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
«____» _____ 2021 р.

# МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «ДОСЛІДЖЕННЯ ШЛЯХІВ ПРОТИДІЇ ЗАСТОСУВАННЮ ЗАСОБІВ МОБІЛЬНОГО ЗВ'ЯЗКУ ВІД НЕСАНКЦІОНОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ»

студент групи СЗДМ-61 Калюжний Олександр Едуардович _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2021 р.

# ЗАВДАННЯ

**на атестаційну роботу магістра**

студенту: Калюжному Олександру Едуардовичу

**1. Тема роботи:** «Дослідження шляхів протидії застосуванню засобів мобільного зв'язку від несанкціонованої передачі інформації»,
затверджена наказом по університету від «  » 2021 р. за № .

**2. Термін здачі** студентом оформленої роботи « 18 » грудня 2021 р.

**3. Об’єкт дослідження:** процес захисту акустичної інформації.

**4. Предмет дослідження:** напрями захисту інформації від витоку радіоканалом.

**5. Мета роботи:** підвищити систему протидії витоку мовної інформації через мобільні телефони стандарту GSM.

**6. Перелік питань, які мають бути розроблені:**

1. загрози мовній інформації на підприємстві;
2. методи захисту мовної інформації;
3. дослідити систему протидії на основі генератора радіозавад.

**7. Перелік публікацій:**

**8. Перелік ілюстративного матеріалу.** Презентація виконана на слайдах для подання за допомогою світлопроекторів та комп’ютерних засобів.

**9. Дата видачі завдання** «____» _____ 2021 р.

**Науковий керівник** _____ Пепа Ю.В.

(підпис)

**Завдання прийняв до виконання** _____ Калюжний О.Е.

(підпис)

# КАЛЕНДАРНИЙ ПЛАН

**Дата видачі завдання** «____» _____ 2021 р.

| № з/п | Назва етапів дипломної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Огляд літератури | до 30.09.21 р. | виконано |
| 2 | Написання першого розділу роботи | до 10.10.21 р. | виконано |
| 3 | Написання другого розділу роботи | до 20.11.21 р. | виконано |
| 4 | Написання третього розділу роботи | до 10.11.21 р. | виконано |
| 5 | Написання четвертого розділу роботи | до 20.11.21 р. | виконано |
| 6 | Оформлення атестаційної роботи | до 10.12.21 р. | виконано |
| 7 | Підготовка демонстраційних матеріалів | до 18.12.21 р. | виконано |

**Студент:** СЗДМ - 61 Калюжний О.Е. _____
(підпис)

**Науковий керівник:** к.т.н., доц. Пепа Ю.В. _____
(підпис)

**Нормоконтроль:** Гребенніков А.Б. _____
(підпис)

# РЕФЕРАТ

Атестаційна робота містить: 76 сторінок, 22 рисунки, 1 таблицю.

Несанкціоновані дії з акустичною інформацією призводять до витоку важливої конфіденційної інформації. Для проведення таємних і важливих нарад на підприємстві велика увага надається засобоам захисту інформації, з метою запобігання втрат. Тому підвищення ефективності систем захисту інформації від витоку технічними каналами є важливою задачею.

**Мета роботи –** підвищити систему протидії витоку мовної інформації через мобільні телефони стандарту GSM.

**Завдання дослідження:**

- розглянути загрози акустичній інформації;

- проаналізувати існуючі методи та засоби захисту від витоку акустичної інформації;

- запропонувати генератор радіозавад для мобільних телефонів стандарту GSM.

**Об’єкт дослідження –** процес захисту акустичної інформації.

**Предмет дослідження –** напрями захисту інформації від витоку радіоканалом.

**Методи дослідження:** аналітичні, порівняння та системного аналізу.

Проведені дослідження рівня небезпеки від витоку акустичної інформації на підприємстві через мобільні телефони та запропоновано застосувати багатофункціональний генератор радіочастотного шуму.

Галузь використання – кібербезпека.

**Ключові слова:** ГЕНЕРАТОР ШУМУ, ВТРАТА ІНФОРМАЦІЇ, ПОСТАНОВНИК РАДІОЗАВАД, ЗАГРОЗА ІНФОРМАЦІЇ, ВИТІК ІНФОРМАЦІЇ.

# ABSTRACT

The thesis contains 76 pages, 22 drawings, 1 table.

Unauthorized actions with acoustic information lead to the leakage of important confidential information. To hold secret and important meetings at the enterprise, much attention is paid to information security, in order to prevent losses. Therefore, improving the efficiency of information leakage protection systems through technical channels is an important task.

**The purpose of the work** to increase the system of counteracting the leakage of voice information through GSM mobile phones.

**Objectives of the study:**

- consider threats to acoustic information;

- to analyze existing methods and means of protection against leakage of acoustic information;

- to offer a radio interference generator for GSM mobile phones.

**Objectives of the study** is the process of protection of acoustic information.

**Object of study –** areas of protection of information from leakage by radio.

**Research methods:** analytical, comparison and systems analysis.

Researches of the level of danger from leakage of acoustic information at the enterprise through mobile phones are carried out and it is offered to apply the multipurpose generator of radio frequency noise.

Area of application - cybersecurity.

**Key words:** NOISE GENERATOR, LOSS OF INFORMATION, STATION OF RADIO FACTORIES, THREAT OF INFORMATION, LEAK OF INFORMATION.

**ЗМІСТ**

# ВСТУП

Відомо, що інформація має цінність в залежності від її змісту та актуальності. Тому, зрозуміло, що певна категорія людей буде зацікавлена в перехопленні та несанкціонованому одержанні такої інформації. Це призводить до того, що таку інформацію необхідно захищати.

Для надійного захисту інформації на підприємствах від витоку її технічними каналами необхідно побудувати системи захисту інформації для об’єкта інформаційної діяльності.

В дипломі основна увага приділена розробці пристрою для придушення радіосигналів від мобільних телефонів стандарту GSM та методам протидії перехоплення інформації від витоку через радіоканал.

На будь-якому підприємстві постає питання побудови комплексної системи захисту інформації, але особливу увагу слід приділити захисту від витоку інформації технічними каналами витоку інформації та проведенню інженерно-технічних заходів щодо захисту такої інформації.

Також слід зазначити, що вирішальну роль під час дипломного проектування займає розробка та виготовлення експериментального пристрою для придушення радіосигналів від мобільних телефонів стандарту GSM, що працюють в зоні дії цього пристрою.

Проведені досліди та вимірювання рівня завадового сигналу від такого пристрою на певних відстанях і визначена зона ефективної дії. Такий пристрій можна застосовувати, як елемент захисту від витоку інформації в приміщеннях через радіоканал в частотному діапазоні 890-1912 МГц через мобільні телефони та обмежити використання мобільних телефонів під час нарад.

Окремо в дипломі наведено нормативно-правову базу в сфері захисту інформації в Україні.

# 1 КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

## 1.1 Огляд каналів витоку інформації

Фізичні процеси, які виникають в технічних пристроях і системах при їх функціонуванні, створюють в навколишньому середовищі побічні електромагнітні, акустичні та інші види випромінень, які в тій чи іншій мірі пов'язані з переробкою інформації. Ці випромінювання можуть знаходитися на досить великих відстанях і, в слідстві, використовуються для несанкціонованого зняття інформації. Сторонні ЕМІ виникають в слідстві непередбачених схемою чи конструкцією розглянутого технічного засобу по паразитним зв'язкам напруги, струму чи магнітного поля. В залежності від фізичної природи елементів паразитних електричних кіл розрізняють:

- паразитний зв'язок через загальний повний опір;
- ємкісний чи індуктивний паразитний зв'язок.

Під паразитним зв'язком розуміють зв'язок по електричним чи магнітним колам, які з'являються незалежно від бажання конструктора.

Джерелами випромінювань в технічних каналах являються технічні засоби, в яких циркулює конфіденційна інформація. Такими засобами можуть бути:

- мережі електроживлення та лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи телеграфного та факсимільного зв'язку;
- засоби гучномовного зв'язку ;
- системи посилення звуку і відеозапису;
- електронно-обчислювальна техніка;
- пожежно-охоронна сигналізація.

Джерелом випромінення технічних каналів витоку інформації може бути і голосовий тракт людини, викликаючи появлення акустичних випромінень в приміщенні чи поза ним.

Канали витоку інформації – це сукупність носія інформації, середовища розповсюдження і засобів розвідки.

Технічні канали витоку інформації поділяються на:

- РАДІОКАНАЛИ – електромагнітні випромінювання радіодіапазону;

- ЭЛЕКТРИЧНІ – напруга і струм в струмопровідних комунікаціях;

- АКУСТИЧНІ – розповсюдження звукових коливань в будь-якому звукопровідному матеріалі;

- ОПТИЧНІ – електромагнітні випромінювання в інфрачервоний, видимій і ультрафіолетовій частині спектру;

- МАТЕРІАЛЬНО-РЕЧОВІ – папір, фотографії, магнітні носії.

Основна увага в даній роботі приділяється радіоканалам, акустичним та матеріально-речовим каналам.

Основними джерелами виникнення технічних каналів витоку інформації є:

- акустичні перетворення фізичних величин;

- випромінювачі електромагнітних коливань;

- паразитні зв’язки і наводки на дроти і елементи електронних пристроїв.

Випромінювачі електромагнітних коливань.

Випромінювачі електромагнітних коливань поділяються на:

- низькочастотні;
- високочастотні;
- оптичні.

Низькочастотні випромінювачі.

Низькочастотними випромінювачами електромагнітних коливань є звукопідсилюючі пристрої будь-якого функціонального призначення і конструктивного виконання. У зоні таких пристроїв найбільш сильними є магнітне поле небезпечного сигналу (сигналу, який несе секретну інформацію).

Високочастотні випромінювачі.

До високочастотних випромінювачів належать:

- ВЧ автогенератори;
- модулятори високочастотних коливань і пристрої, що генерують

паразитні ВЧ коливання.

Джерелами небезпечного сигналу є:

- ВЧ генератори радіоприймачів, телевізорів, обчислювальних генераторів;
- монітори ЕОМ.

Модулятори ВЧ коливань, як елементи які мають нелінійні характеристики створюють нелінійні складові ВЧ характеру.

В колі технічних засобів, які знаходяться в зоні дії сильних ВЧ випромінювань наводяться сигнали напругою від одиниць до десятків вольт. Якщо в даних колах знаходяться елементи, параметри яких змінюються під дією низькочастотних сигналів, то в навколишньому середовищі буде створюватися вторинне поле ВЧ випромінювання, яке модулюється низькочастотним сигналом. В якості нелінійних елементів можуть бути телефони, датчики охоронної і пожежної сигналізації, приймачі та магнітоли. Оптичні випромінювачі.

В волоконних світловодах існує три типа хвилі:

- направляючі – основний тип хвилі;
- випромінюючі – виникають при вводі світла в світловод, і певна частина енергії вже на початку лінії випромінюється;
- витікаючі – частково поширюються вздовж світловода, а частково переходять в оболонку, поширюються там і виходять назовні.

Причини виникнення випромінювань:

- радіальна неузгодженість;
- кутова неузгодженість;
- наявність зазору;
- взаємна непаралельність торців стику;
- різниця в діаметрі.

Фізичні перетворювачі.

В будь-яких технічних засобах існують ті чи інші фізичні перетворювачі, які виконують відповідні їм функції, які засновані на певному фізичному

принципі дії (рис.1.1).

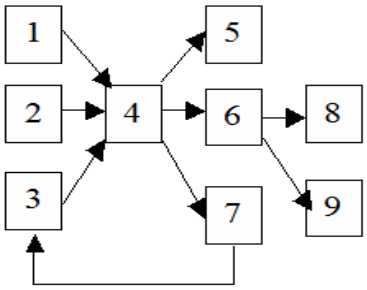


Рисунок 1.1. Принцип дії перетворювача:

1 - наводка ЕМВ (нав'язування); 2 - акустична дія; 3 - позитивний зворотній зв'язок; 4 - перетворювач, елемент, пристрій; 5 – побічні випромінювання; 6 - витік; 7 - паразитна генерація; 8 – в колі живлення; 9 – в колі заземлення

Перетворювачем є пристрій, який трансформує зміни однієї фізичної величини в іншу. Кожен перетворювач діє на окремих фізичних принципах і створює належний цим принципам технічний канал витоку інформації.

Перетворювачі характеризуються набором параметрів:

1. Чутливість – відношення зміни величини вихідного сигналу до зміни сигналу на його вході;

2. Роздільна здатність – найбільша точність, з якою виконується перетворення;

3. Лінійність – рівномірність зміни вихідного сигналу в залежності від зміни вхідного;

4. Інертність (чи час відклику), яка дорівнює часу встановлення вихідного сигналу у відповідь на зміну вхідного;

5. Смуга частот – показує, на яких частотах дії сигналу приймається перетворювачем, створений на виході допустимий рівень сигналу.

Для перетворення інформації про фізичні явища в форму електричного сигналу в електричних системах існують чутливі елементи – датчики. Датчики є початком будь-якої електричної системи. Існує два види датчиків: спеціально розроблені та випадково виниклі.

За фізичною природою перетворювачі поділяють на наступні групи:

- фотоелектричні;
- термоелектричні;
- п’єзоелектричні;
- електромагнітні;
- акустичні.

### 1.2 Акустичний канал витоку інформації

Переносником інформації є мова, шум, звуки, що лежать у смузі від ультра (більше 20 кГц) до інфразвукового діапазону.

За рахунок поширення механічних коливань у повітряному просторі (переговори на відкритому просторі).

За рахунок впливу звукових каналів на елементи й конструкції будинку, викликаючи їхню вібрацію.

За рахунок впливу звукових коливань на технічні засоби обробки інформації, таких як мікрофон.

Класифікація акустичних каналів витоку інформації

Основні визначення акустики

Джерелом утворення акустичного каналу витоку інформації є вібруючі, коливні тіла й механізми, такі як голосові зв'язування людини, що рухаються елементи машин, телефонні апарати, звукопідсилювальні системи й т.д. Класифікація акустичних каналів витоку інформації представлене на рис. 1.2.

Поширення звуку в просторі.

Поширення звуку в просторі здійснюється звуковими хвилями. Пружними, або механічними, хвилями називаються механічні збурення (деформації), що поширюються в пружному середовищі. Тіла, які, впливаючи на середовище, викликають ці збурення, називаються джерелами хвиль. Поширення пружних хвиль у середовищі не пов'язане з переносом речовини. У необмеженому середовищі воно складається в залученні в змушені коливання усе більше й більше вилучених від джерела хвиль частин середовища.

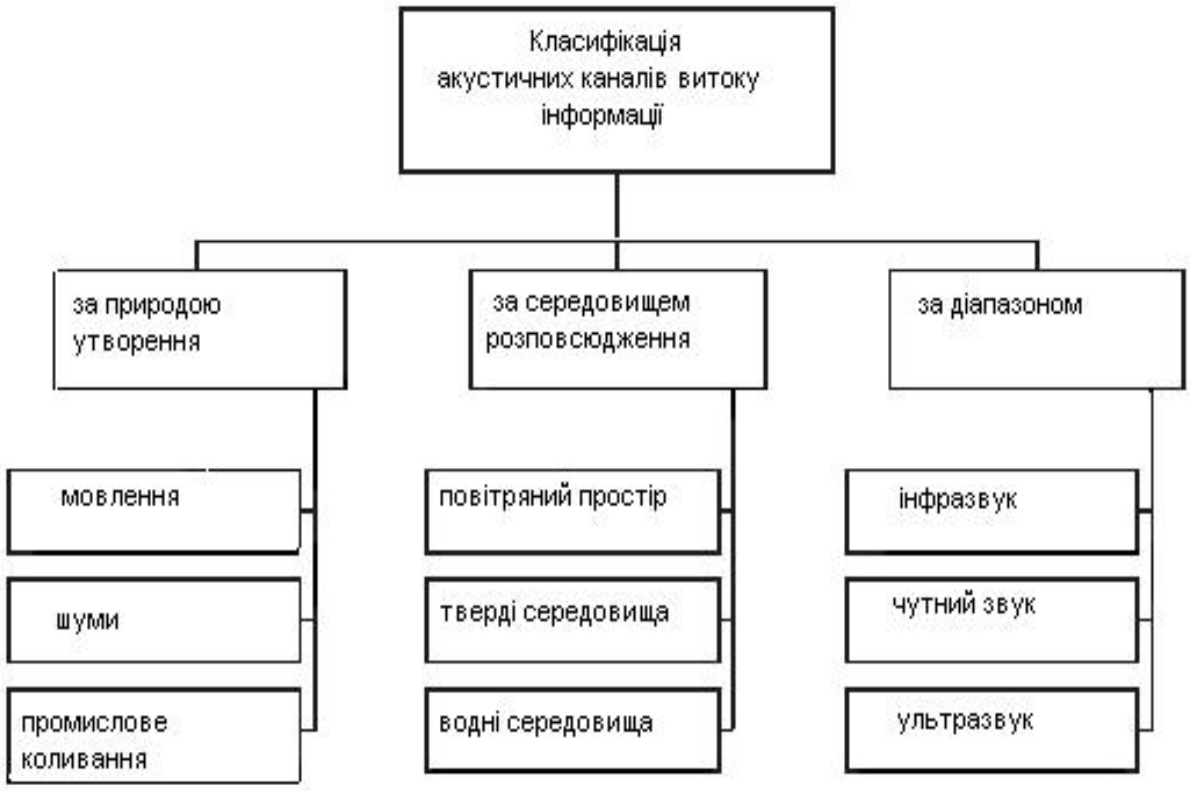


Рисунок 1.2. Класифікація акустичних каналів

Пружна хвиля є поздовжньою й пов'язана з об'ємною деформацією пружного середовища, внаслідок чого може поширюватися в будь-якім середовищі - твердої, рідкої й газоподібної.

Коли в повітрі поширюється акустична хвиля, його частки утворюють пружну хвилю й здобувають коливальний рух, поширюючись в усі сторони, якщо на їхньому шляху немає перешкод. В умовах приміщень або інших обмежених просторів на шляху звукових хвиль виникає безліч перешкод, на які хвилі роблять змінний тиск (двері, вікна, стіни, стелі, підлоги й т.п.), приводячи їх у коливальний режим. Це вплив звукових хвиль і є причиною утворення акустичного каналу витоку інформації.

Акустичні канали витоку інформації утворюються за рахунок (рис. 1.3):

- поширення акустичних коливань у вільному повітряному просторі;
- впливу звукових коливань на елементи й конструкції будинків;
- впливу звукових коливань на технічні засоби обробки інформації.


Рисунок 1.3. Утворення акустичних каналів

Механічні коливання стін, перекриттів, трубопроводів, що виникають в одному місці від впливу на них джерел звуку, передаються по будівельних конструкціях на значні відстані, майже не загасаючи, не послабляючись, і випромінюються в повітря як чутний звук. Небезпека такого акустичного каналу витоку інформації по елементах будинку складається у великій і неконтрольованій дальності поширення звукових хвиль, перетворених у пружні поздовжні хвилі в стінах і перекриттях, що дозволяє прослуховувати розмови на значних відстанях.

Ще один канал витоку акустичної інформації утворять системи повітряної вентиляції приміщень, різні витяжні системи й системи подачі чистого повітря. Можливості утворення таких каналів визначаються конструктивними особливостями повітроводів і акустичними характеристиками їхніх елементів: засувок, переходів, розподільників і ін. Канал витоку мовної інформації можна представити у вигляді схеми, наведеної на рис.1.4


Рисунок 1.4. Схема каналу витоку мовної інформації

Середовища поширення мовної інформації зі способу переносу звукових хвиль діляться на:

- середовища з повітряним переносом;
- середовища з матеріальним переносом (моноліт);
- середовища з мембранним переносом (коливання скла).

Як ми вже відзначали, під акустичною розуміється інформація, носієм якої є акустичні сигнали. У тому випадку, якщо джерелом інформації є людська мова, акустичну інформацію називають мовною.

Первинними джерелами акустичних коливань є механічні системи, наприклад, органи мови людини, а вторинними - перетворювачі різного типу, у тому числі електроакустичні. Останні являють собою пристрій, призначений для перетворення акустичних коливань в електричні й назад. До них відносяться п’єзоелементи, мікрофони, телефони, гучномовці й інші пристрої. Залежно від форми акустичних коливань розрізняють прості (тональні) і складні сигнали. Тональний сигнал - це сигнал, викликаний коливанням, що відбувається за синусоїдальним законом. Складний сигнал включає цілий спектр гармонійних складових.

Мовний сигнал є складним акустичним сигналом у діапазоні частот від 200-300 Гц до 4-6 кГц середовище поширення й спосіб перехоплення.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їхнього перехоплення,

акустичні канали витоку інформації також можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні й параметричні.

Повітряні канали. У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, а для їхнього перехоплення використаються мініатюрні високочутливі мікрофони й спеціальні спрямовані мікрофони.

Мікрофони поєднуються або з'єднуються з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Перехоплена інформація може передаватися по радіоканалі, оптичному каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму, сполучним лініям ВТСС, стороннім провідникам (трубам водопостачання й каналізації, металоконструкціям і т.п.). Причому для передачі інформації із труб і металоконструкцій можуть застосовуватися не тільки електромагнітні, але й механічні коливання.

Вібраційні канали. У вібраційних (структурних) каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будинків, споруджень (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації й інші тверді тіла. Для перехоплення акустичних коливань у цьому випадку використаються контактні мікрофони (стетоскопи).

Електроакустичні канали. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. Перехоплення акустичних коливань здійснюється через ВТСС, що володіють "мікрофонним ефектом", а також шляхом "високочастотного нав'язування".

Оптико-електронний канал. Оптико-електронний (лазерний) канал витоку інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відбивається (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузійні або дзеркальне) модулюється по амплітуді й фазі (за законом вібрації поверхні) і приймається

приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Параметричні канали. У результаті впливу акустичного поля міняється тиск на всі елементи високочастотних генераторів ТСПІ й ВТСС. При цьому змінюється (незначно) взаємне розташування елементів схем, проводів у котушках індуктивності, дроселів і т.п., що може привести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації називається параметричним. Це обумовлено тим, що незначна зміна взаємного розташування проводів у котушках індуктивності (міжвиткового відстані) приводить до зміни їхньої індуктивності, а, отже, до зміни частоти випромінювання генератора, тобто до частотної модуляції сигналу. Точно так само вплив акустичного поля на конденсатори приводить до зміни відстані між пластинами й, отже, до зміни його ємності, що, у свою чергу, також приводить до частотної модуляції високочастотного сигналу генерації.

### 1.3 Матеріально-речовинний канал витоку інформації

Збір інформації про об'єкт здійснюється за допомогою обробки інформації одержуваної з відходів трудової діяльності об'єкта.

По фізичному стані: тверді маси, рідини, газоподібні речовини.

По фізичній природі: хімічні, біологічні, радіоактивні.

По середовищу поширення: у повітрі, землі, воді.

Класифікація матеріально-речовинних каналів витоку інформації

У практиці розвідки широко використовується одержання інформації з відходів виробничої й трудової діяльності. Залежно від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти документів, що становлять, чернетки листів, браковані заготівлі деталей, панелей, кожухів і інших пристроїв для розроблювальних підприємством нових моделей різної техніки. Особливе місце серед такого роду джерел займають залишки бойової техніки й озброєння на іспитових полігонах.

По своєму фізичному стані відходи виробництва можуть являти собою тверді маси, рідини й газоподібні речовини; по фізичній природі вони діляться на хімічні, біологічні, радіаційні, а по середовищу поширення можуть знаходитись в землі, у воді й у повітрі (рис. 1.5).

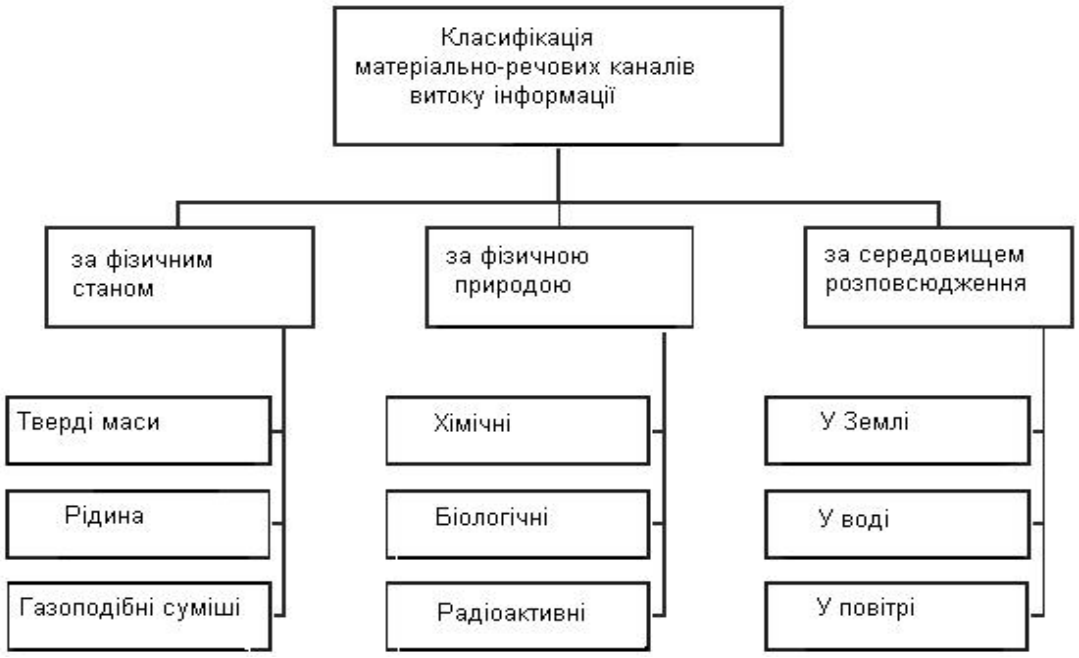


Рисунок 1.5. Класифікація матеріально-речовинних каналів витоку інформації

Особливість матеріально-речовинного каналу, у порівнянні з іншими каналами, обумовлена специфікою джерел і носіїв інформації, що добувається по ньому. Джерелами й носіями інформації в цьому випадку є суб'єкти (люди) і матеріальні об'єкти (макро- і мікро- частинки), які мають чіткі просторові границі локалізації (за винятком випромінювань радіоактивних речовин). Витік інформації по матеріально-речовинних каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межі об'єкта, що захищається. Для більше детального опису розглянутого каналу витоку доцільно уточнити склад джерел і носіїв інформації.

Основними джерелами інформації матеріально-речовинного каналу витоку інформації є:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, розроблювальних у ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- відходи діловодства й видавничої діяльності в організації, у тому числі використаний копіювальний папір, забраковані при оформленні й розмноженні документів аркуші;
- магнітні й інші носії, що вийшли з ладу, інформації ПЄВМ, на яких під час експлуатації втримувалася інформація з обмеженим доступом;
- бракована продукція і її елементи;
- відходи виробництва з демаскуючими речовинами в газоподібному, рідкому й твердому виді;
- радіоактивні матеріали.

Перенос інформації в матеріально-речовинному каналі може здійснюватися наступними суб'єктами й середовищами:

- співробітниками організації;
- повітряними атмосферними масами;
- рідкими середовищами;
- випромінюванням радіоактивних речовин.

Ці носії можуть переносити всі види інформації: семантичну, ознакову, а також демаскуючі речовини.

Семантична інформація втримується в чернетках документів, схем, креслень; інформація про видову й сигнальну демаскуючу ознаки - у бракованих вузлах і деталях, у характеристиках радіоактивного випромінювання й т.п.; демаскуючі речовини - у газоподібних, рідких і твердих відходах виробництва.

Одержувачі інформації, що добувають по матеріально-речовинному каналі, досить різноманітні. Це й з розвідки супротивника, і прилади для фізичного й хімічного аналізу, і засобу обчислювальної техніки, і приймачі радіоактивних випромінювань і ін.

Втрата носіїв коштовної інформації можлива при відсутності в організації чіткої системи їхнього обліку. Наприклад, друкарка, зіпсувавши аркуш звіту,

викидає його в кошик для сміття, з якої він із прибиральницею в сміттєвий бак, що перебуває на території організації. Потім при навантаженні або наступному транспортуванні сміття аркуш несеться вітром і попадає в руки випадкового перехожого. Звичайно, імовірність забезпечення випадкового ознайомлення зловмисника зі змістом цього аркуша невелика. Однак якщо зловмисник активно займається добуванням інформації, область простору, у якій можливий контакт, значно звужується, що приводить до підвищення ймовірності витоку інформації по матеріально-речовинних каналах.

Радіаційні й хімічні методи одержання інформації

Радіаційні й хімічні методи одержання інформації - це порівняно нові методи розвідки, що ґрунтуються на матеріально-речовинному каналі витоку інформації. Вони становлять цілий комплекс заходів, які містять у собі як агентурні заходи, так і застосування технічних засобів.

До агентурного ставляться, попереднє пророблення об'єкта й відбір проб для проведення лабораторних досліджень.

До технічних засобів ставляться космічна розвідка, проведення експрес-аналізів об'єкта й дослідження проб у лабораторії. Для проведення технічної розвідки широко використовуються різні дозиметри й аналізатори хімічного складу.

Хімічні й радіаційні методи аналізу в основному здійснюються над відходами виробництва (стічні води, шлаки й т.д.). Крім того, використання дозиметричних станцій, індивідуальних дозиметрів дозволяє здійснювати контроль за продукцією, що випускає об'єкт, якщо його виробництво пов'язане з радіоактивними речовинами.

Для експрес-аналізу хімічного складу в основному використовуються газоаналізатори й аналізатори хімічного складу рідин. Аналіз ґрунту й інших твердих компонентів проводиться, як правило, над пробами в лабораторних умовах.

Для підприємств хімічної, парфумерної, фармацевтичної й іншої сфер, пов'язаних з розробкою й виробництвом продукції, технологічні процеси яких

супроводжуються використанням або одержанням різних газоподібних або рідких речовин, можливе утворення каналів витоку інформації через викиди в атмосферу газоподібних або скидання у водойми рідких демаскуючих речовин.

Подібні канали утворюються з появою можливості добування демаскуючих речовин шляхом узяття зловмисниками проб повітря, води, землі, снігу, пилу на листах чагарників, дерев і трав'яному покриві на околицях організації.

Залежно від напрямку й швидкості вітру, що демаскують речовини в газоподібному виді або у вигляді зважених твердих часток можуть поширюватися на відстань декількох десятків кілометрів, що цілком достатньо для узяття проб зловмисниками. Аналогічне положення спостерігається й для рідких відходів.

Звичайно, концентрація демаскуючих речовин при видаленні від джерела убуває. Однак при їхньому витоку за досить тривалий період концентрація може перевищувати граничні припустимі значення за рахунок нагромадження демаскуючих речовин у землі, рослинності, підводній флорі й фауні.

Відходи можуть продаватися іншим підприємствам для використання у виробництві іншої продукції, очищатися перед скиданням у водойми, знищуватися або піддаватися похованню на час саморозкладу або розпаду. Останні операції використаються для високотоксичних речовин, утилізація яких іншими способами економічно недоцільна, і для радіоактивних відходів, які неможливо нейтралізувати фізичними або хімічними способами.

Витік інформації про радіоактивні речовини може здійснюватися в результаті виносу радіоактивних речовин співробітниками організації або реєстрації зловмисником їхніх випромінювань за допомогою відповідних приладів.

Дальність каналу витоку інформації про радіоактивні речовини через їхні випромінювання невелика: для α-випромінювань вона становить у повітрі кілька міліметрів, β-випромінювань - кілька сантиметрів і тільки

γ-випромінювання можна реєструвати на відстані в кілька сотень метрів від джерела випромінювань.

### 1.4 Електричний канал витоку інформації

Ланцюга живлення й ланцюга заземлення.

Перехоплення інформації здійснюється за рахунок: випромінювання магнітного поля, паразитної генерації, взаємних впливів, електромагнітних випромінювань, високочастотного нав’язування високочастотних засобів.

Класифікація електричних каналів витоку інформації

Паразитні зв'язки й наведення.

Елементи, ланцюги, тракти, сполучні проведення й лінії зв'язку будь-яких електронних систем і схем постійно є під впливом власних (внутрішніх) і сторонніх (зовнішніх) електромагнітних полів різного походження, що індукуються або навідних у них значні напруги. Такий вплив називають електромагнітним впливом або просто впливом на елементи ланцюга. Як тільки такий вплив утвориться непередбаченими зв'язками, у подібних випадках говорять про паразитні (шкідливих) зв'язки й наведеннях, які приводять до утворення електричних каналів витоку інформації.

Основними видами паразитних зв'язків у схемах радіоелектронного устаткування є ємнісні, індуктивні, електромагнітні, електромеханічні зв'язки й зв'язки через джерело живлення й заземлення обладнання.

Паразитні ємнісні зв'язки

Паразитні ємнісні зв'язки обумовлені електричною ємністю, що утворюється між елементами, деталями й провідниками схем, що несуть потенціал сигналу (рис. 1.6). Тому що опір ємності, що створює паразитний ємнісний зв'язок, падає з ростом частоти, що проходить через неї енергія з підвищенням частоти збільшується. Тому паразитний ємнісний зв'язок може привести до самозбудження підсилювача на частотах, що перевищують його вищу робочу частоту.

Чим більше посилення сигналу між ланцюгами й каскадами, що мають ємнісний зв'язок, тим менше ємності потрібно для його самозбудження. При посиленні в 105 разів (100 дБ) для самозбудження підсилювача звукових частот іноді досить ємності між вхідним і вихідним ланцюгами порядку 0,01 пФ.

Паразитні індуктивні зв'язки

Паразитні індуктивні зв'язки обумовлені наявністю взаємоіндукції між провідниками й деталями РЕО, головним чином між її трансформаторами. Паразитний індуктивний зворотний зв'язок між трансформаторами підсилювача - наприклад, між вхідним і вихідним трансформаторами, - може викликати режим самозбудження в області робочих частот і гармоніках.

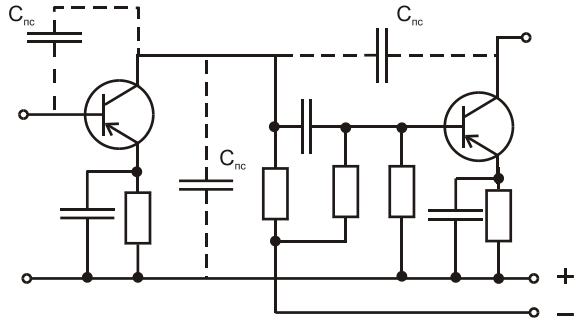


Рисунок 1.6. Схема виникнення паразитного ємнісного зв'язку

Для підсилювачів з малою вхідною напругою (мікрофонні, магнітофонні й ін.) дуже небезпечний індуктивний зв'язок вхідного трансформатора із джерелами змінних магнітних полів (трансформатори харчування). При розташуванні такого джерела поблизу від вхідного трансформатора ЭДС, що наводиться на вторинній обмотці трансформатора середніх розмірів, може досягати декількох мілівольтів, що в сотні разів перевершує припустиме значення. Значно слабкіше паразитний індуктивний зв'язок проявляється при тороїдальній конструкції вхідного трансформатора. При зменшенні розмірів трансформатора паразитний індуктивний зв'язок послаблюється.

Паразитні електромагнітні зв'язки

Паразитні електромагнітні зв'язки приводять до самозбудження окремих каскадів звукових і широкосмугових підсилювачів на частотах порядку десятків і сотень мегагерц. Ці зв'язки звичайно виникають між вивідними провідниками

підсилювальних елементів, що утворюють коливальну систему з розподіленими параметрами й резонансною частотою певного порядку.

Паразитні електромеханічні зв'язки

Паразитні електромеханічні зв'язки проявляються в пристроях, корпус яких має механічний зв'язок із включеним на вхід підсилювача гучномовцем; у підсилювачах розташованих поблизу від гучномовця, а також у підсилювачах, що піддається вібрації (струсу). Механічні коливання дифузора близько розташованого гучномовця через корпус останнього й шасі підсилювача, а також через повітря передаються підсилювальним елементам. Внаслідок мікрофонного ефекту ці коливання викликають у ланцюгах підсилювача появу змінної складової струму, що створює паразитний зворотний зв'язок.

Транзистори майже не мають мікрофонний ефект, тому паразитний електромеханічний зв'язок проявляється в основному в лампових підсилювачах.

Паразитні зворотні зв'язки через джерела живлення.

Паразитні зворотні зв'язки через джерела харчування в багатокаскадному підсилювачі виникають внаслідок того, що джерела живлення мають внутрішній опір.

Так, наприклад, струм сигналу Івих підсилювача (рис. 1.7), проходячи через джерело харчування, створює на внутрішньому опорі Zн останнього спадання напруги U, рівне Івих Zн. Ця напруга подається на попередні каскади разом з постійної складової напруги джерела живлення, а потім через елементи міжкаскадного зв'язку попадає на входи підсилювальних елементів, створюючи в підсилювачах паразитний зворотний зв'язок. Залежно від співвідношення фаз паразитного зворотного зв'язка й корисного сигналу, ця напруга може збільшувати напругу сигналу й (при достатній глибині) привести до його самозбудження.

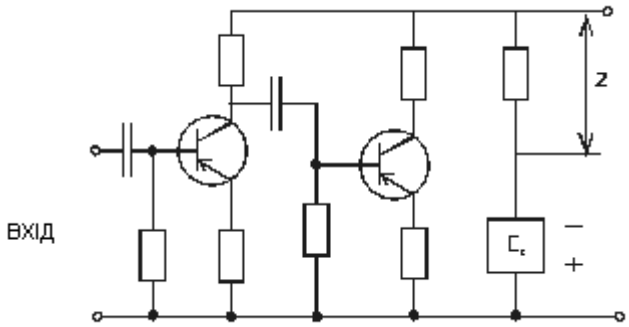


Рисунок 1.7. Схема виникнення паразитного зв'язку в багатокаскадному підсилювачі

Небезпечний сигнал може потрапити в ланцюг електричного живлення, створюючи канали витоку інформації. У лінію електроживлення ВЧ передається за рахунок паразитних ємностей трансформаторів блоків живлення (рис. 1.8).

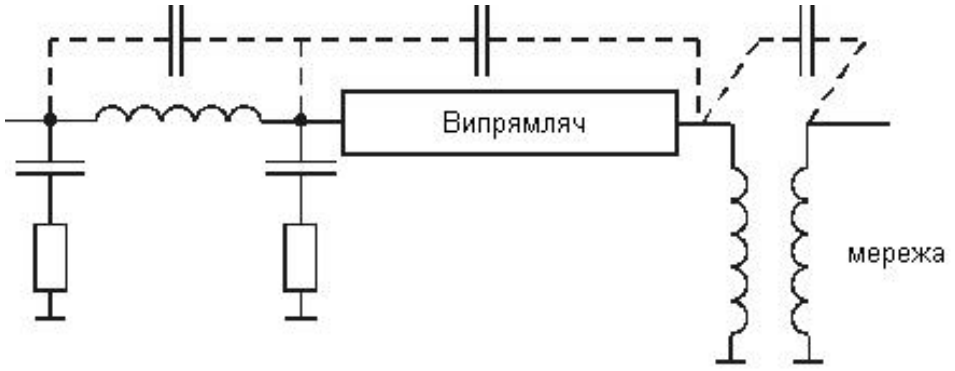


Рисунок 1.8. Схема витоку інформації по ланцюгах живлення

Витік інформації по ланцюгах заземлення

Заземлення (рис. 1.9) - це пристрій, що складається із заземлювачів і провідників, що з'єднують заземлювачі з електронними й електричними пристроями, приладами й т.д. Заземлювачем називають провідник або групу провідників, виконаних із провідного матеріалу й, що перебувають у безпосереднім зіткненні із ґрунтом. Заземлювачі можуть бути будь-якої форми - у вигляді труби, стрижня, смуги, аркуша, дроту й т.п. В основному вони виконують захисну функцію й призначаються для з'єднання із землею приладів.

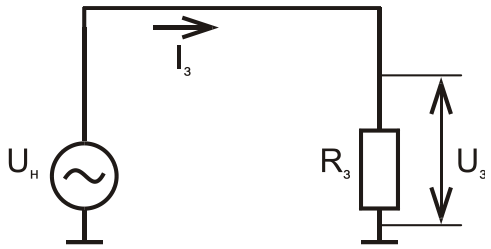


Рисунок 1.9. Схема заземлення

Відношення потенціалу заземлення до стікаючого з його току називається опором заземлення. Величина опору заземлення залежить від питомого опору, ґрунту й площі зіткнення заземлювача із землею.

### 1.5 Радіоканал витоку інформації

Перехоплення інформації здійснюється по засобах радіоприймачів. Інформацією, що перехоплює, є така, що передається по радіоканалі на певній частоті.

Утворення радіоканалів витоку інформації

У сучасних умовах насиченості нашого життя найрізноманітнішими технічними, особливо електронними, засобами виробничої й трудової діяльності, різними засобами зв'язку, різного роду допоміжними системами (телебачення, радіомовлення) конче потрібно розуміти небезпеку виникнення каналу витоку інформації з обмеженим доступом саме через технічні засоби її обробки. Більше того, технічні засоби  чи ставляться не до найнебезпечніших  і широко розповсюджених каналів витоку інформації.

Аналіз фізичної природи численних перетворювачів і випромінювачів показує, що:

- джерелами небезпечного сигналу є елементи, вузли й провідники технічних засобів забезпечення виробничої й трудової діяльності, а також радіо- і електронна апаратури;
- кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;

- кожна електронна система, що містить у собі сукупність елементів, вузлів і провідників, має деяку безліч технічних каналів витоку інформації.

З певним ступенем узагальнення безліч радіоканалів витоку інформації можна представити у вигляді наступної структури (рис. 1.10).


Рисунок 1.10. Структура радіоканалів витоку інформації

Кожний із цих каналів, залежно від конкретної реалізації елементів, вузлів і виробів у цілому, буде мати певний прояв, специфічні характеристики й особливості утворення, пов'язані з умовами розташування й виконання.

Наявність і конкретні характеристики кожного джерела утворення каналу витоку інформації вивчаються, досліджуються й визначаються конкретно для кожного зразка технічних засобів на спеціально обладнаних для цього іспитових стендах і в спеціальних лабораторіях.

Класифікація радіоканалів витоку інформації по природі утворення, діапазону випромінювання й середовищу поширення представлена на рис. 1.11.


Рисунок 1.11. Класифікація радіоканалів витоку інформації

# 2 ОБҐРУНТУВАННЯ ТАКТИКО-ТЕХНІЧНИХ ВИМОГ ДО ГЕНЕРАТОРА ПРОСТОРОВОГО ЗАШУМЛЕННЯ

## 2.1 Постановка завдання

У дипломному проекті необхідно спроектувати пристрій, призначений для забезпечення активного захисту мовної інформації від витоку по акустичному каналу, а саме по віброакустичному каналу. Пристрій повинен захищати від зняття інформації за допомогою лазерних мікрофонів і стетоскопних засобів (стетоскопів, передавачів, стетоскопних мікрофонів, що вбудовуються в стіни мікрофонів і т.д.) і мати наступні параметри: шумовий сигнал з амплітудою не менш 1 В, споживана потужність – не більш 30 Вт, напруга живлення 220В/50Гц. Прилад повинен являти собою конструктивно завершений пристрій.

Габарити генератора і його маса не повинні перевищувати наступних величин:

- довжина 250 мм;
- ширина 150 мм;
- висота 40 мм;
- маса 1.35 кг.

Основними користувачами пристрою є організації, які здійснюють свою професійну діяльність в області технічного захисту інформації, а також структурні підрозділи технічного захисту інформації різних установ, виконання функціональних завдань якими пов'язане з використанням інформації з обмеженим доступом.

В основу розроблювального пристрою захисту мовної інформації від витоку по віброакустичним каналам, покладений генератор просторового зашумлення. Тому в роботі було поставлено завдання розробки структурному й функціональної схем такого пристрою, а також інструкції з його технічної експлуатації. Дані питання розглянуті в наступних розділах.

## 2.2 Короткі відомості про генератори шуму

Первинні джерела шуму

Генератори шуму відрізняються винятковою різноманітністю елементів, що утворюють їх. Це пояснюється, з одного боку, широким вибором первинних джерел шуму, а з іншого сторони, винятковим різноманіттям практичних вимог до самих генераторів.

Від генератора в самому загальному випадку потрібно, щоб він давав широкосмуговий шум з рівномірною спектральною щільністю в заданому діапазоні частот, мав можливість регулювання й контролю вихідної потужності й забезпечував незмінність вихідних параметрів шуму (середньої потужності й законів розподілу миттєвих значень).

Основним вузлом будь-якого генератора шуму є первинне джерело шуму, або, як ще його називають елемент, що шумить. Під первинним джерелом шуму розуміється шумовий генератор, що задає вихідну напругу, яка в наступних каскадах може підсилюватися й перетворюватися по частоті.

Фізична природа флуктуацій електричного струму або напруги може бути досить різноманітною. Вона може полягати в тепловому русі електронів (тепловий шум), у скінченній величині заряду; електрона (дробовий шум), у коливаннях електропровідності електричному кола (контактний шум) і ін.

Тому джерела шуму, застосовувані в якості первинних, наприклад ними можуть бути: активний опір, електронна лампа, газонаповнений тріод, неонова лампа, лампа денного світла, напівпровідниковий діод або тріод, фотопомножувачь, мікрофонна капсула й ін.

Джерело шуму слід вибирати відповідно призначенню й вимогам, які пред'являються до генератора шуму в цілому.

Іноді первинним називають джерело шуму, яке застосовується в якості вихідного для эталонування; тут і далі під первинним джерелом шуму мається на увазі генератор, що задає, шум. Для цієї мети ідеально підходить недороге джерело, що й легко настроюється, шум на напівпровідниковому діоді.

Приведемо класифікацію джерел шуму по джерелу походження електричних шумів (тепловий шум, дробовий шум і т.д.).

Тепловий шум.

Відповідно до сучасних поглядів носіями електричного струму в провідниках є електрони, що володіють елементарним електричним зарядом, рівним $1{,}6 \times 10^{-12}$ Кл.

У кожному атомі речовини є електрони, які оточують позитивно заряджене ядро атома. Орбіти електронів проходять на різній відстані від ядра й утворюють електронні оболонки атомів. Чим ближче електрон до ядра, тим сильніше він з ним зв'язаний. Слабкіше всього пов'язані з ядром електрони, що перебувають на зовнішніх оболонках. Саме ці зовнішні електрони піддаються найбільшим впливам з боку інших атомів.

У металах усі електрони зовнішніх оболонок атомів сильно перекриваються й втрачають зв'язки зі своїми атомами. Тому металеві кристали є такими структурами, які утворені взаємодією позитивних іонів кристалічних ґрат і усуспільнених зовнішніх електронів. Ці електрони можуть вільно переміщатися між атомами ґрат. Поки зовнішнього електричного поля немає, електрони в обсязі провідника, виготовленого з металу, роблять внутрішній хаотичний рух, аналогічний тепловому руху молекул газу або рідини. При своєму русі електрони найчастіше зустрічаються з тепловими коливаннями іонів (атомів) і дефектами кристалічних ґрат, рідше — один з одним.

При зіткненнях вони змінюють і напрямок руху, і величину швидкості. Порядок середнього шляху між зіткненнями, або величина середнього вільного пробігу електронів, становить усього лише 10 нм. Тепловий рух електронів навіть при кімнатній температурі настільки великий, що електрони переміщаються з досить великими швидкостями (близько 100 км/сек).

Струмові шуми недротяних резисторів.

Залежно від технології виготовлення, шуми реальних резисторів, застосовуваних у радіоапаратурі, можуть виявитися значно більше теплового шуму, при цьому спостерігається їхня сильна залежність від напруги, що падає

на резисторі, і від сили струму, що протікає через нього. При протіканні струму через провідний шар резистора його провідність трохи змінюється випадковим образом. Флуктуації провідності викликають випадкові коливання струму, які у свою чергу створюють на опорі напругу шуму. Найбільша спектральна щільність потужності шуму недротяного опору зосереджена в області низьких частот 5 – 1000 Гц.

Шум з рівноімовірним законом розподілу.

Цей шум виникає, коли аналогові сигнали перетворяться в дискретну або цифрову форму. Чим вужчий інтервал квантування, тим менший шум. Практично негативні й позитивні помилки визначаються випадком. У підсумку виходить шум, миттєві значення якого в кожний момент часу мають рівноімовірність або прямокутний закон розподілу.

Шумові діоди.

Шумові діоди використовуються як еталони шумової потужності на частотах до 300 МГц і вище, вони завжди перебувають у режимі насичення анодного струму. Основна вимога до катода шумового діода полягає в тому, щоб він мав яскраво виражений струм насичення. Цій властивості добре задовольняють вольфрамовий або вольфрамові-торієві катоди.

Шумовий діод можна використовувати як широкосмугове джерело шуму. Нижня границя рівна 500 – 1000 Гц, а верхня границя частот розташована звичайно в області 300 – 400 МГц.

Шуми газорозрядних ламп.

У газорозрядних приладах – тиратрон, трубки з неоновим і аргоним наповненням і ін. Вихідна напруга шуму на навантаженні тиратрона досягає сотень мілівольтів, а в особливих випадках і одиниць вольт.

Хаотичні імпульсні шуми.

Існують джерела шуму, які працюють переривчасто, дискретно в часі. Наприклад, такі шуми, спостережуються на виході радіоприймача при дії на його вхід перешкод від пристроїв запалювання двигунів внутрішнього згоряння. Вони сприймаються у вигляді окремих, ізольованих імпульсів. Іншим прикладом може

служити напруга генератора шуму з радіоактивним елементом, у якому зовсім випадково в часі, але дискретно відбуваються акти розпаду, що є причиною виникнення шумових імпульсів.

Ефективне значення напруги імпульсів, випадкових по моментах появи, пропорційно кореню квадратному із середньої потужності. Остання у свою чергу пропорційна смузі прозорості прийомного пристрою. Ця обставина використовується як засіб придушення імпульсних перешкод у відомій системі (широка смуга — обмежник — вузька смуга). Значне зменшення впливу імпульсного шуму на вузькосмугові ланцюги досягається в попередньому широкосмуговому обмежувачі. Дійсно, набагато вигідніше зменшити енергію короткого імпульсу до того, як вона розподілиться, «розтягнеться» на значно більшому інтервалі вузькосмуговими ланцюгами.

При великій кількості імпульсів в одиницю часу розподіл Пуассона дуже близький до нормального. Пуасоновські імпульсні послідовності застосовуються в експериментах і розрахунках «теорії масового обслуговування», у дослідженнях завадостійкості імпульсних систем зв'язку й ін.

Застосування генераторів шуму

Генератори шуму називають також генераторами випадкових, флуктуаційних або нерегулярних сигналів. Вони являють собою сукупності вузлів і пристроїв, що мають, таке ж різноманітне застосування в лабораторній і заводській практиці, як і генератори гармонійних і імпульсних сигналів. Цьому сприяє цілий ряд коштовних якостей, якими вони мають, що забезпечують одержання шумової напруги (струму або потужності) на навантаженні генератора. Спектральний склад шумових коливань на виході генераторів шуму, як правило, рівномірний у дуже широкій смузі частот. Шумові генератори перекривають діапазон від досить низьких частот до найвищих радіочастот (порядку 300 ГГц), застосовуваних у цей час.

Генератори шуму надійні в роботі, прості по конструкції, мають стабільність, що задовольняє вимогам практики. Вони універсальні в тому відношенні, що дозволяють у ряді приватних застосувань за допомогою

порівняно простих засобів, перетворювати шуми з одним законом розподілу миттєвих значень у шуми з іншими законами розподілу останніх або перетворювати флуктуаційні сигнали з одним спектральним составом у шумові коливання з іншим частотним спектром.

Генератори шуму використовуються як калібровані джерела потужності, застосовуваних при вимірах інтенсивності інших шумів або регулярних коливань, наприклад, шумів неземного походження (у радіоастрономії), атмосферних перешкод і ін.

У радіозв'язку генератори шуму застосовуються для виміру перехресних перешкод або діафонії. У багатоканальній телефонії повний сигнал на виході модулятора дуже схожий на шум, що займає ту ж смугу частот, тому виявилося можливим замінити кілька сотень джерел звуку одним широкосмуговим джерелом шуму. Шум, у якому виключені складові спектра частот, що перевіряється, подається на лінію зв'язку, а на випробовуваному каналі прослуховується й виміряється напруга перешкоди. Подібні виміри роблять у проводах зв'язку й у радіозв'язку, особливо на радіорелейних лініях. Такі виміри дозволили встановити припустимі рівні перехресних перешкод.

Більшою різноманітністю відрізняються застосування генераторів шуму також і в електроакустиці. Зокрема, в аудіометрії шуми використовуються для маскування звуків при визначенні розбірливості мови. Генератори шуму застосовують для зняття частотних характеристик гучномовців, мікрофонів і електроакустичних перетворювачів, для виміру часу реверберації приміщень, коефіцієнтів звукопоглинання різних перегородок, стін, звуковбирних матеріалів і ін. У кіно генератори шуму застосовуються для створення шумових ефектів, а в пристроях для синтезу мови (вокодер й ін.) - для одержання узгоджених звуків.

У медичній практиці генератори шуму знаходять застосування як прилади для обезболюючі, наприклад, у процесі лікування зубів і протезування. Ці прилади називаються шумовими аналгезаторами. Дія їх заснована на тому, що

шуми, відтворені головними телефонами, гасять вогнище порушення, обумовлене болючими відчуттями в корі головного мозку.

Нарешті, генератори шуму входять як самостійні вузли в комбіновані вимірювальні прилади, у генератори хаотичних імпульсних перешкод. Вони незамінні в біофізиці при різних досвідах по визначенню граничних величин зору, слуху й ін.

Як правило, генератори шуму необхідно впроваджувати там, де доводиться мати справу з аналізом частотних характеристик, тобто де потрібні не окремі частоти, а цілий спектр частот і широкий діапазон амплітуд сигналів. Застосування шумових генераторів дозволяє автоматизувати цілий ряд ручних операцій електронної й радіотехнічної промисловості.

В основі генерації шумів лежать елементарні фізичні процеси (тепловий рух носіїв електричного заряду, його дискретність і ін.) і комбінації їх. Вимірюючи характеристики шуму, можна по них визначити ряд фізичних постійних, наприклад постійну Больцмана, заряд електрона, рухливість носіїв. Одним з методів визначення електронної температури при термоядерних експериментах є радіоприймання й оцінка інтенсивності радіошумів СВЧ випромінювання плазми.

Але в цьому випадку основна увага приділяється генератору шуму, як було вже зазначене раніше, призначеного для захисту акустичної інформації, наприклад, мови.

Для захисту переговорів від прослуховування використовують генератори акустичної шумової перешкоди – “білого” шуму. Вони дозволяють замаскувати корисну інформацію на тлі шуму. На відміну від однотональної або багатотональної періодичної перешкоди, музики, шуму двигуна й т.п., які шляхом спеціальної обробки сигналу можуть бути відфільтровані, перешкоди типу “білого” шуму практично не піддаються повній фільтрації й тому є найбільш ефективними для закриття корисної інформації. Крім того, акустичні генератори “білого” шуму ефективні ще й тим, що впливають безпосередньо на

НЧ тракти систем, що підслухують, незалежно від особливостей їх схемотехніки й принципів передачі інформації.

Для захисту від витоку інформації по каналах побічних електромагнітних випромінювань електронно-обчислювальної техніки використовують генератори шуму, що випромінюють активну широкосмугову радіоперешкоду, що впливає на вхідні ланцюги радіоприймальних пристроїв. Аналогічні прилади використовуються для захисту від витоку інформації по електричній мережі й телефонним лініям.

В основі розподілу генераторів шуму на класи лежать різні характеристики випадкових сигналів. Розглянемо деякі з можливих класифікацій.

За формою сигналу генератори шуму діляться на два більші класи: генератори безперервних (аналогових) і генератори дискретних (імпульсних) випадкових сигналів.

По частотному діапазону генериручих коливань генератори шуму діляться на наступні групи: інфранизькочастотні, низькочастотні, відеочастотні й надвисокочастотні.

По ширині смуги генеруючих частот розрізняють вузьксмугові (середня частота значно більша, ніж ширина всього спектра частот) і широкосмугові генератори шуму. В останніх ширина спектра близька до середньої частоти. Такі генератори називають іноді генераторами “білого” шуму.

Генератор шуму, який називають широкосмуговим, може працювати в режимі генерації нормального, або релеевського шуму, генератор нормального шуму може бути вузькосмуговим і широкосмуговим.

Універсальним методом захисту від знімання інформації з акустичних і віброакустичним каналам вважається віброакустичне зашумлення приміщень.

Система віброакустичного зашумлення звичайно складається з генератора низькочастотних шумових сигналів, декількох віброакустичних датчиків і 1-2 акустичних датчиків (звукових колонок). За допомогою акустичних датчиків зашумляють акустичні канали, які усунути неможливо,

наприклад, воздуховоди. Далі будуть наведені технічні характеристики деяких із пристроїв призначених для активного захисту аудио - і віброканалів витоку інформації.

## 2.3 Огляд існуючих технічних засобів захисту віброакустичних каналів

Основні існуючі технічні засоби захисту віброакустичних каналів наведен в табл. 2.1

Таблиця 2.1 Основні існуючі технічні засоби захисту віброакустичних каналів

| **Система захисту** / Параметри | **Заслон-2М** | **Соната 1А** | **Кабінет** | **SEL SP-51/A** | **DNG-2300** | **VNG 006DM** |
|---|---|---|---|---|---|---|
| Шумова смуга | 0,1-5 кГц | 0,17-6 кГц | 0,1-6 кГц | 0,1-11 кГц | 0,25-5 кГц | 0,2-5 кГц |
| Включення вібродатчиків | | авто | | авто | | |
| Радиус дії вібродатчика | 1,5 м | | | 5м | 5 м | 2,5 – 3 м |
| Максимальна кількість вібродатчиков | 25 | 12 (6+6) | Не більше 30 | 32 | 18 | 6 - 15 |
| Потужність | | | | | 12 Вт | |
| Напруга живлення | | 220 В, 50 Гц | 220 В, 50 Гц | 220 В,50Гц | 220 В, 50 Гц | 220 В, 50 Гц |
| Габаритні розміри | 46x65x53 | 153x135x65 | 100x200x350 | 160x160x45 | 254x152x43 | 160x150x50 |

## 2.4 Цифрові генератори шуму

DNG-2300 - цифровий генератор “білого” шуму (3 канальний) зображений на рис. 2.1.

Рисунок 2.1. Генератор шуму DNG-2300

DNG-2300 захищає від:

- лазерних і мікрохвильових систем, що використовують відбиття від вікон;
- стетоскопів (контактних мікрофонів);
- мікрофонів, вмонтованих у стіни або стелю;
- інших віброакустичних каналів витоку інформації.

DNG-2300 призначений для захисту від пристроїв, що підслухують, які не реєструються звичайними методами. Прилад захищає периметр приміщення шляхом наведення на конструкції “білого” нефільтрованого шуму за допомогою вібраційних випромінювачів TRN-2000 і акустичних випромінювачів OMS-2000. Кількість випромінювачів визначається приміщенням.

Ступінь захисту DNG-2300 вищий чим в системах з гучномовцями. Вібровипромінювач DNG-2300 здійснює спрямоване покриття площі усередині периметра й має набагато кращі характеристики, роблячи при цьому менше шуму в заданій області. Хоча усередині захищеної області може бути чутний деякий шум, підвищувати голос не прийдеться.

Як здійснюється захист: Генератор DNG-2300 може блокувати подібного роду пристрої. Це досягається поширенням спеціальними випромінювачами нефільтрованого акустичного шуму в будівельні конструкції. У якості вібраційних випромінювачів рекомендується використовувати випромінювачі фірми REI TRN-2000.

Також з DNG-2300 використовуються акустичні випромінювачі фірми REI OMS-2000. Призначення цих випромінювачів у поширенні звукового нефільтрованого шуму в навколишньому просторі. OMS-2000 звичайно використовується для захисту воздуховодів, підвісних стель, просторів за фальш-панелями й т.п.

DNG-2300 працює в діапазоні 250-5000 Гц, що є оптимальним для придушення найпоширеніших типів, підслуховуючих пристроїв.

DNG-2300 містить 3 незалежних цифрових канала генератора "білого" шуму. "Білий" тому, що містить усі частотні гармоніки, що присутні в спектрі людського голосу. Наявність усіх складових гармонік людської мови дозволяє ефективно боротися з різноманітними методами очищення мовної інформації.

**2.5** Забезпечення організаційно-технічних заходів щодо захисту інформації

Організаційні заходи

У процесі організаційних заходів визначають контрольовану територію, у якій виключаються неконтрольоване перебування осіб, що не мають допуску; виділяють із експлуатованих технічних засобів, виявляють наявність у контрольованій зоні ВТС, уточнюють існуюче кабельне розведення, звертаючи особливу увагу на кабелі, що виходять за межі контрольованої зони, становлять переліки виділених приміщень, призначених для проведення закритих заходів (переговорів, обговорень, бесід, нарад і т.д.)

Контрольована зона може обмежуватися периметром охороняємої території, частиною охороняємої території, що охоплює будинок й споруди, у яких проводиться закрите заходу, частини будинків, кімнати, кабінети, зали засідань, у яких проводяться закриті заходи. Контрольована зона може при необхідності встановлюватися більше чим охороняєма територія, при цьому забезпечується постійний контроль над неохороняйомою частиною території.

Постійна контрольована зона - зона, границя якої встановлюється на тривалий строк. Постійна зона встановлюється у випадку, якщо секретні заходи усередині цієї зони проводяться регулярно.

Тимчасова контрольована зона встановлюється для проведення секретних заходів разового характеру. Приміщення, які підлягають захисту, визначаються як виділені й підрозділяються на:

приміщення 1 групи - приміщення, призначені для проведення особливо важливих і зовсім секретних заходів постійного або разового характеру, пов'язаних з обговоренням питань до яких допущено строго обмежене коло осіб;

приміщення 2 групи - приміщення, призначені для постійного проведення закритих заходів, пов'язаних з обговоренням, передачею й обробкою мовної зовсім секретної й секретної інформації;

приміщення 3 групи - приміщення, у яких установлюється апаратура й комутаційне встаткування основних ТСПІ або ВТСС із оконечними пристроями в приміщеннях першої й другої групи.

Приміщення 3 групи для проведення закритих заходів не використовуються.

За результатами робіт становлять протоколи обстежень; узагальнені дані протоколів оформлюють відповідним актом. Після завершення передбачених в акті робіт проводять атестацію виділених приміщень і становлять графік періодичних атестаційних перевірок.

Організаційно технічні заходи

Організаційно-технічні заходи здійснюються шляхом блокування можливих каналів витоку інформації через діючі на об'єкті ТС за допомогою відключення ланцюгів і установки найпростіших схем і пристроїв захисту, демонтажу окремих кабелів, що виходять за межі контрольованої зони, вилучень із виділених приміщень пристроїв ТС, застосування яких може привести до витоку секретної інформації; перемонтажу окремих комутаційних пристроїв і встаткування систем, заміни окремих ділянок кабелів, у тому числі систем заземлення й електроживлення технічних засобів з метою внесення їх у межі контрольованої зони. Етап завершується складанням інструкції з контролю захищеності технічних засобів і систем, змонтованих на об'єкті.

Заходу щодо блокування каналів можливого витоку мовної секретної інформації, системи міського й внутрішнього телефонного зв'язку здійснюється за допомогою відключення на період проведення закритих заходів дзвінкових ланцюгів телефонних апаратів, установлення в ланцюг телефонних апаратів безрозривної розетки, що дозволяє робити відключення апарата на період проведення закритих заходів, установки елементів захисту.

Заходу щодо блокування каналів можливого витоку мовної секретної інформації із приміщень першої й другий груп через діючі системи гучномовної диспетчерській і директорському зв'язку, здійснюється за допомогою розміщення пультів диспетчерів у приміщеннях третє групи, установки у викличних ланцюгах вимикачів, що дозволяють розривати ланцюги в період проведення закритих заходів, установки на вході гучномовців вимикачів, що дозволяють на період закритих заходів розривати ланцюги по двом проводам; забезпечення відключення на період проведення закритих заходів живлення мікрофонних підсилювачів.

Заходу щодо блокування можливих каналів витоку мовної секретної інформації через ланцюги вторинних электрочасових систем електрифікації, розміщених у приміщеннях першої й другої групи до вживання технічних заходів захисту, забезпечується тільки відключенням підведених до них лініям.

Для запобігання витоку мовної секретної інформації в системі пожежної сигналізації застосовуються температурні й димові оптичні датчики DS-260, СИ-1, ДТЛ, КИ-1, РИД-1.

Для захисту мовної секретної інформації від витоку через ланцюги й пристрою охоронної сигналізація рекомендується використовувати датчики стійкі до радіочастотних і електромагнітних перешкод СИ-1, УКД-1, ДМК.

# 3 ГЕНЕРАТОРИ ШУМУ

## 3.1 Електровакуумні і газорозрядні джерела шумів

Шумові діоди. В якості первих джерел шуму у досить великому діапазоні частот (від декількох сот Герц до декількох сот МГерц) використовуються так звані шумові діоди. Ці діоди мають вольфрамові та торієво-вольфрамові катоди прямого накалу і досить невеликі відстані між анодом і катодом. Їх шуми обумовлені дискретною природою електричного струму лампи і називаються дробовими.

Виліт електронів із катоду, а в діодах, які працюють в режимі насищення і їх миттєвого руху до анода приводять до появлення імпульсного анодного струму. Тривалість імпульсу $\tau_{П}$ рівна часу прольоту електрона, який має заряд $q$ і масу $m$, від катода до аноду. Виліт електронів із катоду, поява випадкова і незалежна, тому анодний струм діода представляє суму незалежних випадкових імпульсів тривалістю $\tau_{П}$. Ширина спектру кожного імпульсу визначає ширину спектра дробового шуму. Рівняння руху електрона, який має масу $m$, заряд $q$ які знаходиться під дією електричного поля $E_a = \frac{U_a}{d}$, має вигляд:

$$q\frac{U_a}{d} = m\frac{d^2x}{dt^2},$$

де $d$ - відстань між анодом і катодом; $U_a$ - потенціал аноду відносно катоду.

Початковою швидкістю електрона завжди можна знехтувати, так як її значення не перевищує 0,25 єв, а $U_a \le 100$ в, тому

$$x(t) = \frac{qU_a}{2md}t^2.$$

Звідси слідує, що час $t = \tau_{П}$, яке витрачається електроном на переліт від катоду до анода:

$$\tau_{П} = \sqrt{\frac{3m}{qU_a}}d \approx \frac{d}{6\cdot 10^5\sqrt{U_a}}.$$

Приймаючи $d = 2\cdot 10^{-3}$ м, $U_a$=100 в, отримаємо $\tau_{П} = 3{,}3\cdot 10^{-10}$ с.

В процесі свого руху від катоду до анода електрон накопичує енергію. В той момент, коли він знаходиться на відстані $x(t)$ від катоду, його енергія дорівнює:

$$\theta(t) = \frac{qU_a}{d} x(t).$$

Остання в свою чергу дорівнює роботі, яку потрібно виконати для того, щоб навести на анод заряд $Q$. Робота $A_q = U_a Q$. Порівнюючи $A_q$ і $Q(t)$, знайдемо,

$$Q(t) = \frac{q}{d} x(t).$$

У відповідності з визначенням струм в анодному колі буде змінюватися по закону

$$i_a(t) \frac{dQ(t)}{dt} = I_m t, \ 0 \langle t \le \tau_{II},$$

де $l_m = \frac{q^2 U_a}{d^2 m}$ - амплітуда імпульсу анодного струму, обумовленого перельотом одного електрона у просторі катод – анод.

Виліт електронів із катоду – явища випадкові і незалежні. Одночасно у просторі катод – анод знаходиться дуже багато електронів. Тому, не дивлячись на сурово визначену форму одиночного імпульсу, сумарний струм має нормальне розподілення миттєвих значень.

Математичне очікування цього розподілу визначає середній струм, який проходить через лампу. Останній дорівнює переносному в одиницю часу через лампу заряду

$$I_0 = \overline{n_e} q,$$

де $\overline{n_e}$ - середє число електронів, які пройшли від катоду до анода за 1секунду.

Звідси

$$\overline{n_e} = \frac{I_0}{q}.$$

Приймаючи $I_0 = 40$ ма, отримаємо, що $n_e = 2{,}5 \cdot 10^{17}$ електронів. Звичайно, при суміруванні такого числа імпульсів, які мають випадкові моменти з’являння, флуакції нормалізуються.

Спектральна щільність флуактаційної складальної анодного току описується формулою

$$G(w) = I_0 q \frac{8}{(w\tau_{П})} [(w\tau_{П})^2 + 2(1 - \cos w\tau_{П} - w\tau_{П} \sin w\tau_{П})] .$$

Значення спектральної щільності шумів у нульових частот буде дорівнювати:

$$G(0) = 2qI_0 , \; a^2 \cdot cek .$$

Ширину спектру шумів зручно визначити при значені $wt_{П} = \pi$. При цьому $G(w = w_1) = 0,57G(0)$. Звідси частота спектру, на якій спектральна щільність досягає 0,57 свого максимального значення,

$$f_1 = \frac{w_1}{2\pi} = \frac{1}{2\tau_{П}} = \frac{3 \cdot 10^5 \sqrt{U_a}}{d} .$$

Спектральна щільність характеризує сам діод як джерело шуму.

Природньо, що на ширину спектру сигналу на виході навантаженної на опір $R_H$ лампи впливає величина опору нагрузки.

Напруга шума насищеного діода на нагрузкі $R_H$ визначається формулою

$$P_H = 2qI_0 R_H \Delta f ,$$

де $\Delta f$ - полоса шумів на виході схеми.

Величина нагрузки $R_H$ визначає ширину полоси шумів $\Delta f$, тому $R_H$ і $\Delta f$ пов’язані.

Анодне навантаження у вигляді резистора $R_H$ разом з ємкістю катод – анод $C_{ak}$ створює фільтр нижніх частот з еквівалентною полосою $\Delta f = \frac{1}{2} R_H C_{ak}$.

Тому при активній нагрузці напруга шумів на нагрузці залежить від $R_H$ і дорівнює:

$$P_H = \frac{qI_0}{C_{ak}} .$$

Зі зміною величини $R_H$ змінюється тільки ширина спектру. Для шумового діода 2Д2С $C_{ak}$ =0,78 пф, а струм досягає 40 ма. Максимальна напруга шумів

$$P_{H.\max} = 8,7 \cdot 10^{-9} \text{ Вт.}$$

При резонансній нагрузці можна розширити полосу шумів на виході генератора і, тобто, збільшити їх напругу, але вона залишається настільки низькою, що в генераторах приходиться мати багатокаскадні посилювачі. Але у шумового діода є свої переваги: велика ширина спектру, можливість контролювати інтенсивність шумів по величині анодного струму, мала чутливість до зміни анодної напруги. Остання обставина пов'язана з тим, що струм насищення діода мало залежить від анодної напруги. В той же час анодний струм дуже залежить від напруги накалу. Часто залежність анодного струму від напруги накалу використовують для стабілізації мощності генеруємих шумів.

В діодах з оксидними катодами, які не мають режиму насищення, при роботі в непреривному режимі має місце просторовий заряд. Останній, створюючи гальмівне поле для імітуючих катодом електронів, упорядковує поток електронів від катоду до аноду. Тому спектральна щільність шумів анодного струму у таких діодів нижча, ніж у діодів з насищенням, і визначається формулою

$$G_{o.k}(0) = 2I_0 qF_0,$$

де $F_0$ - коефіцієнт, який визначається параметрами лампи.

Звичайно лампи з великою крутизною $S$ мають і достатньо велике значення середнього струму $I_0$. Тому навіть багатоелектродні лампи при рівних токах $I_0$ уступають шумовим діодам як по ширині спектру, так і по мощності флуктуації струму.

На частотах нижче 1000 Гц спостерігається ріст спектральної щільності флуктуацій струму, зумовленний так званим „ефектом мерегтіння катоду" (флікер - ефектом). Спектральна щільність складової флуктуацій, зумовлений „мерегтінням" катоду , росте зі зменшенням частоти.

Газорозрядні джерела шумів. Найбільш часто в якості первинних джерел шумів в самих різних діапазонах частот використовують газорозрядні пристрої. Для отримання низькочастотних шумів пригодні тиратрони з гарячими та холодними катодами, стабілітрони та газосвітильні лампи. Для генерації шумів в СВЧ діапазоні використовуються спеціально розроблені для цих цілей

газорозрядні трубки. Найбільш високий рівень шумів має тиратрон, поміщений в поле кільцевого магніту, силові лінії якого нормальні до лінії шляху електрона. Фізичні процеси, які приводять до високого рівня шумів тиратрона, вивчені недостатньо добре. Тому можна дати тільки якісне і в певній сфері гіпотетичне пояснення цих процесів.

Під дією електронів, прискорених приложеною між анодом і катодом різницею потенціалів, утворюється плазма. Хоча між числом іонів і електронів в плазмі існує динамічна рівновага, струм тиратрона в основному обумовлений електронами, які потрапляють на анод, так як їхні швидкості в багато раз більше швидкості іонів. Електрона хмара просторового заряду окружає катод і тим самим предохраняє його від інтенсивного бомбардування іонами. Під дією прискорюючого поля позитивні іони проникають в електрону хмару, а часто без рекомбінації досягають катоду. При цьому виникає спалах електрої емісії. Остання призводить до появлення імпульсу анодного струму. Число електронів, визваних проникненням одного іона в область просторового заряду, велике, що і пояснює високий рівень шумів тиратрона.

Тривалість імпульса анодного струму не дорівнює часу прольоту електрона від катоду до анода, так як імпульс визивається великим числом розподілених у часі електронів і на ряду з первиними електронами на анод поступають електрони із плазми. Цим пояснюється порівняно вузька ширина спектру шумів тиратрона. Зі зменшенням щільності газів у балоні падає інтенсивність шумів, але розширюється їх спектр. Амплітуди, тривалості і моменти появлення імпульсів анодного струму є випдковими величинами. Але без магнітного поля в спектрі шумів струму тиратрона спостерігається ярко виражена квазіперіодична складова. Її поява визвана нестійкістю плазми.

Природа появи квазіперіодичної складової може бути пояснена наступним чином.

Нехай в деякий момент часу у пристрої упаде концентрація вільних зарядів і, тому, збільшиться падіння напруги на пристрої. В результаті збільшиться швидкість електронів, зменшиться концентрація електронів у

просторовому заряді і тим самим полегшується їх вихід із катоду. Як слідство росту енергії електронів виникне збільшення числа процесів іонізації, впаде напруга на пристрої, і процес почне розвиватися в зворотньому порядку. Всі ці процеси розтянуті у часі, тобто проходять з деяким запізненням. Таким чином, тиратрон може бути подібним замкнутій системі регулювання з запізненням, яка має деяку зону нестійких станів і находиться під дією випадкових возмущеній. Положення квазіперіодичної складової на шкалі частот для даного типу тиратрона залежить від величини анодного струму: чим більше струм тиратрона, тим нижче частота коливань плазми. Експериментально встановлено, що частота квазіперіодичної складової змінюється в залежності від типу і режиму роботи тиратрона від декількох КГц до декількох МГц. Більш того, коливання можуть мати одночасно декілька некратних частот.

Якщо тиратрон знаходиться у магнітному полі, силові лінії якого перпендикулярні по направленю руху електронів, то траекторія останіх закручується довкола магнітних силових ліній і шлях електрона до анода достатньо удліняється. Це призводить до зросту ймовірності співударів електрону з нетральним атомом газу і, тому, росту щільності іонів. Кордон плазми наближається до катода, і число імпульсів анодного струму зростає. Одночасно зростає і їх тривалість. Імпульси перекривають один одного, завдяки чому падає спектральна щільність на низьких частотах, а в цілому вона вирівнюється. Збільшення анодного струму тиратрона за рахунок зміни напруги анодного живлення чи зменшення анодної нагрузки приводе до транформації спектру флуктуацій в область більш низьких частот. Суттєвим недоліком тиратронів як джерел шумів є великий розброс параметрів отриманих флуктуацій. Заміна тиратрона, як правило, потребує регулювання схеми. Найкращі результати можна отримати, використовуючи для отримання магнітного поля електромагніт, а регулювання виконувати шляхом заміни напруги магнітного поля. Для зміни потоку розсіювання обмотку краще помістити у феромагнітний кожух, а центральну трубку виробляти з немагнітного матеріалу. Нормальна робота тиратрона забезпечується при

проходжені струму 2-15 ма на обмотці, який має близько 10000 витків. Використаня електромагнітів дозволяє з успіхом використовувати і тиратрони, які спеціально не предназначені для отримання шумів, для яких магніти не випускаються. Регулювання магнітного поля шляхом заміни струму через обмотку електромагніту дозволяє значно вирівняти спектральну щільність генерующих шумів. Спектральна щільність шумів сильно залежить від величини опору нагрузки. Найбільше підходить до тиратрона ТГП1 є навантаження 2-3 ком при анодному струмі $I_0 = 10 \div 30$ мА.

Інколи в якості первих джерел шуму використовують і інші газорозрядні пристрої: неонові лампи, стабілітрони, тиратрони з холодним катодом та ін. Напруга шумів, які можна отримати від таких пристроїв, дсягає одиниць мілівольт при навантажені в декілька кОм. Недоліками цих пристроїв є мала інтенсивність і нерівномірність спектру. Для отримання шумів з максимальною інтенсивністю потрібно регулюванням напруги ставить пристрій в режим появи тліючого розряду. Потрібно відмітити, що для інтенсивності генеруючих шумів всі перераховані вище, газорозрядні пристрої уступають тиратрону в десятки і навіть сотні раз. Найбільшою повторюваністю характеристик від прибора до прибора і стійкістю параметрів у процесі використання мають стабілітрони.

### 3.2 Джерела випадкових напруг, які використовують явища радіоактивного розпаду

Ядерне випромінювання находить широке застосування в багатьох областях науки і техніки. Використовують його і для цілей генерування випадкових електричних сигналів. Це обумовлено тим, що радіоактивний розпад за своєю природою - явище випадкове, досить стабільне у часі і не залежить від зовнішніх умов. Продукти радіоактивного розпаду мають постійну енергію чи заряд. Кожен акт радіоактивного розпаду атома – явище випадкове і незалежне чи, у будь-якому випадку, досить слабо пов’язане з іншими аналогічними актами.

Ймовірнісні характеристики процесу реактивного розпаду принято характеризувати законом Пуассона. Останій справедливий для стаціонарних потоків випадкових подій. Радіоактивний розпад же за своєю природою- явище нестаціонарне: середне число актів розпадів зменшується у часі. Для інженерної практики ця обставина особливого значення, очевидно, не має, так як навіть при використані такого джерела випромінювання, як фосфор-32, на протязі часу спостереження процес можна вважати стаціонарним. В якості джерел $\beta$-випромінювання використовують світлові маси постійної дії, які випускаються для нанесення на головки електричних перемикачів. У загальному випадку радіоактивні ізотопи випускають $\alpha$- , $\beta$-частини і $\gamma$-лучі. Діючи на дектори випромінювання, вони в решті перетворюються в імпульси напруги. Характеристики цієї напруги залежать не тільки від ізотопу, но і від типу детектора випромінювання. В залежності від вимог, які пред'являються до генератора, використовуються різні типи детекторів. Переважно в них використовується явище іонізації газового середовища.

При необхідності отримувати високі середні частоти руху імпульсів потрібно використовувати сцинтиляційні і полупровідні детектори.

Газорозрядний лічильник являє собою герметичну скляну трубку, яка заповнена сумішшю газів: аргона, неона, парів спирту та інш. Кінцевий тиск газу в трубкі складає 1-2% від атмосферного. Внутрішньо трубка покривається тонким шаром металевої фольги, яка служе в якості катоду. Роль аноду виконує тонка проволока, натянута в поперек віссі трубки. Газові лічильники можуть працювати у двух режимах: імпульсному і струмовому. Імпульсний використовується для регістрації окремих часток, а струмовий – для вимірювання середньої інтенсивності випромінювання. В генераторах випадкових сигналів використоувється, як правило, імпульсний режим.

При проходжені через газове середовище часток чи кванту електромагнітної енергії достатньої величини виникає початкова іонізація, вивільнюються електрони, які при русі до аноду прискорюються і визивають лавиноподібне нарощування числа іонізованих часток. Розряд який виник

приводе до різкого падіння опору трубки, і на нагрузці $R_H$ виникає імпульс напруги. Опір навантаження настільки великий, що розряд у газі виконується тільки до тих пір, доки не зарядиться паразитна ємкість схеми $C_П$. Процес рекомбінації триває 100-200 мксек, тому середня частота роздільно регеструючих частинок не може бути великою. Характер проходження процесу можна змінити, змінюючи напругу анодного навантаження $R_H$.

Сцинтиляційні лічильники складаються із перетворювача енергії ядерних частинок в енергію випромінювання і приймача цього випромінювання. В якості приймача, як правило, використовують фотоелектроні множники. В залежності від типу використовуваної рідини тривалість спалаху світла коливається від $0,25\cdot10^{-6}$ до $10^{-5}$ сек для неорганічних з'єднань і от $0,8\cdot10^{-8}$ до $6\cdot10^{-6}$ сек для органічних рідин. Дякуючи малій тривалості світлових спалахів можна отримати випадкові по моментам появи і досить короткі імпульси, наступні з великою середньою частотою.

У теперішньому часі настільки високої частоти руху випадкових імпульсів (до $5\cdot10^{7}\ {}^{1}\!/\!_{сек}$) важко досягти з допомогою інших пристроїв, тому там, де потрібно отримувати такі сигнали, відносна сложність пристрою може окупитись високою якістю генеруючих чисел. При використані фотоелектроного множника потрібно мати на увазі, що амплітуди імпульсів на його виході у більшому ступені залежать від прикладених до його анода і діодам напруги і інтенсивності спалахів. Тому висока стабільність середньої частоти руху імпульсів може бути досягнута тільки при використані достатньо складних схем стабілізації фотоелектроного множника. В основу побудови систем регулювання середньої частоти імпульсів можна покласти залежність щільності потока частинок $J[\ {}^{1}\!/\!_{(сек\cdot см^2)}\ ]$ від відстані до джерела.

Для фотоелектроного множника характерний високий рівень власних шумів, але це ні в якій мірі не накладує обмежень на використання сцинтиляційних лічильників у якості первинних джерел випадкових сигналів. Крім того, фотоелектронний множник потрібно розглядати як джерело

нормальних широкополосних шумів. Причиною виникнення флуктуацій струму фотоелектроного множника є дробовий ефект. Флуктуації струму фотокатоду посилюються в стільки раз, в скільки раз посилюється середня складова струму фотоелектроної емісії. Значення дисперсії флуктуацій струму фотоелектроного множника визначається формулою:

$$I_E^2 = 2I_0 q\Delta f K(1+B),$$

де $B$ - експериментально визначений коефіцієнт; $I_0$ - середній струм фотокатоду.

Коефіцієнт посилення $K$ у сучасних фотоелектроних множниках досягають величини $10^6 - 10^8$, а ефективна напруга шумів при вірному виборі режиму - декілька Вольт. Найбільш вигідним режимом фотоелектроного множника як джерела шумів є режим, який забезпечує отримання максимального $K$ , а світловий потік має забезпечувати роботу у районі верхнього згибу його характеристики, яка складає для більшості фотоелектроних множників $10^{-3} - 10^{-2}$ лм. Збільшення світлового потоку за вказану норму приводить до появи просторового заряду, швидкому втомленю катоду і падінню ефективної напруги шумів. Полупровідні детектори ядерного випромінювання являють собою кремнієві діоди, ввімкнені в обратній полярності і охолоджені до температури рідкого азоту. За електричними характеристиками вони близькі до фотоелектроних множників, але в зв'язку з необхідністю використовувати кріогенну техніку використання у генераторах випадкових сигналів не знайшли.

### 3.3 Радіочастотний генератор шуму GSM діапазону

Пропонується симетричний двотактний генератор флуктуаційного шуму на паралельних транзисторах (рис. 3.1).

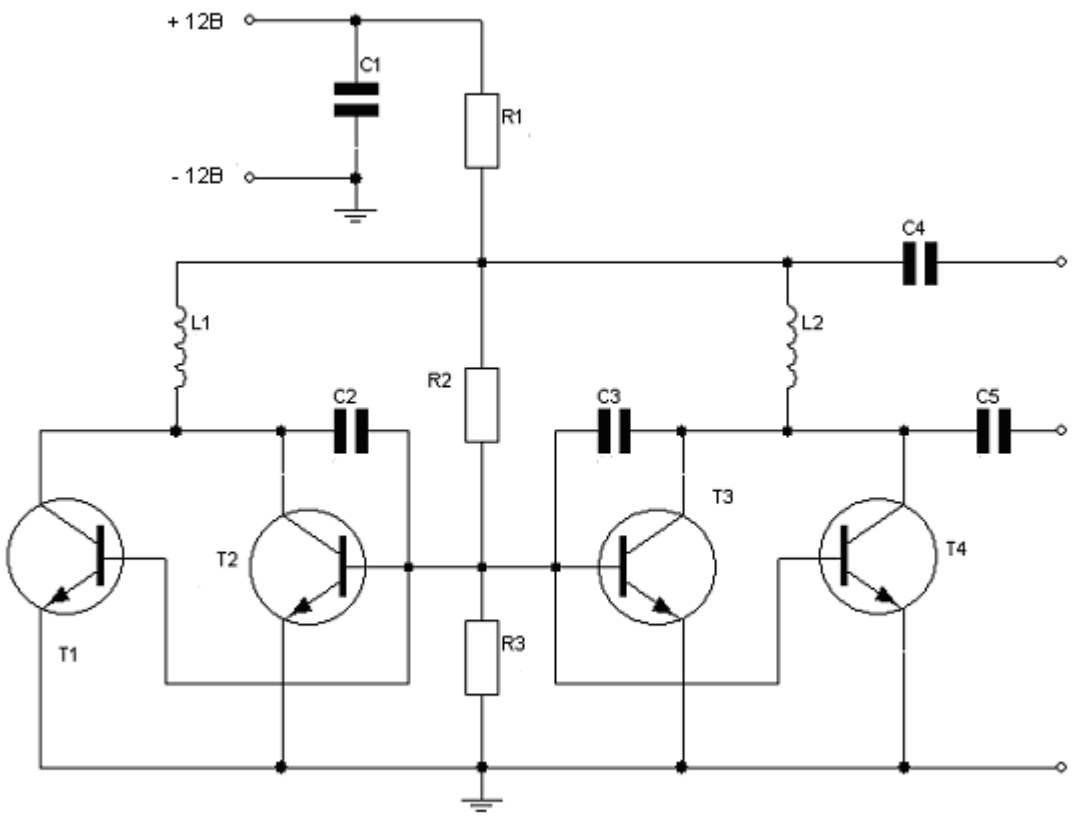


Рисунок 3.1. Широкосмуговий шумовий генератор

Цей широкосмуговий шумовий генератор, оптимізований для задач захисту від аудіохуліганів, для прослуховуваннння радіотелепередач на допустимих рівнях гучності. Він перевірений в роботі, простий у виготовлені та настройці, простіший, ніж генератор подавлення радіопередатчиків, число деталей преведено до мінімума. Діапазон випромінюваних частот від сотен кГц до 1 ГГц. Схема настільки проста, що зібрать її може будь-який радіолюбитель. Не потребує настройки, одразу готовий до роботи. Має два вихода - звичайний (MiddleOut) і високої потужності (PowerOut). Використання потужнього вихода посилює використовуємий струм і розігрів елементів. Примусовий обдув при вказанній напрузі живлення обов’язковий.

Монтаж потрібно виконувати з врахуванням потреб СВЧ-пристроя (рис. 3.2) - компактний монтаж, широкі печатні провідники мінімальної довжини, виключення в них різких поворотів, прямих углів, конденсатори

повинні бути високочастотними (навіть керамічні не всі являються такими), і т.д. До  виходa під'єднується трьохрамочна антена (як в генераторі подавлення радіопередавачів), але часто можна обійтись і однією рамкою - залежить від конкретних умов.

Після зборки пристрою перевіряється правильність монтажу, під'єднується до будь-якого виходу шматок метрової проволоки  і  вмикається. Далі потрібно  правильно зорієнтувати плоскість антени і вибрати вихід, який необхідний для приглушення аудіохуліганского дивайса.

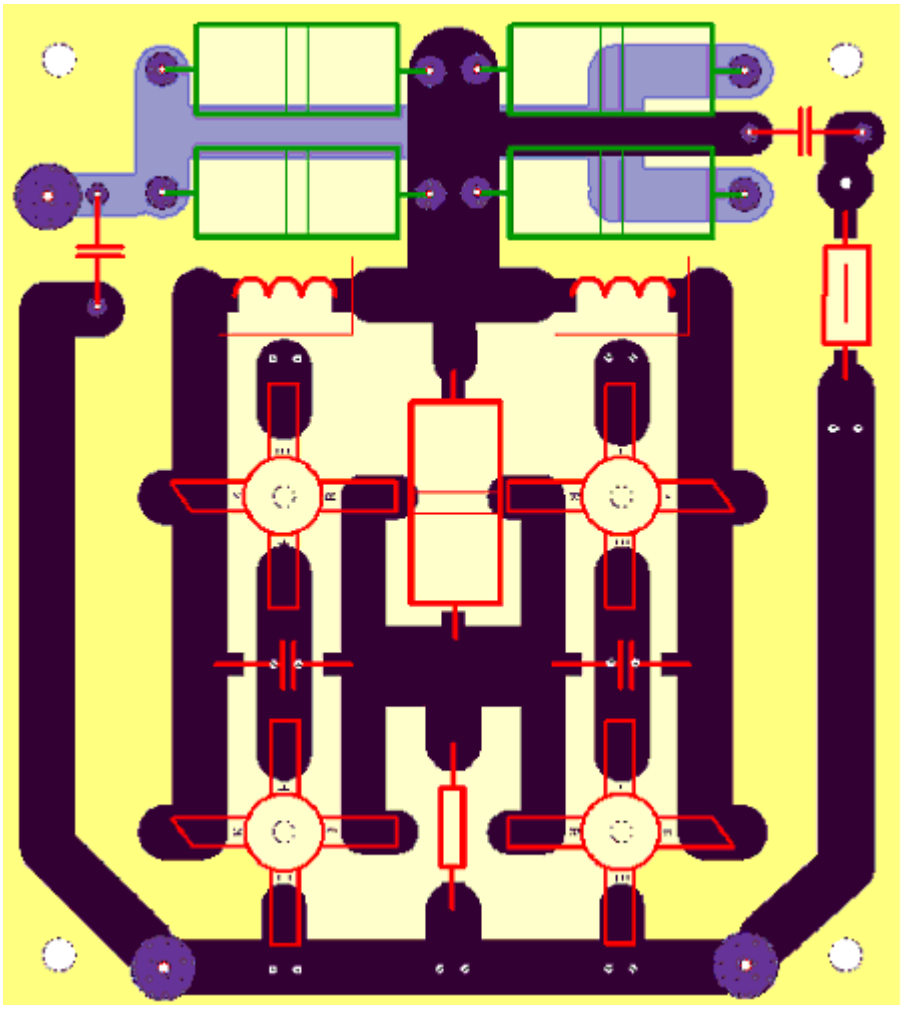

Рисунок 3.2 Друкована плата

Оригінальні разміри печатки 80x90. Конденсатор C5 - навісний. Монтаж (рис. 3.3-3.7) 2-сторонній, переважно поверхневий (SMD). Чорні провідники - верхня сторона печатка, синя - нижня. Крім того, майже на всій нижній стороні плати фольга залишена і заземлена.

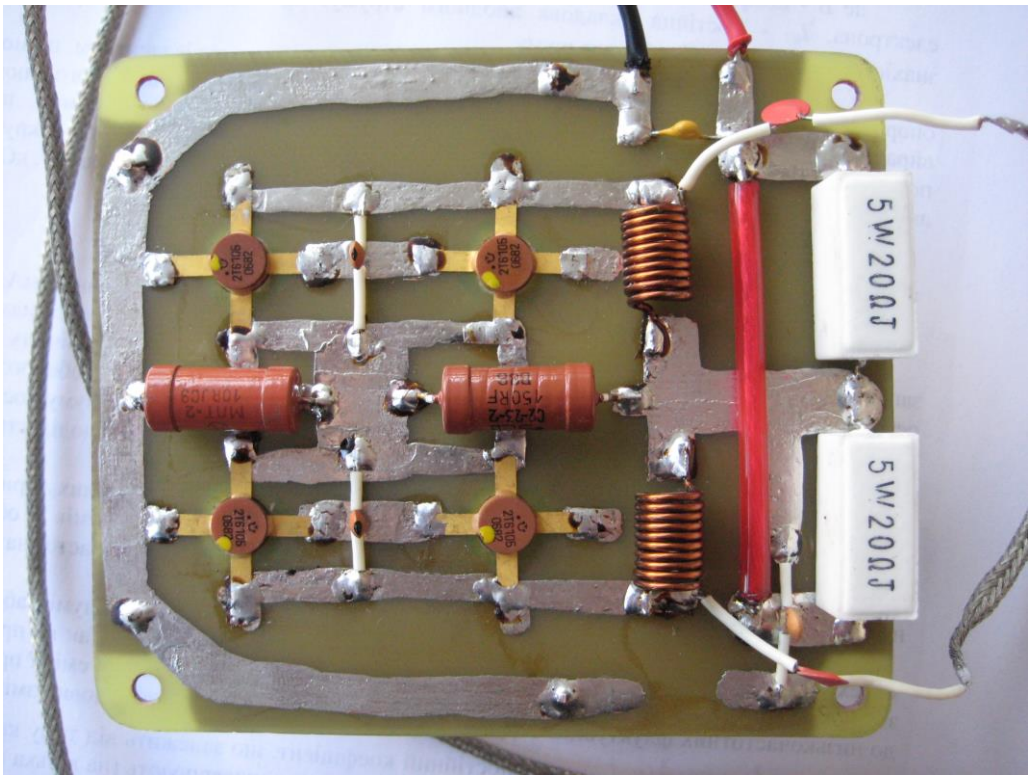


Рисунок 3.3. Друкована плата в зборі (вид зверху)

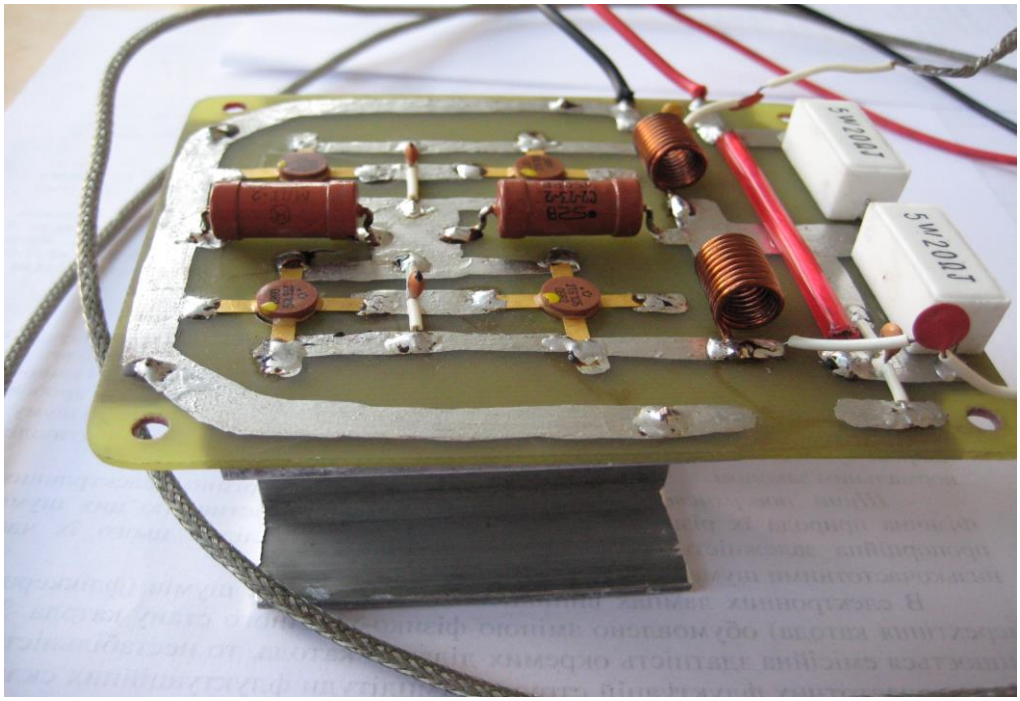


Рисунок 3.4. Друкована плата в зборі (вид збоку)

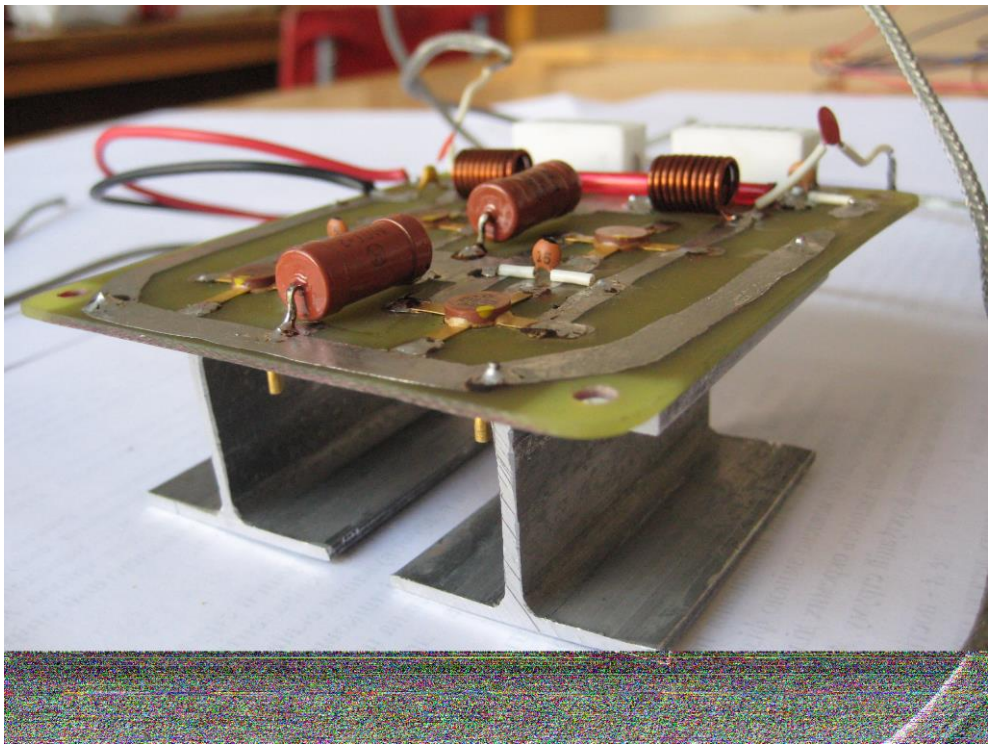

Рисунок 3.5. Друкована плата в зборі (вид під кутом)

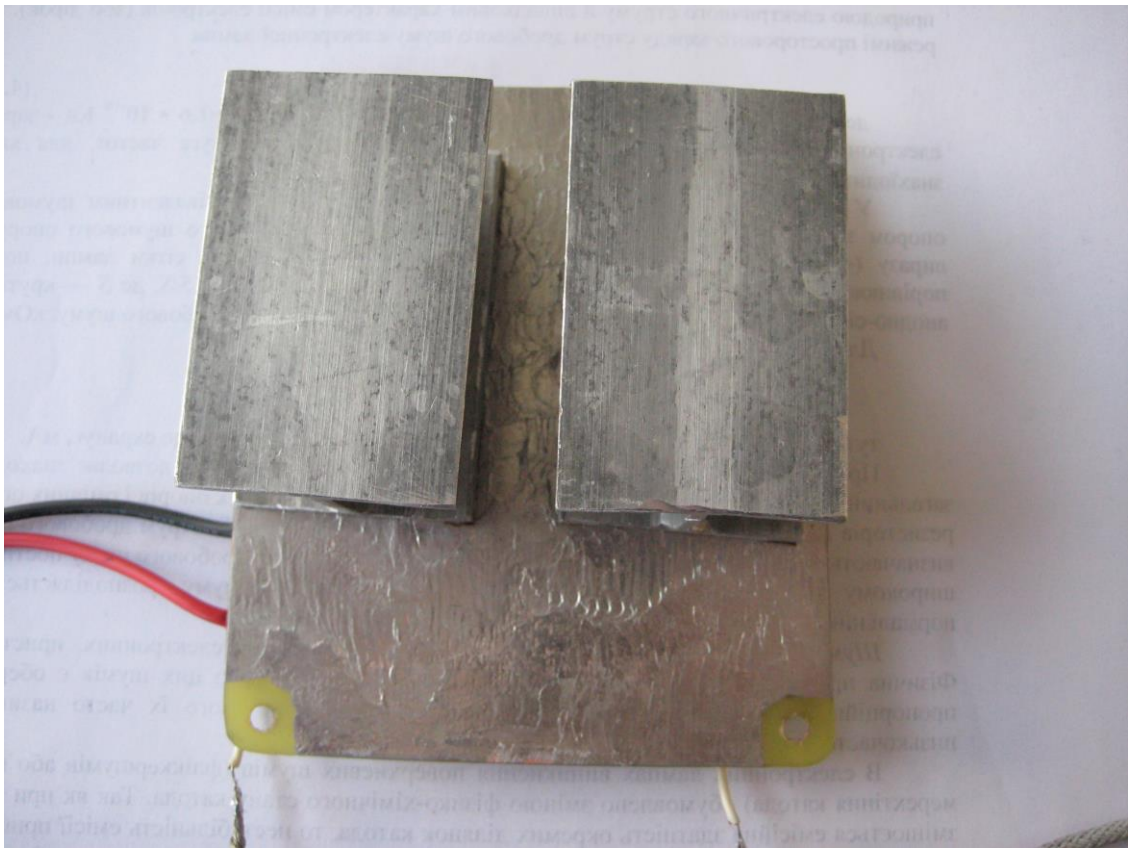

Рисунок 3.6. Друкована плата в зборі (вид знизу)

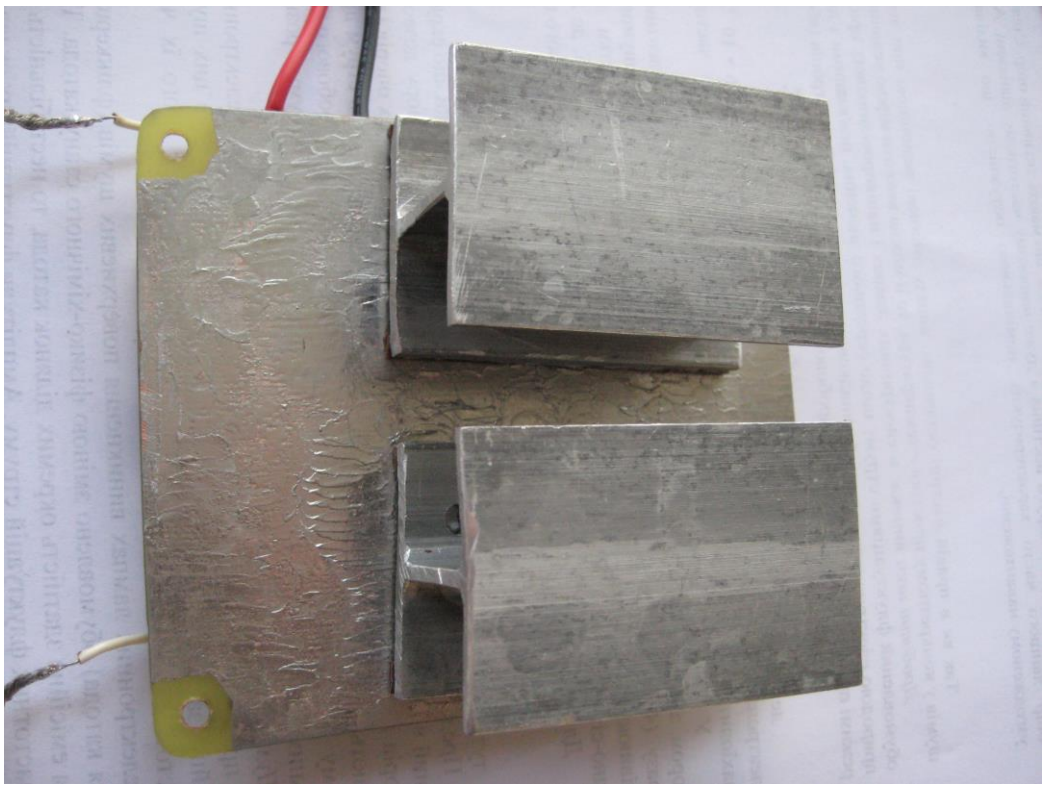

Рисунок 3.7. Друкована плата в зборі (вид знизу збоку)

Виміряні осцилограми, амплітуда шуму і верхня частота показані на рис. 3.8-3.9.

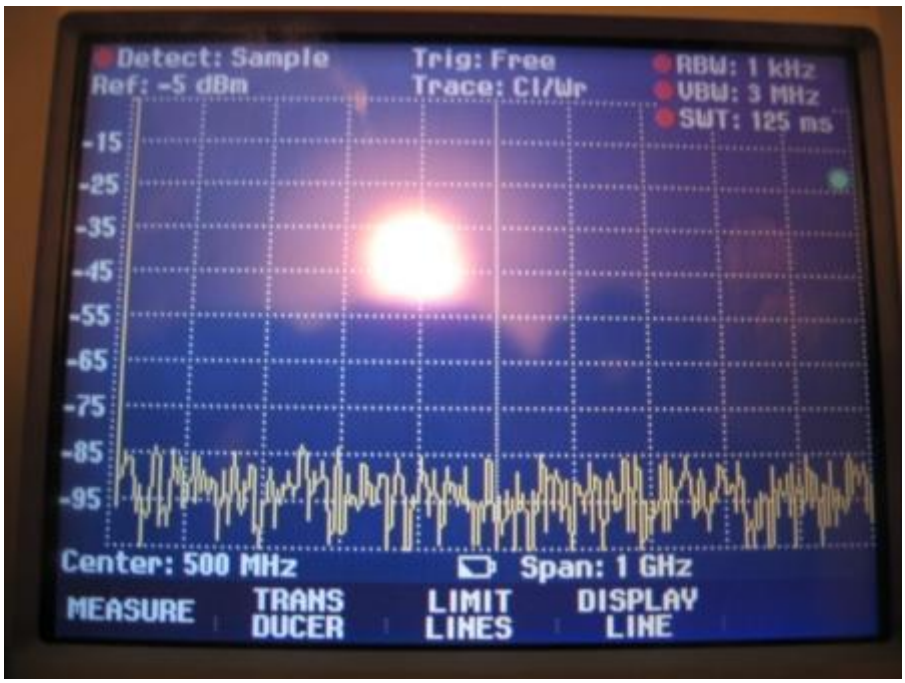


Рисунок 3.8. Шумовий сигнал генератора на осцилографі


Рисунок 3.9. Шумовий сигнал в антені на осцилографі

Головною задачею в цій схемі- це замінить резистор 10 Ом на 20 Ом, 10 Вт у BFG591 то коллектора меньше ніж у кт610, хоча потужність 2 Вт .

Дві штирьові антени підключаються на два „плеча" генератора. Одна через роздільну ємкість в 5 пФ, друга непосредственно на коллектори.

Використовуємий струм 0,45 А.

Схема стійко працює приблизно з 350 МГц до 2500 МГц , нижче можуть спостерігатися нерівномірності АЧХ.

GSM за містом глушить в радіусі 30 метрів.

На рис. 3.10 показана структурна схема пристрою придушення сигналів від мобільних телефонів GSM стандарту.


Рисунок 3.10. Структурна схема пристрою придушення сигналів від мобільних телефонів GSM стандарту

Запропонований пристрій придушення сигналів GSM-телефонів (рис. 3.10) складається з:

- генератор коливаючої частоти;
- двотактного підсилювача потужності;
- пристроїв узгодження з антеною;
- та двох антен.

Робота схеми полягає у наступному генератор коливаючої частоти генерує синусоїдальну напругу високої частоти в діапазоні 850-920 Мгц з двома фіксованими частотами на які перестроюється генератор. З виходу генератора високої частоти сигнал подається на двотактний посилювач потужності високої частоти. Цей підсилювач збільшує рівень завадового сигналу до необхідного значення потужності в антені. На одне „плече" підсилювача під'єднується антена А1 через пристрій узгодження з антеною. Таким чином в антені А1 протікає максимальний струм, що створює необхідну потужність випромінюємих радіохвиль. На інше „плече" під'єднується антена А2 також через пристрій узгодження з антеною та аттенюатор, змінюючи коефіцієнт послаблення аттенюатора можна змінювати струм в антені А2. Таким чином змінюється випромінювана потужність, тобто, зменшується. Блок живлення, що входить до складу схеми забезпечує живлення всіх каскадів генератора завад постійною напругою 12 В. Генератор завад під'єднується до електромережі зі змінною напругою 220 В, 50 Гц. Використовуючи різні антени (А1 чи А2) можна забезпечити необхідний рівень завадового сигналу у захищаємому приміщені:

- або велику потужність для великих приміщень;
- або меншу для невеликих приміщень, тим самим не створюючи завади іншим мобільним пристроям на підприємстві чи в офісі.

# 4 НОРМАТИВНО-ТЕХНІЧНА ДОКУМЕНТАЦІЯ

## 4.1 Законодавче забезпечення охорони інформації

Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повині відповідати їй. На сьогоднішній день законодавча база України по питанням захисту інформації опирається на дії наступних Законів та нормативних актів:

- Закон України “Про інформацію ”;
- Закон України “Про основи Національної безпеки України”;
- Закон України “Про державну таємницю”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах ”;
- Закон України “Про науково-технічну інформацію ”;
- Закон України “Про державну службу спеціального зв’язку та захисту інформації ” ;
- Положення про технічний захист інформації в Україні;
- Концепція технічного захисту інформації в Україні;
- Державний стандарт України. ДСТУ3396 0-96. Основні положення;
- Державний стандарт України. ДСТУ3396 1-96. Порядок проведення робіт.

Закон України “Про інформацію” введений в дію 02.10.92 р. (зі змінами та доповненнями).

Закон України “Про інформацію”

Цей Закон закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. В законі для захисту інформації найбільш важливими є ст.1, ст.5, ст.28, ст.30, ст.39.

Ґрунтуючись на Декларації про державний суверенітет України й Акті проголошення незалежності України, Закон затверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в області інформації.

Стаття 1. Визначення інформації

Поняття ”інформація” цей Закон тлумачить як документовані або привселюдно оголошені зведення про події і явища, що відбуваються в суспільстві, державі і навколишньому природному середовищі.

Стаття 5. Основні принципи інформаційних відносин

Основними принципами інформаційних відносин є:

- гарантованість права на інформацію;

- відкритість, доступність інформації і воля її обміну;

- об'єктивність, достовірність інформації;

- повнота і точність інформації;

- законність одержання, використання, поширення і збереження інформації.

Стаття 28. Режим доступу до інформації

Режим доступу до інформації - це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Держава здійснює контроль за режимом доступу до інформації. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необгрунтованого віднесення відомостей до категорії інформації з обмеженим доступом. Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією заінтерисованих осіб (кількість випадків відмови у наданні доступу до інформації із зазначенням мотивів таких відмов; кількість та обгрунтування застосування режиму обмеженого доступу до окремих видів

інформації; кількість скарг на неправомірні дії посадових осіб, які відмовили у доступі до інформації, та вжиті щодо них заходи тощо).

Стаття 30. Інформація з обмеженим доступом

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюється за їхнім бажанням відповідно передбаченими ними умовами.

Громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного й іншого характеру, отриманої власними засобами, або такої, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного й іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційної, і встановлюють для неї систему (способи) захисту.

Виключення складає інформація комерційного і банківського характеру, а також інформація, правовий режим якої встановлений Верховною Радою України за представленням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків і т.п.), і інформація, збереження якої являє загрозу життю і здоров'ю людей.

До таємної інформації відноситься інформація, що містить відомості, що складають державну й іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, що складають державну таємницю, і доступ до неї громадян здійснюється згідно Закону про цю інформацію.

Порядок обороту таємної інформації і її захисту визначається відповідними державними органами за умови дотримання вимог, установлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Стаття 39. Інформація як товар

Інформаційна продукція та інформаційні послуги громадян і юридичних осіб, які займаються інформаційною діяльністю,можуть бути об'єктами товарних відносин, що регулюються чинним цивільним та іншим законодавством.

Ціни і ціноутворення на інформаційну продукцію та інформаційні послуги встановлюються договорами, за винятком випадків, передбачених Законом.

Стаття 47. Відповідальність за порушення законодавства про інформацію

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну та кримінальну відповідальність згідно з законодавством України.

Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як :

- необгрунтована відмова від надання відповідної інформації;

- надання інформації, що не відповідає дійсності;

- несвоєчасне надання інформації;

- навмисне приховування інформації;

- примушення до поширення або перешкодження поширенню чи безпідставна відмова від поширення певної інформації;

- поширення відомостей, що не відповідають дійсності, ганблять честь і гідність особи;

- використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків;

- розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю;

- порушення порядку зберігання інформації;

- навмисне знищення інформації;

- необгрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом.

Закон України “Про основи Національної безпеки України”.

Загрози національним інтересам і безпеці України в інформаційній сфері:

- обмеження свободи слова та доступу громадян до інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп’ютерна злочиність та комп’ютерний тероризм;

- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

### 4.2 Закон України “Про державну таємницю”

Закон “Про державну таємницю” був прийнятий 21.01.94 р. зі змінами і доповненнями.

Цей Закон регулює соціальні відносини, пов язані з відношенням інформації до державної таємниці, її засекреченням і захистом з метою збереження життево важливих інтересів України в сфері оборони, економіки, зовнішніх відносин, державної безпеки і охороні правопорядку.

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

**державна таємниця** (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості в сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України і які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

**віднесення інформації до державної таємниці** – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з встановленням ступеня їхньої таємності шляхом обґрунтування і визначення можливої шкоди національній безпеці України; у випадку розголошення цих відомостей, включенням цієї інформації в Звід зведень, що складають державну таємницю, і з опублікуванням цього Зводу і змін до нього;

**гриф таємності** – реквізит матеріального носія секретної інформації, що засвідчує ступінь таємності даної інформації;

**державний експерт із питань таємниць** – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці в сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, зміна ступеня таємності цієї інформації і її розсекречення;

**допуск до державної таємниці** – оформлення права громадянина на доступ до секретної інформації;

**доступ до державної таємниці** – надання уповноваженою, посадовою особою дозволу громадянину на ознайомлення з конкретною, секретною інформацією і проведенням діяльності, пов'язаної з державною таємницею або ознайомлення з конкретною секретною інформацією і проведення діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно його службовим повноваженням;

**засекречування матеріальних носіїв інформації** – введення у встановленому законодавством порядку обмежень на поширення і доступ до конкретної секретної інформації шляхом надання відповідного грифа таємності документам, виробам або іншим матеріальним носіям цієї інформації;

**звід відомостей, що складають державну таємницю** – акт, у якому зведені переліки зведень, що відповідно до рішень державних експертів з питань таємниць складають державну таємницю у визначених цим Законом сферах;

**категорія режиму таємності** – категорія, що характеризує важливість і обсяги відомостей, що складають державну таємницю, зосереджених в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

**криптографічний захист секретної інформації** – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою збереження (або відновлення) змісту інформації, підтвердження її дійсності, цілісності, авторства і т.п.;

**матеріальні носії секретної інформації** – матеріальні об'єкти, у тому числі фізичні поля, в яких відомості, що складають державну таємницю, відображені у виді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів і т. п.;

**охорона державної таємниці** – комплекс організаційно-правових, інженерно-технічних, криптографічних і оперативно-розшукових заходів, спрямованих на запобігання розголошення секретної інформації і втратам її матеріальних носіїв;

**режим таємності** – установлений відповідно до вимог цього Закону й інших виданих згідно нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;

**розсекречення матеріальних носіїв секретної інформації** – зняття у встановленому законодавством порядку обмежень на поширення і доступ до конкретної секретної інформації шляхом скасування раніше наданого грифа таємності документам, виробам або іншим матеріальним носіям цієї інформації;

**спеціальна експертиза щодо наявності умов для проведення діяльності, пов'язаної з державною таємницею** – експертиза, що проводиться з метою визначення в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для проведення діяльності, пов'язаної з державною таємницею;

**ступінь таємності** (“особливої важливості”, “абсолютно секретно”, “секретно”) – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї і рівень її охорони державою;

**технічний захист секретної інформації** – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності і недопущення блокування інформації.

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці.

З метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов язаної з державною таємницею;

- обмеження опрелюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об’єктів і технічних засобів, що їм належать;

- особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що проводять діяльність, пов’язану з державною таємницею;

- режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і оганізацій, що проводять діяльність, пов’язану з державною таємницею;

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний та криптографічний захисти секретної інформації.

Закон України “Про Державну службу спеціального зв’язку та захисту інформації України”.

Цей Закон відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв’язку та захисту інформації України.

Цей Закон практично повноваження Департаменту Спеціальних телекомунікаційних систем ЗІ СБУ передає Державній службі ССЗІ України. Ознайомлення з цим Законом необхідний для усіх фахівців, пов’язаних із захистом інформації.

Стаття 2. Статус Державної служби спеціального зв’язку та захисту інформації України

1. Державна служба спеціального зв’язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку:

1.1. Державної системи урядового зв’язку;

1.2. Національної системи конфіденційного зв’язку;

1.3. Захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

1.4. Криптографічного та технічного захисту інформації.

2. Діяльність Державної служби спеціального зв’язку та захисту інформації України спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування.

3. Державна служба спеціального зв’язку та захисту інформації України підконтрольна Верховній Раді України. З питань, пов’язаних із забезпеченням Національної безпеки України, Державна служба спеціального зв’язку та захисту інформації України підпорядковується і підконтрольна Президентові України.

**4.3 Концепція технічного захисту інформації**

Має такі розділи:

1. Загальні положення:

Концепція визначає основи державної політики в сфері захисту інформації інженерно-технічними заходами. ТЗІ є складовою частиною забезпечення національної безпеки України. Концепція може забезпечити єдність принципів формування і проведення такої політики в сферах життєдіяльності особи, суспільства і держави (соціальної, політичної, економічної, військової, екологічної, науково-технічної, інформаційної і т.п.) і служити підставою для створення програм розвитку сфери ТЗІ.

2. Загрози безпеки інформації і стан його технічного захисту:

Відповідно до Концепції одна з основних можливих загроз національній безпеці України в інформаційній сфері – виток інформації, що складає державну й іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави. Напрямок розвитку ТЗІ обумовлюються необхідністю своєчасного проведення заходів, адекватних масштабам загроз для інформації, і будуються на основах правової демократичної держави відповідно правам суб'єктів і інформаційних відносин на доступ до інформації і її захисту.

3. Система ТЗІ:

Система ТЗІ – це сукупність суб'єктів, об'єднаних цілями і задачами з інженерно-технічними заходами, нормативно-правовою і матеріально-технічною базою. Основне правове забезпечення ТЗІ складають: Конституція України, Закон України: “Про основи Національної безпеки України”, «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію», та інші нормативно-правові акти і договори.

4. Основні напрямки державної політики в сфері ТЗІ:

Першочергові заходи щодо реалізації державної політики в сфері технічного захисту інформації, до яких відносять фінансування систем ТЗІ, координування дій і поділ сфер діяльності організаційних структур ТЗІ, а також ієрархічну побудову цих структур, обов'язку захисту інженерно-технічними засобами інформації, що належить до державної таємниці або конфіденційної інформації.

### 4.4 Положення про технічний захист інформації

Положення визначає правові й організаційні основи технічного захисту важливої для держави, суспільства й особистості інформації, охорона якої забезпечується державою відповідно до законодавства.

ТЗІ, здійснюється щодо органів державної влади, органів місцевого самоврядування, органів керування Збройних Сил України й інших військових формувань, підприємств, організацій.

Державна політика ТЗІ, реалізується Державною службою спеціального зв язку та захисту інформації у взаємодії з органами, щодо яких здійснюється ТЗІ.

Організація ТЗІ, в органах, щодо яких здійснюється технічний захист інформації, покладається на їхніх керівників.

Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ, порядок контролю в цій сфері, характеристики погроз для інформації, норми і вимоги до технічного захисту, порядок атестації й експертизи комплексів ТЗІ, визначаються нормативно-правовими актами, прийнятими у встановленому порядку відповідними органами.

Матеріально-технічна база системи ТЗІ, складається з технічних засобів загального призначення і спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що підтверджує їхню відповідність вимогам нормативно-правових актів по ТЗІ, отриманий у порядку, що встановлює Державна служба спеціального звязку та захисту інформації і Комітет України з питань спеціалізації, метрології і сертифікації.

Під час розробки і впровадження заходів щодо ТЗІ, використовуються засоби, дозволені Державною службою спеціального зв’язку та захисту інформації для застосування і включені до відповідних переліків.

Державний стандарт України. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення.

ДСТУ 3396.0-96 отримав чинність від 01.01.1997 р. та втановлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації, неправомірний доступ до якої може завдати шкоди громадянам, організаціям та державі.

Цей стандарт складається із наступних частин:

- галузь використання;
- нормативні посилання;
- загальні положення;
- побудова системи захисту інформації;
- нормативні документи з технічного захисту інформації.

Носіями інформації з обмеженим доступом (ІзОД) можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення. Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, електричної мережі, інженерні комунікації і споруди, повітряне, водне, та інше середовища, грунт тощо.

Мета технічного захисту інформації може бути досягнена побудовою системи захисту інформації, що є організаційною сукупністю методів і засобів забезпечення технічного захисту інформації.

Технічний захист інформації здійснюється поетапно:

1 етап –визначення й аналіз загроз;

2 етап – розробка системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації.

Розробка системи захисту інформації – розробка плана технічного захисту інформації,що включає:

- організаційні заходи захисту ІзОД;
- первинні технічні заходи захисту ІзОД;
- основні технічні заходи захисту ІзОД.

Державний стандарт України.ДСТУ 3396.1-96. Захист інформації.Технічний захист інформації. Порядок проведення робіт.

Цей стандарт отримав чинність від 01.01.1997 р. і має слідуючі розділи:

- галузь використання;
- нормативні посилання;
- загальні положення;
- організація проведення обстеження;
- організація розроблення системи захисту інформації;
- реалізація організаційних заходів захисту;
- реалізація первинних технічних заходів захисту;
- реалізація основних технічних заходів захисту;
- приймання,визначення повноти та якості робіт.

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації. Він також визначає варіанти постанови задач захисту інформації:

- досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності;

- досягнення найбільш можливого рівня захисту ІзОД за досягнутих затрат і заданого рівня обмежень видів інформаційної діяльності;

- досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності.

ЗІ, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту.

Захист інформації, яка становить державну таємницю, забезпечується застосуванням третього варіанту.

Вибір засобів забезпечення технічного захисту інформації зумовлюється фрагментним або комплексним способом захисту інформації. Засоби технічного захисту інформації застосовують автономно або спільно з механічними засобами забезпечення інформаційної діяльності для пасивного або активного приховування ІзОД.

# ВИСНОВКИ

В результаті дипломного проектування було розроблено пристрій для придушення радіосигналів від мобільних телефонів GSM стандарту.

Проведено аналіз існуючих методів і засобів захисту інформації, проаналізовані можливі причини утворення каналів витоку інформації та небезпека витоку інформації цими каналами, розглянуті питання нормативно-правового забезпечення.

Запропоновано розробити комплексну систему захисту інформації на об’єкті інформаційної діяльності.

Розглянуто будову генераторів радіочастотних завад, що дозволяють ефективно придушувати радіосигнали від передавачів в певних діапазонах частот.

Розроблено структурну схему генератора радіозавад для діапазону 890-1912 МГц, в якому працюють мобільні телефони стандарту GSM та деякі радіотелефони.

Виготовлено пристрій для придушення радіосигналів від мобільних телефонів GSM стандарту, який був досліджений та перевірений в ході експерименту і налагоджено на потрібний частотний радіодіапазон.

Також у дипломі розглянута нормативно-правова база в сфері захисту інформації, яка на сьогоднішній день існує в Україні.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Халяпин Д.К. Защита информации в телефонных линиях (каналах) связи // Охрана, № 4. - 2001. - С. 24 - 55.

2. Гирин С.Н., Лысов А.В. Защита информации в телефонных сетях // Разведка, № 4. - 2001. - 52 с.

3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

4. Андрианов В.И., Бородин В.А., Соколов А.В. Шпионские штучки и устройства защиты объектов и информации: справочное пособие. - М.: Лань, 1997. - 272 с.

5. Лазарев Г.П. Защита информации в информационно-телекоммуникационных системах // Безопасность информации, № 2, 2000. - С. 45 - 50.

6. Ананский Е.В. Защита информации – основа безопасности бизнеса. - СПб: «ЛОТ». - 2003. - 230 с.

7. Матвеев В.А., Молотков С.В. Проблемы организации защиты информации. - К.: ООО «ПолиграфКонсалтинг». - 2001. - 330 с.

8. Дмитриев Ю.В., Минаев В.А., Потанин В.Е., Скрыль С.В. Классификация видов угроз безопасности в информационно-телекоммуникационных системах // Журнал депонированных рукописей, № 9. - 2000. - С. 32 - 40.

9. Чернявский А.А. Радиозакладка на частоты 22,95 МГц и 100 МГц // Защита информации: сборник научных трудов. - 2004. - С. 25 - 30.

10. Максименко Г.А., Хорошко В. А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. - К.: ООО «ПолиграфКонсалтинг», 2004. - 317 с.

11. Мусиенко Д.И. Радиоизлучающая подслушивающая аппаратура // «Бизнес и безопасность», №4. - 2004. - С. 23 - 30.

12. Виноградов А.В., Волков В.В. Спецтехника. - М.: Связь, 1996. - 136 с.

13. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. - К.: Юниор, 2003. - 502 с.

14. Ронин Р. Своя разведка: практическое пособие. - М: «АСТ», 2001. - 234 с.

15. Бобнев М.П. Генерирование случайных сигналов. - М.: «Энергия», 1971. - 240 с.

16. Швець В.А., Скворцов С.М., Домарев В.В. Проектування пристроїв систем захисту інформації. - К.: НАУ, 2006. - 38 с.