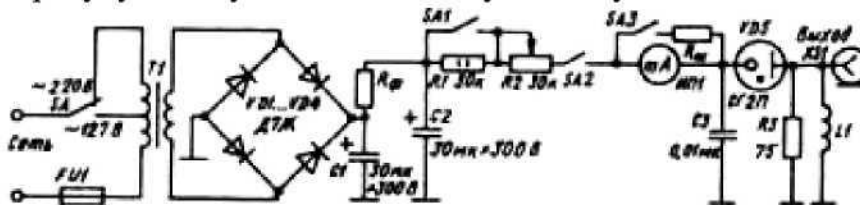


Рисунок 4.4 – генератор шуму на ламповому стабілітроні.

Як вимірювальний прилад застосовано міліамперметр чутливістю 10 мА. Паралельно йому вимикачем SA3 підключається шунтуючий резистор Rш, з тим щоб розширити чутливість приладу до 30 мА. Тоді прилад матиме два діапазони вимірювань, що дозволить

достатньо точно встановлювати як велику, так і малу вихідну потужність. Катод підключається до плюса джерела високої напруги, чим досягається підвищення потужності шумів.

4.1.5 Генератор шуму на ламповому шумовому діоді

Шумовий діод повинен працювати в режимі насичення, тобто анодна напруга діода повинна бути достатньо високою. Змінити анодний струм можна струмом накаливання діода, оскільки із зміною цього струму змінюється температура катоду, а слідовно, і число «викинутих» катодом електронів.

Зміна струму емісії при зміні напруги накаливання повинна відбуватися практично миттєво, оскільки в іншому випадку можлива поява провалів в спектрі шумів. Цим вимогам найкращим чином відповідають прямонакальні катоди з чистого або тарованого вольфраму. У останніх режим насичення досягається при відносно низькій анодній напрузі близько 100 - 150 В.

Головна перевага лампових шумових діодів полягає в тому, що їх дробовий шум має рівномірний спектр до надзвичайно високих частот. При цьому вони забезпечують більшу потужність, ніж резистивні генератори.

Проте, з-за наявності шунтуючої ємності, складеною міжелектродною ємністю анод-катод, а також ємністю між виводами в реальному шумовому діоді, межа спектру, що генерується, дорівнює 300 – 400 МГц. У шумових генераторів для компенсації впливу шунтуючих ємностей часто паралельно виходу включають індуктивність, створюючи спільно з шунтуючими ємностями паралельний коливальний контур, настроєний на робочу частоту.

Для отримання генератора шуму, у якому шум калібрується за рівнем, використовують спеціальні шумлячі вакуумні діоди., що працюють в режимі насичення. Спектральна щільність потужності шуму, що генерується, пропорційна анодному струму діода.

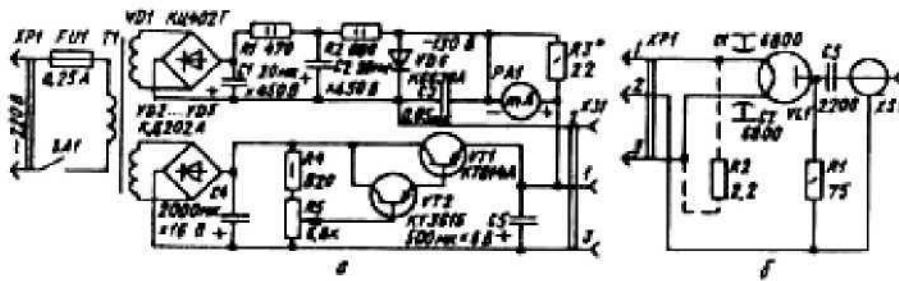


Рисунок 4.5 – Генератор шуму на ламповому шумовому діоді

Свого часу в СРСР набули поширення шумові діоди двох типів - 2ДЗБ і 2Д2С. Перший з них застосовується в діапазоні високих частот (до 30 МГц), а другий - в діапазоні ультрависоких частот (до 600 МГц). Діод 2ДЗБ допускає максимальний струм аноду 5 мА, а 2Д2С - 40 мА.

Принципова схема генератора шуму зображена на рис.4.5. Він складається з блоку живлення (рис 8.5,а), і виносної головки (рис 8.5,б). У блоці живлення є випрямляч (VD1), стабілізатор анодної напруги (VD6), випрямляч напруги живлення катода (VD2 - VD5) і схема регулювання струму катода на транзисторах VT1 і VT2. Регулюють струм розжарення за допомогою змінного резистора R5, вісь якого виведена на передню панель блоку. На панелі також розташовано міліамперметр, яким вимірюється анодний струм діода.

Прилад має дві змінні генераторні головки з діодами обох типів. Вони зібрані за однією схемою. Анодним навантаженням і еквівалентом антени служить резистор R1 типу МЛТ-0,25 на 50 або 75 Ом. Конденсатор C3 служить для розділення напруг. Резистор R2 дотрятий опором 2,2 Ом. Він використовується в головці з діодом 2ДЗБ і служить для створення однакового навантаження для схеми регулювання струму розжарення катода діода.

4.1.6 Простий генератор шуму на напівпровідниковому стабілітроні

Особливість сигналу такого генератора в його хаотичній формі і широкому діапазоні частот - від сотень герц до десятків мегагерц. Схема генератору шуму зображена на рис. 4.6. Характерно, що

«шумлять» практично всі стабілітрони серій Д808-Д813, Д814А-Д814В, а стабілітрони КС133А, КС147А і багато інших непридатні для роботи в подібному режимі. Слід також пам'ятати, що напруга батареї GB1 залежить від використовуваного стабілітрона і вона повинна перевищувати напругу стабілізації мінімум на 2 В.

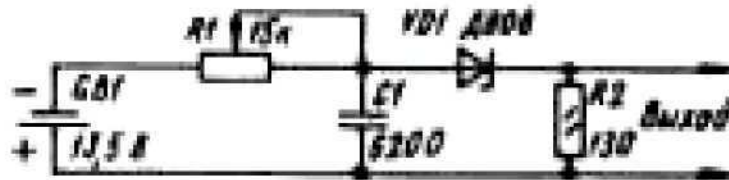


Рисунок 4.6 – Простий генератор шуму на напівпровідниковому стабілітроні

Одним з варіантів генератору шуму на стабілітроні є схема, зображена на рис. 4.7, взята зі схеми імітатора шуму прибою, яка складається з генератора шуму (транзистор VT1 і стабілітрон VD1) і емітерного повторювача (VT2). Джерелом шумового електричного сигналу є кремнієвий стабілітрон VD1, що працює в так званому режимі лавинного пробою при малому зворотному струмі.

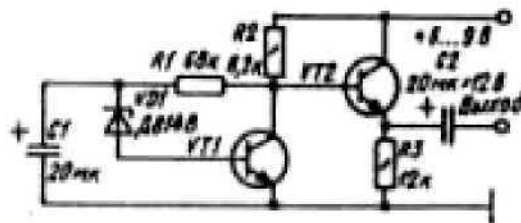


Рисунок 4.7 – Генератор шуму на стабілітроні

Найпростішим методом отримання білого шуму є використання шумлячих електронних елементів (ламп, транзисторів, різних діодів) з посиленням напруги шуму. Принципова схема нескладного генератора шуму приведена на мал. 4.8.

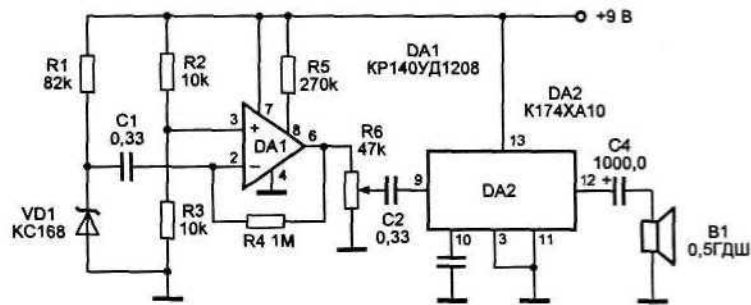


Рисунок 4.8- Генератор білого шуму

Джерелом шуму є напівпровідниковий діод — стабілітрон VD1 типу KC168, що працює в режимі лавинного пробію при дуже малому струмі. Сила струму через стабілітрон VD1 складає всього лише близько 100 мкА. Шум, як корисний сигнал, знімається з катода стабілітрона VD1 і через конденсатор C1 поступає на інвертуючий вхід операційного підсилювача DA1 типу KP140UD1208. На неінвертуючий вхід цього підсилювача поступає напруга зсуву, рівна половині напруги живлення з дільника напруги, виконаної на резисторах R2 і R3. Режим роботи мікросхеми визначається резистором R5, а коефіцієнт посилення — резистором R4. З навантаження підсилювача змінного резистора R6 посилена напруга шуму поступає на підсилювач потужності, виконаний на мікросхемі DA2 типу K174XA10. З виходу підсилювача шумовий сигнал через конденсатор C4 поступає на малогабаритний ширококутовий гучномовець B1. Рівень шуму регулюється резистором R6.

Стабілітрон VD1 генерує шум в широкому діапазоні частот від одиниць герц до десятків мегагерц. Проте на практиці він обмежений АЧХ підсилювача і гучномовця. Стабілітрон VD1 підбирається по максимальному рівню шуму, оскільки стабілітрони є джерелом шуму, що не калібрується. Він може бути будь-яким з напругою стабілізації менш напруги живлення.

Мікросхему DA1 можна замінити на KP1407UD2 або будь-який операційний підсилювачі з високою граничною частотою коефіцієнта одиничного посилення. Замість підсилювача на DA2 можна використовувати будь-які УЗЧ.

4.1.7 Генератор шуму на шумовому діоді

На рис. 4.9 показана схема генератора шуму на спеціальному шумовому діоді типу 2Г401 (єдиний в СНД серійний), який характеризується досить високою спектральною щільністю шумової напруги - $10\text{мкВ}/\sqrt{\text{Гц}}$. Діод забезпечує широкосмуговий «білий» шум, який посилюється будь-яким операційним підсилювачем.

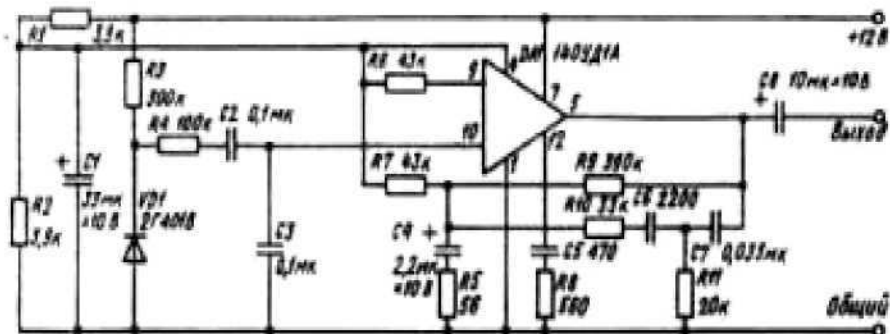


Рисунок 4.9 – Генератор шуму на шумовому діоді

Наприклад, 140УД1А з відповідними коректуючими ланцюгами СЗС4R5 і R10C6C7R1, що формують АЧХ генератору шуму в діапазоні частот його роботи.

4.1.8 Генератори шуму на транзисторах

Як відомо, генератор так званого «білого» шуму характеризується рівномірним по частоті розподілом середніх значень спектральних складових. Як задаючі (що шумлять) елементи в таких генераторах можна використовувати і транзистори, включені особливим способом. Генератори шуму на транзисторах мають невеликі розміри, економічні і нескладні (рис.4.10). Власне генератором шуму служить емітерний перехід транзистора, що назад змішав VT1. Даний генератор шуму використовується як задаючий для електронних музичних інструментів, і його можна використовувати в пристроях придушення мережевих закладних пристроїв.

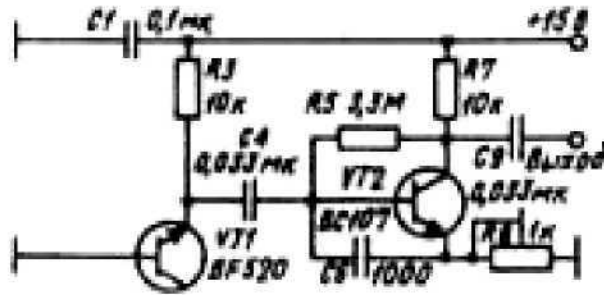


Рисунок 4.10 – Генератор шуму на транзисторах

На рис. 4.11 як джерело «білого» шуму використаний надрегенеративний каскад на транзисторі VT1. З нього через фільтр нижніх частот R5, C5 сигнал «білого» шуму поступає на підсилювальний каскад VT2.

Розглянемо ще одну оригінальну схему генератора шуму на транзисторах, що працює в найбільш поширеному для радіомікрофонів частотному діапазоні. Пристрій складається з генератора шуму (ГШ), імпульсного модулятора (ІМ), низькочастотного генератора (ГНЧ) і джерела живлення (ІП) (рис.4.12,б). Смуга шумового сигналу 100 – 350 МГц при амплітуді вихідного сигналу не менше 5мВ, низькочастотного 60 Гц – 6 кГц не менше 100 мВ.

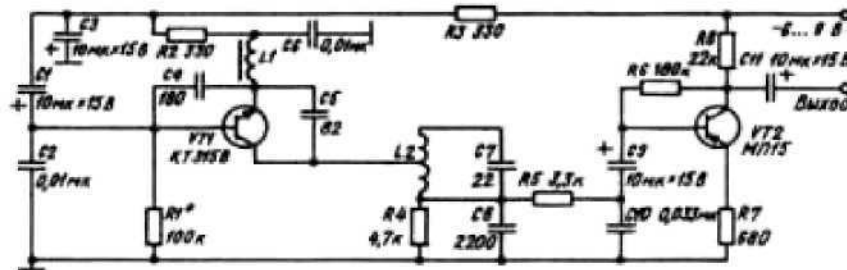


Рисунок 4.11 – Генератор шуму на надрегенеративному каскаді

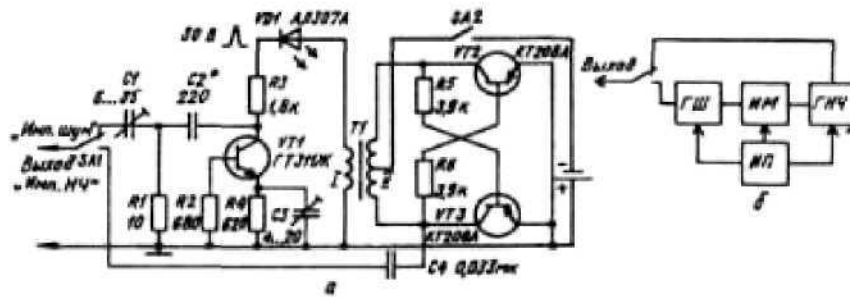


Рисунок 4.12 – Генератор шуму на мультивібраторі

Принципова схема приладу показана на рис. 4.12,а. Через світлодіод VD2 на колектор транзистора VT1 поступають модулюючі імпульси з частотою 50 – 60 Гц, що виробляються мультивібратором на транзисторах VT2 і VT3. Під час дії модулюючого імпульсу генератор на VT1 виробляє шум. Таким чином, напруга шумів виявляється промодульованою імпульсом мультивібратора. Підбором ємності коректуючого конденсатора C3 в ланцюзі емітера VT1 вирівнюють нерівномірність шумового спектру, а рівень шумів регулюють резистором R4. Імпульси НЧ з мультивібратора поступають через конденсатор C4 на перемикач SA1. Ємність атенюатора C1 служить для регулювання рівня шуму на виході приладу.

Індикатор включення - світлодіод АЛ307А служить одночасно випрямлячем напруги мультивібратора - модулятора. Джерело живлення - батарея «Крона» або будь-яка інша з напругою 7 - 10В.

Монтаж приладу виконаний друкованим методом на платі з фольгованого склотекстоліту розміром 65х25 мм. Вона розміщена в металевому корпусі – екрані.

SA1 і SA2 – мікрореле типу МП-4. Вони пов'язані з движками, встановленими на корпусі генератора. Трансформатор Т1 намотаний на сердечнику з пермалою 50НП, товщина набору 6 мм. Обмотка II містить 2х50 витків, а обмотка I – 2700 витків дроту ПЕВ-1 0,08.

Конденсатори і резистори будь-яких типів, але наскільки можливо менші за розмірами. Позначені в схемі транзистори можна замінити будь-якими іншими відповідного типа провідності, а світлодіод –

звичайним напівпровідниковим діодом.

Налагодження приладу починають з мультивібратора. Для цього в місці з'єднання резистора R3 і світлодіода VD1 підключають осцилограф і вимірюють величину модулюючого імпульсу. Вона повинна складати 30 – 40 В. Потім осцилограф під'єднують до виходу шумового генератора і перевіряють наявність шуму на всіх діапазонах. Якщо генерація на окремих частотах відсутня, підбирають опір резистора R4 і смінь конденсатора C3. нерівномірність шумового спектру коректують конденсаторами C3 і C2.

4.1.9 Простий пристрій придушення радіомікрофонів

У разі відсутності пристроїв для пошуку радіозакладок, але відомий діапазон роботи закладного пристрою, можна скористатися передавачем прицільної завади, описаного нижче, для придушення приймачів, які приймають інформацію від радіозакладок. На рис.4.13 зображена схема простого, але дуже надійного передавача завад діапазону 130 - 270 кГц з амплітудою випромінювання більше 3 В.

Передавач перешкод складається із задаючого генератора (виконаний у вигляді мультивібратора на транзисторах VT1 і VT2) і підсилювача потужності на транзисторі VT3. У ньому застосована частотна модуляція з частотою приблизно 8 Гц і девіацією близько 80 кГц. Передавач зібраний в металевій коробці розмірами 34х82 мм. Високочастотна частина схеми зібрана навісним монтажем.

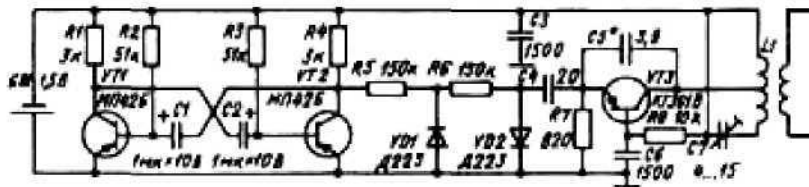


Рисунок 4.13 – Генератор прицільної завади

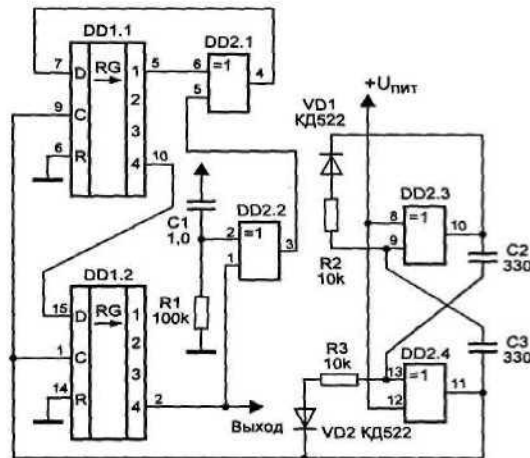
Аналогічним чином проектується пристрої постановки завад для любого заданого діапазону. Необхідно розробити задаючий генератор заданого діапазону, який забезпечить роботу всього пристрою з заданим типом модуляції. Окрім того до складу генератору такого класу необхідно включити підсилювач потужності та антену.

4.1.10 Цифровий шумовий генератор

Цифровий шум є часовим випадковим процесом, близьким по своїх властивостях до процесу фізичних шумів і називається тому псевдовипадковим процесом. Цифрова послідовність двійкових символів в цифрових генераторах шуму називається псевдовипадковою послідовністю, що є послідовністю прямокутних імпульсів псевдовипадкової тривалості з псевдовипадковими інтервалами між ними. Період повторення всієї послідовності значно перевищує найбільший інтервал між імпульсами. Найчастіше застосовуються послідовності максимальної довжини — М-послідовності, які формуються за допомогою регістрів зрушення і суматорів по модулю 2, що використовуються для отримання сигналу зворотного зв'язку.

Принципова схема генератора шуму з рівномірною спектральною щільністю в робочому діапазоні частот приведена на рис. 4. 13.

Цей генератор шуму містить послідовний восьмирозрядний регістр зрушення, виконаний на мікросхемі К561ІР2, суматор по модулю 2 (DD2.1), тактовий генератор (DD2.3, DD2.4) і ланцюг запуску (DD2.2), виконані на мікросхемі К561ЛП2.



Малюнок 4.13- Цифровий генератора шуму

Тактовий генератор виконаний на елементах DD2.3 і DD2.4 по схемі мультівібратора. З виходу генератора послідовність прямокутних імпульсів з частотою проходження близько 100 кГц поступає на входи "С" регістрів зрушення DD1.1 і DD1.2, створюючих 8-розрядний регістр зрушення. Запис інформації в регістр відбувається по входах "D". На вхід "D" регістра DD1.1 сигнал поступає з елемента зворотного зв'язку суматора по модулю 2 — DD2.1. При включенні живлення можливо стан регістрів, коли на всіх виходах присутні низькі рівні. Оскільки в регістрах М-послідовності заборонено появу нульової комбінації, то в схему введений ланцюг запуску генератора, виконаний на елементі DD2.2. При включенні живлення останній формувач на своєму виході рівень логічної одиниці, який виводить регістр з нульового стану. На подальшу роботу генератора ланцюг запуску не робить ніякого впливу. Сформований псевдовипадковий сигнал знімається з 8-го розряду регістра зрушення і поступає для подальшого посилення і випромінювання. Напруга джерела живлення може бути від 3 до 15 В.

У пристрої використані КМОП мікросхеми серії 561, їх можна замінити на мікросхеми серій К564, К1561 або К176. У останньому випадку напруга живлення повинна бути 9 В.

Правильно зібраний генератор налагодження не потребує. Зміною тактової частоти можна регулювати діапазон частот шуму і інтервал між спектральними складовими.

4.1.11 Потужний генератор завад

Схема (рис. 4.14), створена на розповсюдженій зараз в

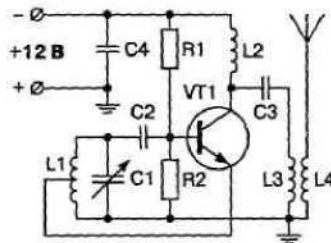


Рисунок 4.14- Потужний генератор завад

Деталі, що використані в схемі, надано нижче:

$R1 - 750 \text{ Ом}$; $R2 - 240 \text{ Ом}$; $C1 - 5 \dots 25 \text{ пФ}$; $C2 - 30 \text{ пФ}$; $C3 - 10 \text{ пФ}$; $C4 - 0,01 \text{ мкФ}$. Транзистор VT1 – КТ 904А.

Котушки мають такі параметри:

- ♦ L1 – 4 витка ПЭВ-1,0 на оправці 12 мм, відвод від середини;
- ♦ L2 – дросель 20 мкГн, (можливо використовувати від китайського приймача);
- ♦ L3 має 8 витків ПЭВ-1,0 на оправці 8 мм, намотана на оболочці кабелю РК-75;
- ♦ L4 – має 6 витків того ж проводу і на тій же оправці, розташована між 2-х половин L3.

Живлення від батарей тут не ефективне, оскільки струм живлення є більшим за 0,5 А, тому потрібний потужний блок живлення. Транзистор необхідно закріпити на тепловідводі.

У якості антени необхідно використати штир довжиною 1 м. Генератор завад починає працювати одразу і настроювань не потребує.

Опис пристрою наведено на сайті <http://www.general.pop3.ru/generato.gif>.

5 ЗАХИСТ АКУСТИЧНОГО ТА ВІБРОАКУСТИЧНОГО КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Завжди, і особливо в даний час неослабний інтерес викликає контроль мовної інформації, живої розмови. Це пов'язано з рядом специфічних особливостей, властивих саме мовній інформації і деяким рисам людської психіки:

- конфіденційністю, що припускає, що усно робляться повідомлення або віддаються розпорядження, які не можуть бути довірені ніякому носію інформації або засобу передачі;
- оперативністю, що полягає в тому, що інформація може бути перехоплена у момент її озвучування;
- віртуальністю, що полягає в тому, що, досліджуючи живу мову людини, можна зробити висновок про його емоційний стан, особисте відношенні до повідомлення, скласти психологічний портрет і т.д.

Незайве також нагадати про те, що перехоплена мовна інформація, особливо так званий первинний сигнал (мова, що не пройшла ніякої обробки), є, по суті, документом з особистим

«підписом» людини, що озвучила повідомлення, оскільки сучасні методи аналізу мови дозволяють ідентифікувати його особу.

Людська мова є шумоподібним акустичним сигналом, що несе амплітудну і частотну модуляцію. Основна енергія акустичних коливань мовного сигналу поміщена в діапазоні 70 Гц - 7 кГц, причому більше 95% смислової інформації розміщується у вузькому діапазоні - 200 Гц - 5 кГц. Акустичні коливання вище і нижче за ці частоти несуть інформацію про емоції і особу того, хто говорить (усний почерк), сприяє впізнанності і декілька підвищують розбірливість мови в умовах підвищених шумів.

Ці особливості пояснюють неослабний інтерес протиборчих сторін до безпосереднього прослуховування розмов, циркулюючих в приміщеннях, по віброакустичному і акустичному каналах. Тому питанням захисту мовної інформації приділяється першочергова увага при вирішенні питань захисту від втрат інформації по технічних каналах.

Для захисту мови від несанкціонованого прослуховування застосовуються пасивні і активні методи. Пасивні методи припускають ослаблення акустичних сигналів, циркулюючих в приміщенні, а також продуктів електроакустичних перетворень в сполучних лініях вторинних технічних засобів, що виникають як природним чином, так і в результаті ВЧ навіювання.

Активні метод передбачають створення маскуючих завад, придушення апаратів звукозапису і підслуховуючих пристроїв, а також знищення закладок.

5.1 Критерії захисту мовних повідомлень

Для кількісної оцінки необхідно виробити критерій, що встановлює співвідношення між рівнем випромінюваного в простір сигналу (електромагнітного або акустичного) і рівнем шуму на межі контрольованої зони. Критерієм оцінки безпеки мовних повідомлень при їх поширенні акустичним каналом Еб може бути характеристика розбірливості мови, яка визначається співвідношенням

$$Еб = Вм - Вш ,$$

де $Вм$ і $Вш$ відповідно середні спектральні рівні мови і шуму за

захищаючою конструкцією.

Для того, щоб мова була **нерозбірлива**, необхідно, щоб виконувалось співвідношення $E_b = -10$ дБ в спектральній смузі частот з середньгеометричним значенням 1000 Гц. Саме це може служити критерієм безпеки мовних повідомлень. Рівень, при якому виконується умова **неможливості розпізнавання ознак** мови, ще на 3 дБ нижче, ніж при розпізнаванні її сенсу, тобто $E_b = -13$ дБ.

Виходячи з цих критеріїв оглянемо методику оцінки безпеки мовних конфіденційних повідомлень, що поширюються акустичним каналом. Вона заснована на розрахунку розбірливості в кожній октавній смузі мовного діапазону, при якій неможливо буде визначити сенс повідомлення або його ознака. Процедури за оцінкою безпеки мовних конфіденційних повідомлень, циркулюючих в приміщенні, що захищається, розроблені як для однорідних, так і неоднорідних перегородок (з вікном або дверима).

5.2 Випадок використання однорідної перегородки

Початковими даними для розрахунків є характеристики матеріалу і товщини захищаючої конструкції (табл. 5.1), на підставі яких визначається коефіцієнт звукоізоляції в октавних смугах. Рівень шумів в суміжному приміщенні визначається з тих міркувань, що вони не повинні перевищувати рівнів граничних спектрів шумів (ГСШ), відповідних санітарним нормам (табл. 2).

Рівень мовного сигналу (дБ) за звукоізолюючою однорідною перегородкою визначається за формулою

$$B_{p2} = B_{p1} - Q_{\text{пер}},$$

де B_{p2} рівень мовного сигналу за звукоізолюючою перегородкою; B_{p1} рівень мовного сигналу в контрольованому приміщенні; $Q_{\text{пер}}$ – звукоізолююча здатність захищаючої конструкції. Відзначимо, що в октавних смугах з середньгеометричними частотами нижчим за 1000 Гц коефіцієнт звукоізоляції захищаючих конструкцій приймається (з фізичних міркувань) на 6 дБ нижче, а в октавних смугах з середньгеометричними частотами вище 4000 Гц

коефіцієнт звукоізоляції захищаючих конструкцій приймається на 6 дБ вище.

Таблица 5.1- Звукоізолюючі здібності деяких матеріалів і конструкцій

Материал или конструкция	Толщина, мм	Поверхностная плотность, ρ , кг/м ²	$Q_{\text{нео}}$, дБ
Материалы			
Доска сплошная сосновая	30	19,5	12
Доска сплошная дубовая	45	33,5	27
Фанера многослойная	3,2	2,54	19
Стеклопластик	3	5,1	21
Плиты из прессованной пробки	50	30	20
Железо листовое	2,0	15,6	33
Свинец	1,5	19	30
Стекло зеркальное	6,3	17,5	30
Стены и перегородки			
Стена из кирпичной кладки без штукатурки в два красных кирпича	520	884	58
Виброкирпичная панель, неоштукатуренная	140	240	49,5
Стена из пустотелого кирпича	380	-	51
Стена из железобетона	100	240	49
Гипсобетонная (гипсолитовая) плита	80	115	39,7
Перекрытия			
Несущая сплошная ж/б панель	140	336	50
Несущие ж/б плиты с круглыми пустотами	220	290	54
Окна			
Одинарное остекление без уплотняющих прокладок	3	-	22
Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом	3,3	-	42

Продовження таблиці 5.1

Материал или конструкция		Q _{пер} , дБ
Двери		
Дверь обычного типа с филёнкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см	Без уплотняющих прокладок	18
	С уплотняющими прокладками	23
Щитовая дверь из твердых древесно-волоконистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненная стекловатой	Без уплотняющих прокладок	30
	С уплотняющими прокладками	33
Та же, заполненная минеральным войлоком	Без уплотняющих прокладок	28
	С уплотняющими прокладками	32
Тяжелая дубовая дверь 90х210 см		25
Металлическая дверь (герметичная)		30

Таблица 5. 2- Рівні інтенсивності мови в октавних смугах і деякі значення граничних спектрів шумів

Номер октавы	Средняя частота, Гц	Уровни речи и предельные спектры шумов (ПСШ), дБ							
		Речь	ПСШ-25	ПСШ-30	ПСШ-35	ПСШ-40	ПСШ-45	ПСШ-50	ПСШ-55
1	250	67,9	35	40	45	49	54	53	
2	500	66,9	29	34	39	44	49	54	58
3	1000	61,5	25	30	35	40	45	50	55
4	2000	57,0	22	27	32	37	42	47	52
5	4000	53,0	20	25	30	35	40	44	50
6	6000	48,5	18	23	28	33	38	43	49
Суммарные уровни, дБ		71	36,6	41,6	47	51	60	61	65

Примітка:

ПСШ-25 кабінет з одним працюючим, ПСШ-30 бібліотека, ПСШ-35 кімната для сну і відпочинку, ПСШ-40 коридор, ПСШ-45 кабінет для розумової роботи, ПСШ-50 кабінет для мовного і телефонного зв'язку, ПСШ-55 кабінет для конторської праці.

5.3 Випадок використання неоднорідної перегородки

При розгляді як захищаюча конструкція стіни з вікном враховуються такі параметри, як кількість стекол, товщина скла, відстань між стеклами, відношення у відсотках площі вікна до площі захищаючої конструкції, товщина глухої частини захищаючої конструкції і її матеріал, характеристика вулиці (величина шуму), на яку виходить вікно.

У випадках, коли захищаюча конструкція є стіна з дверима, то враховуються наступні чинники:

- одинарні двері або подвійні;
- відстань між ними;
- відношення у відсотках площі дверей до площі всієї захищаючої конструкції;
- товщина глухої частини захищаючої конструкції і її матеріал;
- вид суміжного приміщення, куди виходять двері.

Рівень мовного сигналу за неоднорідною перегородкою $Q_{пер}$ визначається так само, як і у попередньому випадку, але звукоізолююча здатність вимагає складніших обчислень:

$$Q_{пер} = Q_1 - 10 \lg \left[1 + \frac{S_0}{S_1 + S_0} (10^{0,1(Q_1 - Q_0)} - 1) \right]$$

де Q_1 величина звукоізоляції глухої частини перегородки (без урахування вікна або дверей); Q_0 величина звукоізоляції дверей або вікна; S_1 площа глухої частини стіни; S_0 площа дверей або вікна.

Так, для поліпшення звукоізолюючих властивостей огорожуючих конструкцій необхідно зробити наступне:

- перегородки повинні бути багатошаровими, матеріали шарів підібрані з акустичними характеристиками, що різко відрізняються (наприклад, бетон-поролон), і масивними для зменшення мембранного перенесення;
- двері бажано робити подвійними з повітряним прошарком між ними і ущільнюючими прокладками;
- вікна краще робити з подвійним або потрійним склінням, застосовуючи звукопоглинальний матеріал і збільшуючи відстань між стеклами для підвищення звукоізоляції;
- вентиляційні отвори під час ведення конфіденційних розмов слід перекривати звукоізолюючими заслінками, які краще виготовляти з матеріалів з різними акустичними параметрами. При цьому потрібно прагнути досягти рівня звукоізоляції глухої стіни.

Застосування викладеної методики в декілька десятків разів зменшує вартість робіт з визначення акустичної захищеності приміщень, і це особливо важливо для невеликих фірм, де розуміють всю важливість захисту конфіденційної інформації, але не мають коштів для використання дорогої вимірювальної апаратури.

У [1] також наведено методику розрахунку захищених приміщень і є багато даних з будівельних матеріалів.

6 ЗАХИСТ ТЕЛЕФОННИХ ЛІНІЙ

Захист телефонних переговорів є одним з найважливіших завдань в загальному комплексі заходів щодо забезпечення інформаційної безпеки будь-якої організації.

6.1 Захист телефонних переговорів

Для прослуховування телефонних переговорів найчастіше використовуються електронні пристрої перехоплення мовної інформації (телефонні закладки), що несанкціоновано підключаються до телефонних ліній послідовно (у розрив одного з дротів), паралельно (одночасно до двох дротів) або за допомогою індукційного датчика (безконтактне підключення).

Одержувана телефонними закладками інформація записується на магнітний носій, в оперативну пам'ять пристрою, що запам'ятовує, або передається по радіоканалу на пункт прийому. За звичай телефонна закладка активізується тільки на час телефонної розмови.

Захист інформації, що передається телефонними лініями зв'язку, може здійснюватися на семантичному або енергетичному рівнях. На **семантичному** рівні захист інформації досягається застосуванням криптографічних методів і засобів захисту. При цьому виключається її виділення у разі перехоплення злоумисником. Методи захисту інформації на енергетичному рівні направлені на виключення або затруднення прийому супротивником інформаційних сигналів шляхом зменшення відношення сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом несанкціонованого знімання інформації.

Надалі розглянемо тільки методи захисту інформації на енергетичному рівні.

6.2 Захист інформації на енергетичному рівні. Активні методи захисту телефонних каналів

У разі захисту телефонних розмов на енергетичному рівні здійснюється придушення електронних пристроїв перехоплення інформації з використанням активних методів і засобів, до основних з яких відносяться методи:

- «синфазної» низькочастотної маскуючої завади;
- високочастотної маскуючої завади;
- «ультразвукової» маскуючої завади;
- низькочастотної маскуючої завади;
- підвищення напруги;
- пониження напруги;
- компенсаційний;
- «випалювання» телефонних закладок.

6.3 Метод «синфазної» маскуючої низькочастотної завади

Метод «синфазної» маскуючої низькочастотної завади використовується для придушення електронних пристроїв перехоплення мовної інформації, що підключаються до телефонної лінії послідовно в розрив одного з дротів або через індукційний датчик до одного з дротів. Суть методу полягає в подачі під час розмови в кожен дріт телефонної лінії узгоджених по амплітуді і фазі щодо нульового дроту електромережі 220 В маскуючих сигналів завади мовного діапазону частот (маскуючого низькочастотного шуму). Внаслідок узгодження по амплітуді і фазі в телефонному

апараті, що підключається паралельно телефонній лінії, ці завадові сигнали компенсують один одного і не приводять до спотворення корисного сигналу, тобто не погіршують якість зв'язку. У будь-яких пристроях, що підключаються до одного телефонного дроту (як послідовно, так і через індукційний датчик), завадовий сигнал не компенсується і «накладається» на корисний сигнал. А оскільки його рівень значно перевершує корисний сигнал, то перехоплення передаваної інформації стає неможливим. У ролі маскуючих завадових сигналів, як правило, використовуються дискретні сигнали (псевдовипадкові М-послідовності імпульсів) в діапазоні частот від 100 до 10000 Гц.

6.4 Метод високочастотної маскуючої завади

Метод високочастотної маскуючої перешкоди полягає в подачі під час розмови в телефонну лінію маскуючого завадового сигналу в діапазоні високих частот звукового діапазону (маскуючого високочастотного шуму). Частоти маскуючих завадових сигналів підбираються так, щоб після проходження низькочастотного підсилювача або селективних ланцюгів модулятора телефонної закладки їх рівень виявився достатнім для придушення корисного сигналу (мовного сигналу в телефонній лінії), але в той же час щоб вони не погіршували якість зв'язку. Чим нижча частота завадового сигналу, тим вище його ефективність. Звичайно використовуються частоти в діапазоні від 6-8 кГц до 12-16 кГц.

Для виключення впливу маскуючого завадового сигналу на якість зв'язку в пристрої захисту, що підключається паралельно в розрив телефонної лінії, встановлюється спеціальний фільтр нижніх частот з граничною частотою вище 3,4 кГц, який пригнічує (шунтує) завадові сигнали високої частоти (не пропускає їх у бік телефонного апарату) і не робить істотного впливу на проходження низькочастотних мовних сигналів.

В якості маскуючого шуму використовуються широкосмугові аналогові сигнали типу «білого шуму» або дискретні сигнали типу псевдовипадкової послідовності імпульсів з шириною спектру не менше 3-4 кГц.

Даний метод використовується для придушення практично всіх типів електронних пристроїв перехоплення мовної інформації, що підключаються до телефонної лінії як послідовно, так і паралельно.

Проте ефективність придушення засобів знімання інформації з підключенням до лінії послідовно (особливо за допомогою індукційних датчиків) значно нижче, ніж у разі використання методу «синфазної» маскуючої низькочастотної завади.

6.5 Метод «ультразвукової» маскуючої завади

Метод «ультразвукової» маскуючої завади в основному аналогічний розглянутому вище. Відмінність полягає в тому, що частота завадового сигналу знаходиться в діапазоні від 20-30 кГц до 50-100 кГц, що набагато спрощує схему пристрою придушення, але при цьому ефективність даного методу в порівнянні з методом високочастотної маскуючої завади погіршується.

6.6 Метод низькочастотної маскуючої завади

При використанні цього методу в лінію при покладеній телефонній трубці подається маскуючий низькочастотний завадовий сигнал. Цей метод застосовується для активізації (включення на запис) диктофонів, що підключаються до телефонної лінії за допомогою адаптерів або індукційних датчиків, що приводить до змотування плівки (заповненню-пам'яті) в режимі запису шуму, тобто за відсутності корисного сигналу.

6.7 Метод підвищення напруги

Метод підвищення напруги полягає в «піднятті» напруги в телефонній лінії під час розмови і використовується для погіршення якості функціонування телефонних закладок за рахунок переведення їх передавачів в нелінійний режим роботи. Підвищення напруги в лінії до 25-35 В викликає у телефонних закладок з послідовним підключенням і параметричною стабілізацією частоти передавача «відхід» несучої частоти і погіршення розбірливості мови. У телефонних закладок з послідовним підключенням і кварцевою стабілізацією частоти передавача спостерігається зменшення відношення сигнал/шум на 3-10 дБ. Передавачі телефонних закладок з паралельним підключенням до лінії при таких напругах у ряді випадків просто відключаються.

6.8 Метод пониження напруги

Метод пониження напруги передбачає подачу під час розмови в

лінію постійної напруги, відповідній напрузі в лінії при піднятій телефонній трубці, але зворотної полярності. Цей метод застосовується для порушення функціонування всіх типів електронних пристроїв перехоплення інформації з контактним (як послідовним, так і паралельним) підключенням до лінії, що використовують її як джерело живлення.

Розглянуті вище методи забезпечують придушення пристроїв знімання інформації, що підключаються до лінії тільки на ділянці від телефонного апарату, що захищається, до АТС. Для захисту телефонних ліній використовуються пристрої, що реалізують одночасно декілька методів придушення. На вітчизняному ринку є багатий асортимент засобів захисту.

6.9 Компенсаційний метод

Компенсаційний метод використовується для стеганографічного маскування (утаснення) мовних повідомлень, передаваних абонентом по телефонній лінії. Даний метод має високу ефективність придушення всіх відомих засобів несанкціонованого знімання інформації, що підключаються до лінії на всій ділянці телефонної лінії від одного абонента до іншого. Суть методу полягає в наступному: перед початком передачі приховуваного повідомлення по спеціальній команді абонента на приймальній стороні включається генератор шуму, що подає в телефонну лінію шумову заваду (як правило, «цифровий» шумовий сигнал) мовного діапазону частот, яка в лінії «змішується» з передаваним повідомленням. Одночасно цей же шумовий сигнал ("чистий" шум) подається на один з входів двоканального адаптивного фільтру, на інший вхід якого поступає аддитивна суміш мовного сигналу, що приймається, і маскуючого шуму. Аддитивний фільтр компенсує (пригнічує) шумову складову і виділяє приховуваний мовний сигнал (передаване повідомлення). Наявність таких пристроїв захисту у обох абонентів дозволяє організувати напівдуплексний закритий канал зв'язку.

6.10 Метод «випалювання»

Метод «випалювання» реалізується шляхом подачі в лінію високовольтних (напруга більше 1500 В) імпульсів, потужністю 15-50 ВА. Оскільки вхідні каскади електронних пристроїв перехоплення інформації і блоки їх живлення, гальванічно підключені до телефонної

лінії, то це приводить до їх електричного «випалювання». Подача високовольтних імпульсів здійснюється при відключенні свого телефонного апарату від лінії. Для знищення паралельно підключених пристроїв подача високовольтних імпульсів здійснюється у разі розімкнутої на АТС, а послідовно підключених пристроїв - у разі замкненої телефонної лінії. Основні характеристики деяких «випалювачів» телефонних закладок приведені табл.2

Таблица 2. Основные характеристики "выжигателей" телефонных закладок

Характеристики	Тип устройства		
	"Кобра"	КС- 1300	КС- 1303
Напряжение на выходе, В	1600	-	-
Мощность импульса, ВА		15	50
Режимы работы	Автоматический, ручной	Автоматический, ручной	Ручной
Время непрерывной работы в автоматическом	20 с	24 часа	-
Время непрерывной работы в ручном режиме,	10	-	-
Временные интервалы, устанавливаемые таймером	-	От 10 минут до 2 суток	-
Габаритные размеры, мм	65х170х185	170х180х70	170х180х70
Напряжение питания, В	220	220	220
Количество подключаемых телефонных линий	1	2	2

6.11 Пасивні методи захисту телефонних ліній та пристроїв

З точки зору безпеки, телефонний зв'язок має недолік, який складається у тому, що мовна інформація може бути перехоплена як у період ведення розмови, так і після сигналу «відбій». Найбільш вразливим елементом телефонного зв'язку є телефонні апарати. Вони дозволяють розміщувати в них несанкціоновані під'єднання, радіозакладні пристрої, вони самі здатні випромінювати сигнали на відстані у сотні метрів, вони

можуть стати джерелом інформації за допомогою мікрофонного ефекту та «ефекту ВЧ-нав'язування».

До пасивних методів захисту телефонних ліній та апаратів відносяться:

- амплітудне обмеження небезпечних сигналів;
- фільтрація небезпечних сигналів;
- вимкнення джерел небезпечних сигналів.

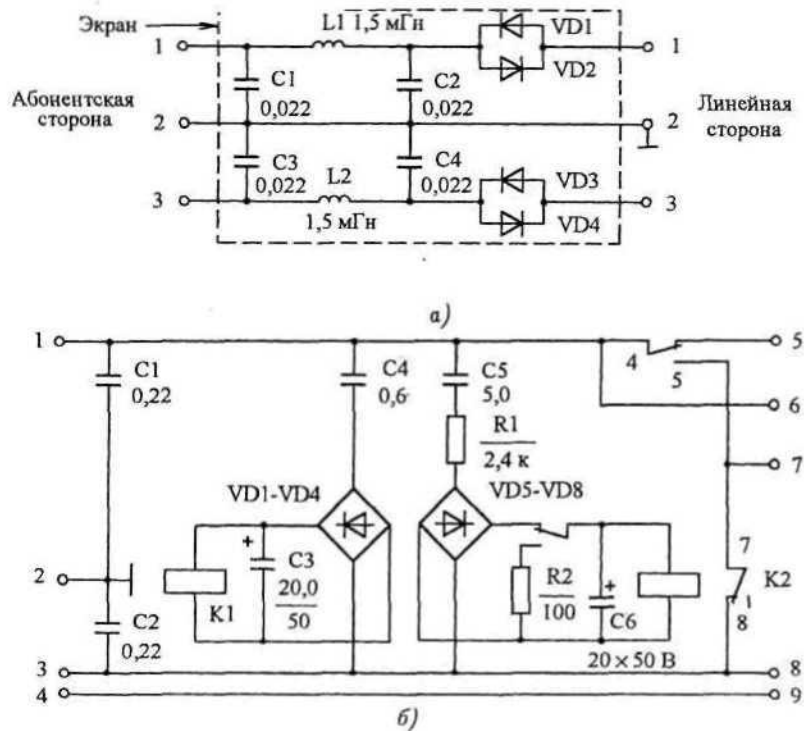


Рисунок 6.1- Схеми захисту телефонної лінії за допомогою фільтра та комутації мережі дзвінка і розмови

На рис. 6.1... наводяться схемні рішення, які практично застосовуються для пасивного захисту телефонних ліній від

мікрофонного ефекту дзвоника телефонного апарату та ефекту ВЧ-нав'язування.

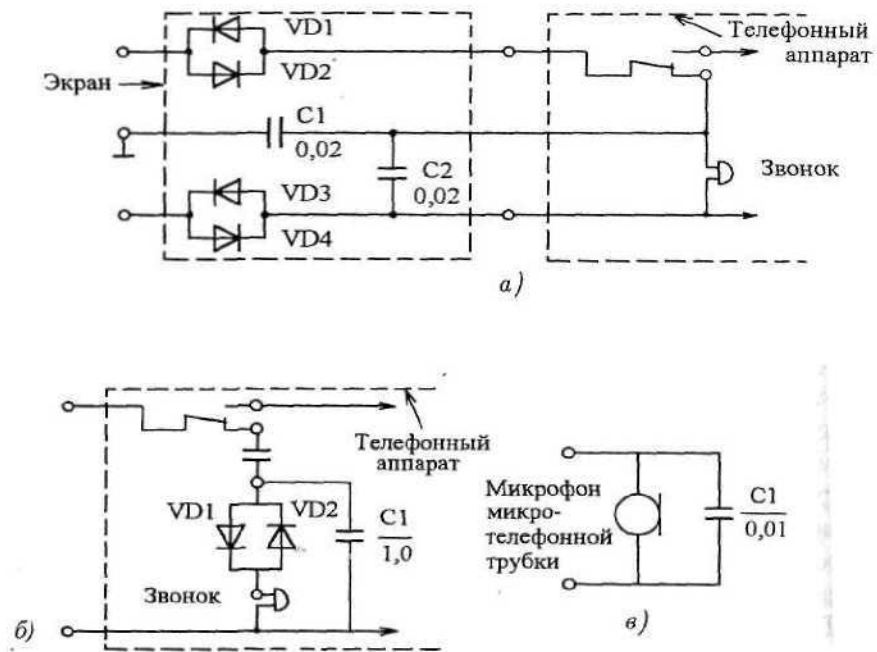


Рисунок 6.2 - Схеми захисту телефонного апарату

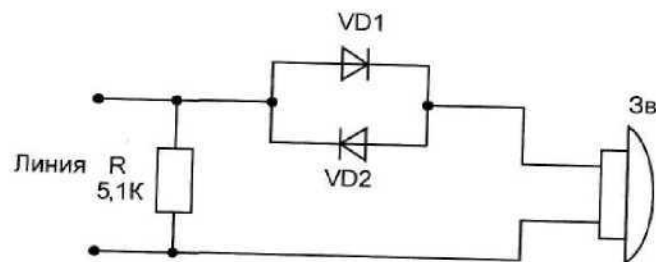


Рисунок 6.3 – Схема захисту дзвоника телефонного апарату

7 ПЕРЕДАВАЧІ ПО МЕРЕЖІ ЕЛЕКТРОЖИВЛЕННЯ 220 В

Дуже поширеним на практиці є метод несанкціонованого отримання мовної інформації або постійного контролю акустики приміщень за допомогою закладних пристроїв, які для передачі отриманої інформації використовують мережу електроживлення на ділянці від приміщення і до мережевого трансформатора.

Для таких пристроїв звичайно використовуються частоти у діапазоні від 30 кГц до 150 кГц.

Простішим рішенням цього напряму є створення генераторів ВЧ та детекторних приймачів, як то показано на рис. 7.1.

Автогенератор (рис. 1) створено за звичайною двотактною схемою. Генератор модулюється по амплітуді угольним мікрофоном ВМ1, який включено в ланцюг живлення колекторів VT2, VT3. Котушки L1...L4 розміщено в сердечниках СБ-12 або їм аналогічних. Важливо, щоб L1 та L4 були ідентичними за кількістю витків, діаметру провoda і способу намотки. L1 має 100 витків з відводом від середини. Провод — діаметром 0,1...0,15 мм. Обидві половини котушки намотуються в різних секціях каркасу, тобто, половина — в одній секції а друга половина — в іншій.

Котушка L2 має приблизно 50 витків провoda діаметром 0,1...0,15 мм и намотується поверх L1. L4 — 100 витків і намотується аналогічно L1, але без відводу. L3 — 50 витків, поверх L4.

З метою збільшення дальності дії в схемі можливо застосування підсилювач потужності для передавача і підсилювач високої частоти — для приймача. Для більш якісної модуляції можливе застосування модулятора на транзисторі або на мікросхемі, але бажано також застосувати мікрофонний компресор.

Але слід пам'ятати, що значне підвищення потужності приведе до появи завад в апаратурі, яка живиться від цієї мережі електроживлення. Не варто також використовувати частоти, вищі за 150 кГц, оскільки це може призвести до випромінювання передаваних частот.

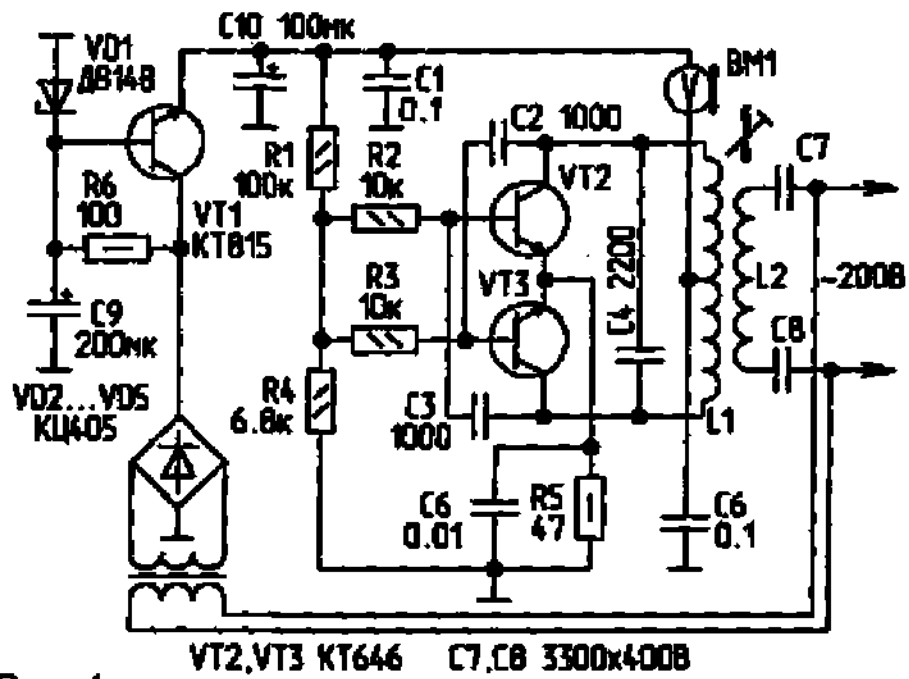


Рис. 1

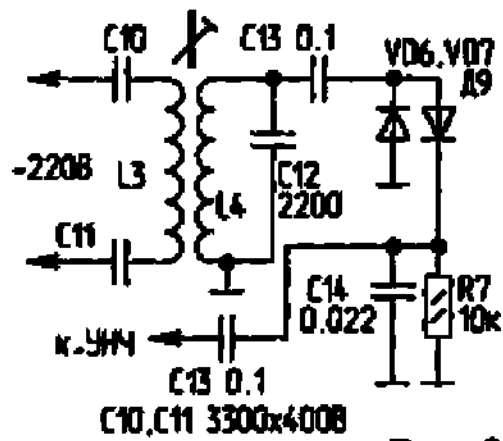


Рис. 2

Рисунок 7.1- Схеми мережєвих передавача і приймача

Ще одна схема мережевого передавача наведена на рис. 7.2. Він працює з ЧМ, а задаючий генератор виконано по оригінальній схемі на мультівібраторі на MC DD1. Робоча частота -

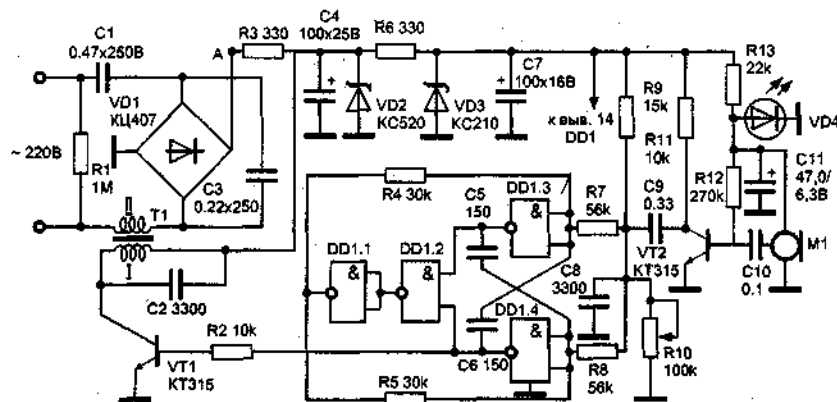


Рисунок 7.2- Мережевий низькочастотний передавач

Аналогічним чином створюються приймально-передавальні пристрої для мережі 220 В. На рис. 7.3 наведено схему мережевого приймача-передавача, який має реверсивний тракт і обидві схеми якого працюють як в режимі передавання, так і в режимі приймання. Схему виконано на поширених елементах і вона має простий принцип дії. Пристрій живиться від трансформаторного блоку живлення ± 9 В. Гучномовець ВА 1 у режимі передавання використовується у ролі мікрофону.

Основою схеми являється мікросхема фазового автопідстроювання DA1. Кнопкою S1 здійснюється переключення пристрою в режим передавання, кнопка S2 здійснює передавання тонової визивної посилки (сигналу).

На базі пристрою легко створити окремі як передавач, так і приймач, що значно спрощує схему і зменшує розміри конструкції.

В режимі приймання пристрій здатний приймати любі низькочастотні сигнали ЧМ передавачів у разі відповідного налаштування контурів L4, L5 і мікросхеми DA1 резистором R16.

Для більш стабільної роботи пристрою мікросхему ПНЧ DA2 бажано замінити наприклад на MC K174УН7 у відповідному включенні. У наведеній схемі хідні кола приймача також виконано оборотними, що дозволило звести до мінімуму кількість намоточних елементів (до двох) і застосувати лише один високовольтний конденсатор.

Каскадний підсилювач ВЧ на транзисторах VT1, VT2 має значний коефіцієнт підсилення, добру розв'язку «вхід-вихід» і не самозбуджується.

Котушки L3, L4 намотано на загальному броньованому або кільцевому сердечнику з магнітною проникністю 100 – 600. З метою підвищення електроізоляваності котушку L3 намотано монтажним ізольованим проводом і вона має 1/5 частину витків відносно котушки L4. Котушки L4 та L5 намотуються на такому ж сердечнику, мають однакову кількість витків, яка є не меншою за 50.

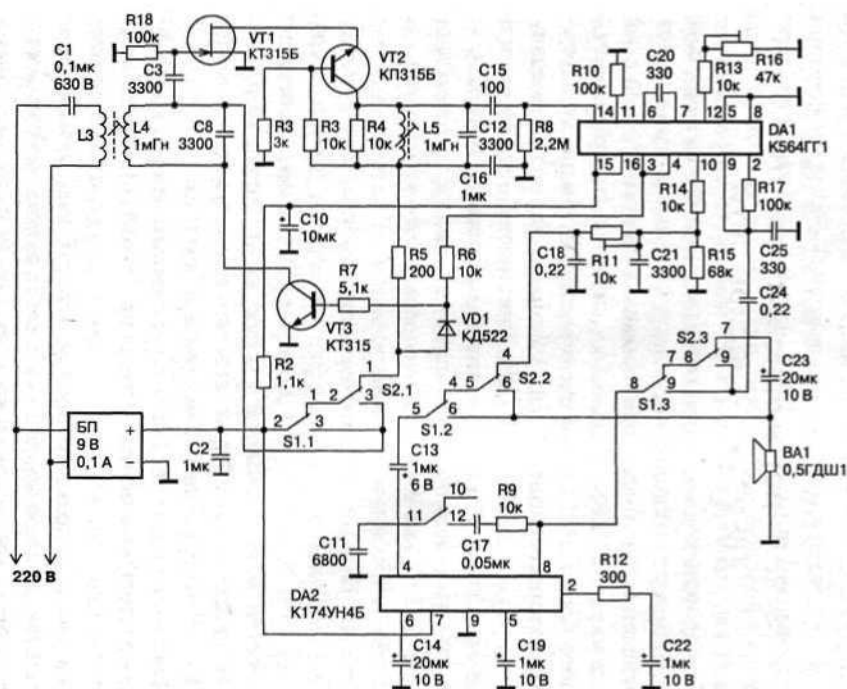


Рисунок 7.3- Мережевий приймач – передавач

На ри. 7.4 наведено схему низькочастотного ЧМ-передавача для передавання сигналу по мережі електроживлення 220 В. Живлення самої схеми забезпечується за допомогою стабілізованого блоку ± 9 В. Пристрій оздоблений схемою акустопуску. Звуковий сигнал мікрофону ВМ1 підсилюється двокаскадним підсилювачем на транзисторах VT1, VT2 після чого надходить на два каскади - генератор, і детектор акустопуску VD1, VD2.

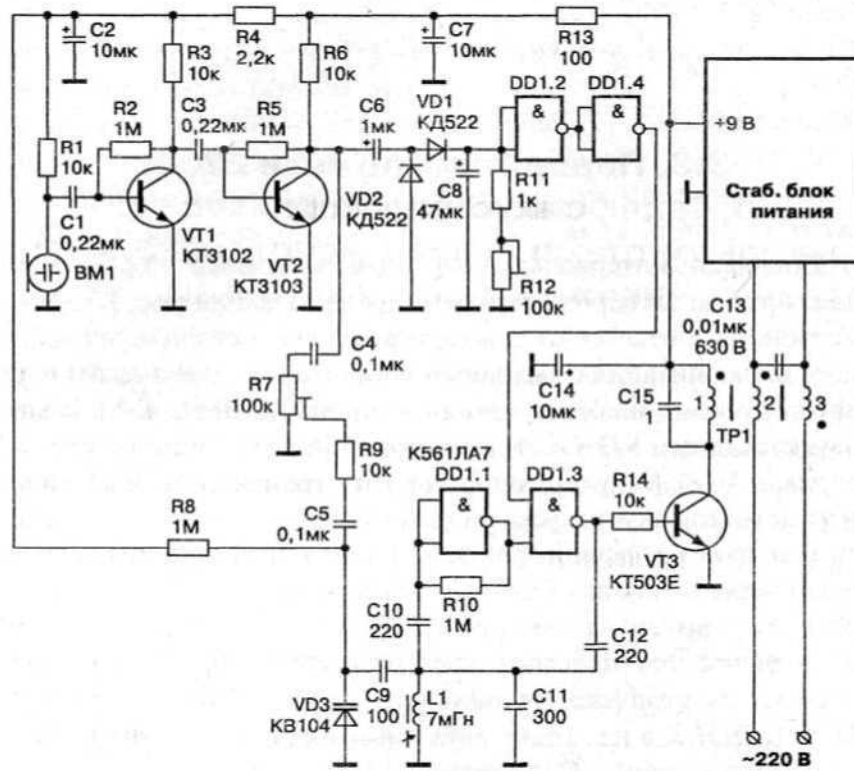


Рисунок 7.4- Мережений передавач з акустопуском

Великий коефіцієнт підсилення каналу НЧ необхідний для запуску акустопуску, поріг чутливості якого регулюється за допомогою R12. Рівень ЧМ модуляції підстроюється резистором R7. Пороговий елемент акустопуску виконано на двох КМОП-інверторах DD1.2, DD1.4, а двох інших елементах цієї мікросхеми виконано керований задаючий LC генератор. Використання LC контуру в такій низькочастотній схемі забезпечує високу стабільність частоти передавача.

Але на частоті роботи пристрою – 100 кГц – доволі важко за допомогою варикапа «розгойдати» контур до необхідного рівня модуляції.. З цією метою необхідно мати значну індуктивність контуру.

Вихідний каскад передавача виконано на транзисторі VT3. Навантаження цього транзистору є ВЧ трансформатор TP1, який передає ВЧ сигнал до електромережі.

Котушку L1 задаючого генератора намотано на броньованому феритовому сердечнику типу СБ-18, або йому подібному, з магнітною проникливістю 2000НН, який має феритовий підстроювальний сердечник. Кількість витків – 50. Для частоти роботи пристрою 100 кГц її індуктивність дорівнює 7 мГн.

Трансформатор TP1 виконується на будь-якому феритовому кільцевому сердечнику діаметром 12 – 20 мм з магнітною проникливістю 1000 – 3000. Обмотка I має 50 витків мідного проводу діаметром -,1 мм, а обмотки 2 і 3 мають по 10 витків монтажного ізолюваного проводу.

Конденсатор C15 повинний бути підібраний з врахуванням максимальної напруги на колекторі VT3.

8 ФІЛЬТРУВАННЯ НАПРУГИ ЕЛЕКТРОЖИВЛЕННЯ РЕА. БОРІТЬБА З ПЕВМІН

У сучасному світі великі об'єми інформації обробляються, зберігаються і передаються електронними методами, і, отже, супроводжуються електромагнітними випромінюваннями. Тому існує реальна можливість несанкціонованого доступу до цієї інформації.

Інформацію можна перехопити і шляхом підключення до ланцюгів електроживлення. Так, існує можливість перехоплення інформації, що відображається на моніторі комп'ютера, шляхом аналізу напруги в лінії електроживлення.

Персональний комп'ютер (ПК) є центральною ланкою в

інформаційних системах обробки інформації і знаходиться в зоні пильної уваги конкурентів, зловмисників і розвідувальних служб. Для отримання інформації використовуються всі доступні засоби, у тому числі і різні аналізатори, що підключаються до ліній електроживлення.

Технічні канали просочування інформації залежно від фізичної природи освіти і середовища розповсюдження побічних випромінювань і наведень розділяють на електромагнітні, електричні і параметричні. Електромагнітні і електричні канали просочування інформації формуються за рахунок електромагнітних випромінювань і наведень, що модулюються сигналами, що формуються в комп'ютері в процесі обробки інформації. Параметричний канал просочування інформації утворюється за рахунок зміни параметрів радіокомпонентів і елементів функціональних зв'язків (що виходять за межі контрольованої зони), які відбуваються при дії на них акустичних полів і сигналів ВЧ-нав'язування. Існує також канал просочування інформації, що утворюється за допомогою закладок (радіотрансляторів), що встановлюються безпосередньо в комп'ютер або в ланцюгах електроживлення.

В даний час на ринку засобів обчислювальної техніки доступні вироби в загальнопромисловому виконанні із зарубіжними і вітчизняними сертифікатами, підтверджуючими, що ці вироби задовольняють вимогам діючих норм на рівні електромагнітного випромінювання. Як правило, маються на увазі медичні норми або норми по забезпеченню електромагнітної сумісності засобів. Для забезпечення захисту інформації дотримання вказаних норм виявляється недостатнім.

У загальному випадку джерела ПЕМВІН, середовище і шлях їх розповсюдження однозначно і нероздільно фізично пов'язані з елементами комп'ютера, що здійснюють зберігання, обробку або передачу інформації, а також з паразитними контурами ланцюгів електроживлення і заземлення.

Побічні електромагнітні випромінювання і наведення (ПЕМВІН) можна розглядати як радіотехнічні відходи процесів обробки інформації і формування допоміжних сигналів управління і індикації. При цьому всі ці процеси супроводжуються виникненням коливань на комбінаційних частотах і різного роду шумами. Випадковий характер утворення побічних коливань не дозволяє

однозначно визначити спосіб гарантованого їх придушення, тобто в цьому випадку присутній імовірнісний підхід. Сформулюємо тільки деякі практичні рекомендації по зниженню впливу цих процесів на параметри каналів просочування інформації.

Дослідимо систему електроживлення ПК в загальнопромисловому виконанні, тобто те, що пропонується на комп'ютерному ринку. Для електроживлення ПК використовують промислову мережу змінної напруги 220В, 50Гц.

Система електроживлення ПК вирішує наступні задачі:

- формування необхідних стабілізованих постійних напруг;
- фільтрацію індустриальних завад;
- захист споживачів електроенергії від перевантажень і т.д.;

Типова структурна схема електроживлення комп'ютера представлена на рис. 8.1.

На цьому малюнку:

ИБП - джерело безперебійного живлення (ДБЖ);

П - перетворювач змінної напруги 220В в постійну 12В;

АС - акустична система.

Первинними і загальними пристроями електроживлення для комп'ютера є мережевий фільтр і ДБЖ, а розподіл електроживлення для окремих пристроїв здійснюється по наступній схемі:

- сканер, акустична система і TFT монітор споживають електричну енергію через відповідні перетворювачі змінної напруги в постійні 12В, конструктивно виконані як автономні пристрої (адаптери);

- принтер одержує електроживлення безпосередньо від первинної мережі через фільтр або від ДБЖ (джерела безперервного живлення);

- пристрої системного блоку (НЖМД, НГМД, CD-ROM, материнська плата, відео і інші карти), клавіатура і миша одержують електроживлення від мережі ~220В 50Гц через багатоканальний блок вторинного живлення, вбудований в корпус системного блоку, тобто що знаходиться в одному конструктиві з пристроями обробки і зберігання інформації.

З практики проектування виробів з нормованими рівнями випромінювань відомо, що необхідно прагнути мінімізувати паразитні контури і виключити їх взаємний вплив. Як же ці питання вирішені в типовій схемі електроживлення ПК?

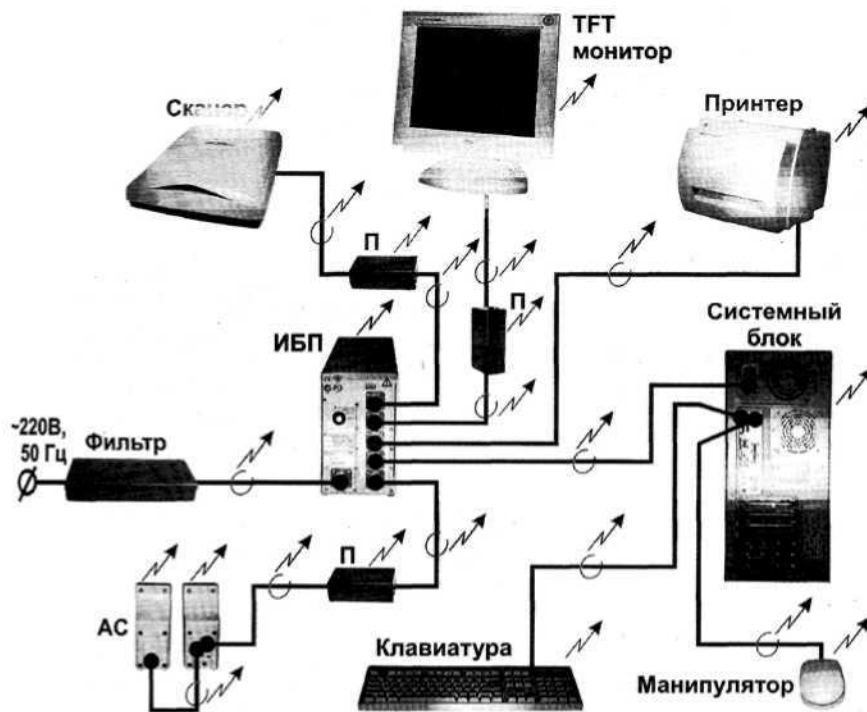


Рисунок 8.1- Типова схема електроживлення ПК

1. Автономні перетворювачі змінної напруги в постійне створюють додаткові паразитні контури, такі як: первинна мережа - вхід адаптера, вихід адаптера - навантаження; а вбудовані перетворювачі: первинна мережа - перетворювач - навантаження.

2. Наявність загальної крапки (мережевий фільтр або ІБП) в схемі розподілу електроживлення для всіх пристроїв ПК створює умови для взаємного проникнення побічних коливань від одного пристрою в інші, наприклад, від принтера до монітора і навпаки, не тільки шляхом випромінювання і наведень, але і безпосередньо по ланцюгах електроживлення.

3. Загальне багатоканальне джерело вторинного

електроживлення для пристроїв системного блоку перетворює завдання розділення паразитних контурів практично у важковирішувану проблему.

Слід звернути увагу на вельми істотну особливість в електроживленні лазерного принтера. При підготовці до друку принтер споживає з мережі струм в 5-10 разів більше вказаного в паспорті, тому принтер підключають тільки до транзитного (білого) рознімання ДБЖ, а якщо такий відсутній, то безпосередньо до первинної мережі або до виходу мережевого фільтру. Таким чином, ланцюг електроживлення принтера утворює додатковий паразитний контур.

Окремого розгляду заслуговує блок вторинного електроживлення системного блоку як джерело побічних електромагнітних коливань. Завади від блоків вторинного електроживлення створюються побічними випромінюваннями, що виникають в процесі роботи блоку живлення. Ці випромінювання можуть бути промодульовані сигналами, що формуються в процесі обробки інформації, або мовною інформацією. В цьому випадку їх можна перехопити і виділити інформацію, що міститься в ній. Розглянемо тільки ті види перешкод, які мають пряме відношення до формування каналів просочування інформації по ланцюгах електроживлення.

Джерело безперервного живлення (ДБЖ) є загальним для периферій -них пристроїв і системного блоку і одержує електроживлення безпосередньо від первинної мережі, отже, всі паразитні контури від різних пристроїв мають загальну крапку, яка по ланцюгу первинного електроживлення сполучена з пристроями за межами контрольованої зони.

Таким чином, перераховані особливості схеми електроживлення комп'ютера, а, саме, неоптимізована кількість паразитних контурів, наявність у них загальної крапки, що забезпечує взаємний обмін електромагнітними коливаннями, і різноманіття видів паразитних коливань джерела вторинного живлення створюють умови для формування технічних каналів просочування інформації.

На основі вищевикладеного приходимо до висновків, що ланцюги електроживлення комп'ютера і периферійних пристроїв можуть утворювати канали просочування інформації двох видів:

1. Ненавмисно утворювані за рахунок:

- побічного електромагнітного випромінювання ланцюгами електроживлення і пристроями комп'ютера;
- безпосередньої зміни струмів, напруг, фаз і т.д. в первинній мережі електроживлення адекватного кодовим представленням інформації, що обробляється в комп'ютері.

2. Спеціально організовані:

- шляхом контактного введення сигналів ВЧ-нав'язування в ланцюги електроживлення і заземлення з подальшим прийомом відбитих сигналів промодульованих інформаційними сигналами;
- мережевими закладними пристроями, які транслюють по радіоканалу інформаційні сигнали.

До традиційних рішень по захисту інформації відносяться:

- екранування, як спосіб ослаблення ПЕВМІН;
- використання автономних джерел електроживлення для забезпечення гальванічної розв'язки з промисловою мережею;
- установка мережових фільтрів для придушення побічних коливань, проникаючих в мережу електроживлення за рахунок кондуктивних зв'язків;
- активний метод - зашумлення (створення маскуючих завад) в просторі і дротах.

Екранування і автономні джерела електроживлення як і раніше знаходять достатньо широке застосування, оскільки забезпечують гарантований надійний захист інформації з обмеженим доступом.

Активний метод, бажано застосовувати в обмежених масштабах, оскільки він: екологічно «брудний» (забруднює ефір і мережу електроживлення), біологічно шкідливий для здоров'я людини, не забезпечує гарантованого захисту в широкому діапазоні частот і є демаскуючою ознакою об'єкту. Мережеві фільтри останніми роками зазнали істотну зміну як з погляду конструктивних і схематичних рішень, так і варіантів їх застосування. У рекомендаціях основна увага приділяється важливості обліку імпедансу для забезпечення стабільних характеристик придушення побічних коливань.

Загальні рекомендації по проектуванню фільтрів вимагають звернути особливу увагу на створення основного елементу фільтру - дроселя, а саме :

- вибору типу дроселя;
- вибору магнітопроводу;
- вибору напрямку намотування обмоток;

- вибору технології виготовлення обмоток;
- технології виготовлення дроселя;

Необхідно з позиції запобігання просочуванню інформації задовольнити умові, при якій результуючий опір дроселя змінний напрузі електромережі буде рівний активному опору обмотки дроселя, що досягається при виконанні умови $I_{пр} = I_{обр}$ і *рівності індуктивностей обмоток*.

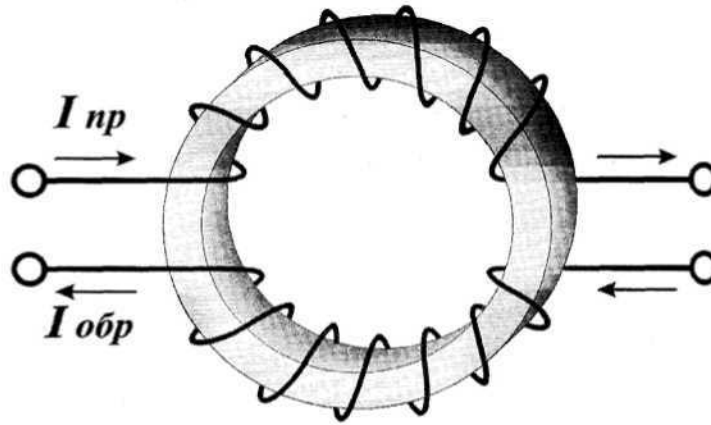
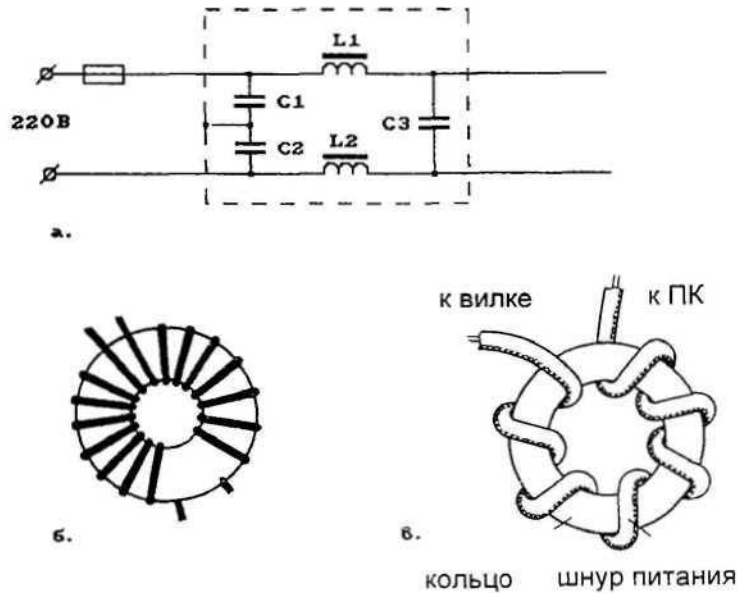


Рисунок 8.2 – Схема дроселю

Вирівнювання індуктивностей обмоток досягається вимірюванням їх значень вимірювачем RLC і зменшенням кількості витків однієї з обмоток до отримання значення, рівного меншій індуктивності

Для виключення переміщення витків обмоток від зовнішніх дій необхідно передбачити заливку дроселя, наприклад, епоксидним компаундом. Так забезпечується виключення прояву мікрофонного ефекту в дроселі при дії на нього акустичних полів і зниження параметричних властивостей для сигналів ВЧ-нав'язування.

З метою зниження рівнів електромагнітних випромінювань, які проникають в мережу електроживлення, дросель слід встановлювати в екранованому відсіку, а монтаж всіх компонентів фільтру виконувати згідно рекомендаціям. Правильний вибір мережевого фільтру або виготовлення фільтру власної оригінальної конструкції не завжди дає позитивні результати при рішенні задач захисту інформації. За інших рівних умов на ефективність захисту робить великий вплив спосіб під'єднання мережевого фільтру до навантаження.



а- LC – ВЧ фільтр; б- індуктивний фільтр; в- простий ВЧ- фільтр

Рисунок 8.3 – Приклади ВЧ-фільтрації в мережах електроживлення

Розглянемо наступні варіанти:

1. Колективна організація фільтрації електроживлення - коли один мережевий фільтр забезпечує декілька однорідних або таких, що трохи відрізняються, споживачів.
2. Індивідуальна фільтрація електроживлення для кожного споживача, яка може бути виконана по схемі:

2.1. фільтр, розміщений в конструктиві навантаження, тобто він є вузлом комп'ютера;

2.2. фільтр тільки для одного навантаження, тобто, як автономний виріб;

2.3. декілька фільтрів, об'єднаних в одному багатосекційному екранованому конструктиві, де кожне навантаження одержує відфільтроване електроживлення від фільтру автономно екранованої секції, тобто виключається можливість взаємного проникнення побічних коливань і знижується рівень випромінювань. У цих секціях розміщені і перетворювачі змінної напруги 220В 50Гц в постійне 12В.

Варіант 1. Колективна організація фільтрації електроживлення з-за наявності загальної точки підключення різних і різномірних споживачів не завжди задовольняє нормативним вимогам захисту інформації. Недоліки - наявність загальної точки для всіх паразитних контурів і зміна якості захисту інформації від кількості споживачів (чим менше споживачів, тим вище якість).

Варіант 2.1. За певних умов може задовольняти вимогам по реалізації функції захисту інформації, але не завжди його можна реалізувати в корпусах покупних виробів. Найбільш він підходить для технічних засобів, що знов розробляються. Недолік - не завжди конструктивна сумісність з виробом.

Варіант 2.2. По реалізації . функцій захисту інформації задовольняє вимогам, але основним недоліком є кількість фільтрів, яка дорівнює кількості пристроїв, і розгалужена кабельна система при організації електроживлення навіть для одного персонального комп'ютера.

Варіант 2.3. Вільний від вищеназваних недоліків і має високі показники по запобіганню просочуванню інформації по технічних каналах, що утворюються по мережі електроживлення.

Ефективним способом зниження рівнів ПЕМВІН є екранування ланцюгів електроживлення, вузлів комп'ютера і периферійних пристроїв у тому числі і від радіозакладок. При цьому слід враховувати, що для досягнення необхідних показників ослаблення випромінювань необхідне нормативне рішення задач по заземленню екранів, з метою виключення утворення паразитних контурів і зменшення рівнів побічних випромінювань, що виникають при одночасно працюючих пристроях (наприклад, на комбінаційних частотах).

Проте, у зв'язку з тим, що електроживлення ПК зарубіжного виробництва вимагає трьохпровідної системи: фаза-нуль-земля, а традиційно виконана вітчизняна розводка має тільки фазу і нуль, слід запам'ятати, що забороняється використовувати як заземлюючі пристрої нульові фази електромереж, металоконструкції будівель, сполучені із землею, металеві оболонки підземних кабелів, металеві труби систем опалювання, водопостачання і т.д.

Кабелі електроживлення необхідно розміщувати в екранованих конструктивах типу металевих рукавів, труб, коробів, що дозволить виключити або значно зменшити взаємні паразитні наведення від різних споживачів електроенергії і понизити рівні випромінювань від розсереджених джерел. Таким чином, буде створений загальний екранований об'єм для системи електроживлення комп'ютера і всіх периферійних пристроїв, що обробляють інформацію з обмеженим доступом. Ступінь ефективності вжитих заходів по запобіганню просочуванню інформації залежатиме в основному від якості виготовлення і монтажу екрануючих конструктивів, вибраних систем електроживлення і заземлення.

ЗАКЛЮЧЕННЯ

Ці методичні вказівки не в змозі висвітлити всі питання можливої тематики курсових проектів, тому студентам необхідно творчо підходити до запропонованої або обраної теми курсового проекту. Любий курсовий проект обов'язково повинний містити розділ електричних розрахунків блоків, вузлів, каскадів. У цьому розділі студенти виявляють свою здатність з виконання розрахунків конкретного пристрою, який використовується для завдань захисту інформації.

ЛІТРАТУРА

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие.-М.:Горячая линия-Телеком, 2005.-416с.
2. Максимов Ю.Н., Сонников В.Г., Петров В.Г., Паршутин А.В., Еремеев М.А. Технические методы и средства защиты информации – С-Пб.: Полигон, 2000. – 314 с.
- 3.Конахович Г.Ф. и др. Защита информации в телеком - муникационных системах.- К.: «МК-Пресс», 2005.- 288с.

4. Конструкции СВЧ устройств и экранов: Учебное пособие для вузов / Под ред. А.М.Чернушенко. – М.: Радио и связь, 1983. – 400 с.
5. Гроднев И.И. Электромагнитное экранирование в широком диапазоне частот. – М.: Связь, 1972. – 251 с.
6. Акустика: Справочник / Ефимов А.П., Никонов А.В., Сапожков М.А., Шоров В.И. / Под ред. М.А.Сапожкова 2-изд. перераб. и доп. – М.: Радио и связь, 1989. – 336 с.
7. Сапожков М.А. Электроакустика: Учебник для вузов. – М.: Связь, 1978. – 272 с.
8. Сапожков М.А. Звукофикация помещений: Проектирование и расчет. – М.: Связь, 1979.
9. Лагутин В.С., Петряков А.В. Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1996. – 304 с.
10. Петряков А.В., Лагутин В.С. Защита абонентского телетрафика. – М.: Радио и связь, 2001. – 504 с.
11. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации / Под. ред. Ю.С. Ковтаниюка. – К.: Издательство Юниор, 2003. – 504 с.
12. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие – М.: Гостехкомиссия России, 1998. – 320 с.
13. Торокин А.А. Основы инженерно-технической защиты информации – М.: Ось-89, 1998. – 336 с.
14. Домарев В.. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004.- 992 с.
15. Энциклопедия промышленного шпионажа/ Ю.Ф.Которин, Е.В.Куренков, А.В.Лысов, А.Н.Остапенко. – С-Пб. : Полигон, 1999. – 512с.

Додаток А

Зразок оформлення титульної сторінки пояснювальної записки

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Запорізький національний технічний університет

Кафедра захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО КУРСОВОГО ПРОЕКТУ

з дисципліни

„Фізико-технічні методи захисту інформації”

на тему

ЗАХИСТ АКУСТИКИ ВИДІЛЕНИХ ПРИМІЩЕНЬ

Розробив
ст.гр. РП-716

Петров В.С.

Керівник
ст. викладач

Клочко В.В

2008