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
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗОВНІШНІМ ЗАГРОЗАМ ЗА РАХУНОК ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ**

Студент групи СЗД-41 Вєтоха Михайло Сергійович _____
(підпис)

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

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Вєтохі Михайлу Сергійовичу

1.Тема роботи: Організація протидії зовнішнім загрозам за рахунок технічних засобів захисту інформації наказом від « 24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту інформації.

4. Предметом дослідження: технології захисту, які забезпечують захист інформації при її передачі, прийому та обробки інформації.

5. Мета роботи: удосконалення та рекомендації щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз радіотехнічних засобів захисту інформації;
- аналіз акустичних засобів захисту інформації;
- аналіз оптичних засобів захисту інформації;
- створення рекомендацій щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняв до виконання _____Вєтоха М.С.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «____» _____2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 20.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗД -41 Вєтоха М.С. _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Г.В. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 55 сторінок, 3 рисунки, 6 таблиць.

На теперішній час багато задач з технічного захисту інформації, які виникають на об`єктах інформаційної діяльності (ОІД) є актуальними, і їх застосування отримало необхідність в створенні автоматизованих систем (АС), які забезпечують інформаційну динаміку в їх розв`язуванні. Варто відмітити, що на теперішній час принципи створення таких систем відсутні. Основними підходами до їх створення є динамічні зміни в галузі захисту інформації, створення нових інформаційних технологій, швидка заміна програмного та прикладного програмування старого на нове, розширення області загроз інформаційній безпеці, постійна зміна законодавства. В роботі запропоновано визначати окремі показники для здійснення оцінки повноти інформації, її достовірності, її актуальності та її захищеності. Дані показники потрібні для забезпечення технічного захисту інформації. Також розглянуті в роботі комплексні показники, які забезпечують оцінку ефективності захисту інформації.

Об’єктом дослідження: є процеси захисту інформації.

Предметом дослідження є технології захисту, які забезпечують захист інформації при її передачі, прийому та обробки інформації.

Мета роботи удосконалення та рекомендації щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз радіотехнічних засобів захисту інформації;
- аналіз акустичних засобів захисту інформації;
- аналіз оптичних засобів захисту інформації;
- створення рекомендацій щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

ABSTRACT

Thesis contains 55 pages, 3 figures, 6 tables.

At present, many problems of technical protection of information that arise at the objects of information activity (OIA) are relevant, and their application has necessitated the creation of automated systems (AS) that provide information dynamics in their solution. It is worth noting that at present there are no principles of creation of such systems. The main approaches to their creation are dynamic changes in the field of information security, creation of new information technologies, rapid replacement of old software and application programming with new ones, expansion of the field of threats to information security, constant change of legislation. The paper proposes to define certain indicators for assessing the completeness of information, its reliability, its relevance and its security. These indicators are necessary to ensure technical protection of information. The paper also considers complex indicators that provide an assessment of the effectiveness of information protection.

Object there are information security processes.

The subject there are security technologies that ensure the protection of information during its transmission, reception and processing.

The purpose of the work is improvements and recommendations on the use of technical means for information protection at the objects of information activity.

To achieve this goal, the following main tasks are performed:

• analysis of radio engineering means of information protection;

• analysis of acoustic means of information protection;

• analysis of optical means of information protection.

creation of recommendations on the use of technical means for information protection at the objects of information activity.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС	Автоматизована система	Automated system
ОІД	Об`єкт інформаційної діяльності	Object of information activity
НС	Несанкціонований доступ	Unauthorized access
ТЗЗ	Технічні засоби захисту	Technical means of protection
ІБ	Інформаційна безпека	Information security
ЗІ	Захист інформації	Protection of information
РЕБ	Радіоелектронна боротьба	Electronic warfare
РЕЗ	Радіоелектронний захист	Radio electronic protection
РЕП	Радіоелектронна протидія	Electronic countermeasures
РЕЗа	Радіоелектронне забезпечення	Radio electronic support
ЕМВ	Електро-магнітне випромінювання	Electromagnetic radiation
ПЕМВ	Побічне електромагнітне випромінювання	Indirect electromagnetic radiation
ЕМС	Електромагнітна сумісність	Electromagnetic compatibility
ВЧ	Високі частоти	High frequencies
ЗЗІ	Засоби захисту інформації	Means of information protection
АРП	Автоматичне регулювання підсилювання	Automatic gain control
ІТС	Інформаційно-телекомунікаційна система	Information and telecommunication system
УВЧ	Ультра високі частоти	Ultra high frequencies
УНЧ	Ультра низькі частоти	Ultra low frequencies

ВСТУП

На теперішній час розширився спектр методів нападу на інформацію, яка отримується, передається та зберігається на ОІД. Для забезпечення захисту інформації від несанкціонованого доступу (НД) необхідно застосовувати різні технічні засоби. Зняття інформації може бути здійснено по радіотехнічним каналам, акустичним, віброакустичним, оптичним, та за рахунок внутрішніх інсайдерів.

Актуальність теми пояснюється тим, що в загальному комплексі заходів щодо ведення розвідки взагалі, важливою її складовою є технічна розвідка, яка на теперішній час є основним джерелом отримання конфіденційної та таємної інформації.

На основі аналітичних даних було встановлено, що технічна розвідка забезпечує 50% всієї інформації, яка видобувається за рахунок розвідувальних дій. З цього можна зробити висновок, що задачі захисту інформації на ОІД від засобів технічної розвідки є актуальною на теперішній час.

Технічні засоби захисту (ТЗЗ) інформації є невід`ємною складовою наукової та виробничої діяльності підприємств, установ та організацій усіх форм власності.

Варто відмітити, що в сучасних умовах отримав широкого розповсюдження економічний та промисловий шпіонаж, який не має зв`язки з міждержавними, політичними та воєнними протиріччями.

Основною причиною промислового шпіонажу є конкуренція між виробничими, фінансовими ті іншими компаніями. Промисловий шпіонаж на теперішній час охоплює всі кластери ринкової економіки, а в умовах жорсткої конкуренції його масштаби різко зросли.

При здійсненні промислового шпіонажу застосовують технічні засоби отримання інформації. Отже, завдання організації протидії зовнішнім загрозам за рахунок технічних засобів захисту інформації є актуальною на теперішній час.

Об’єктом дослідження: процеси захисту інформації.

Предметом дослідження є технології захисту, які забезпечують захист інформації при її передачі, прийому та обробки інформації.

Мета роботи удосконалення та рекомендації щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз радіотехнічних засобів захисту інформації;
- аналіз акустичних засобів захисту інформації;
- аналіз оптичних засобів захисту інформації;
- створення рекомендацій щодо застосування технічних засобів для захисту інформації на об`єктах інформаційної діяльності.

РОЗДІЛ 1 ЗАХИСТ ІНФОРМАЦІЇ В РАДІОТЕХНІЧНИХ КАНАЛАХ

1.1. Концептуальна модель інформаційного захисту

В загальному випадку інформаційна безпека (ІБ) – це стан захищеності інформаційного середовища суб`єктів, яке забезпечує їх формування розвитку для інтересів суспільства та підприємств. З цього можна зробити висновок, що для забезпечення захисту інформації (ЗІ) необхідно визначити загрози ІБ, джерела цих загроз, способи та реалізацію мети ЗІ, а також інші умови та наміри з діями, які направленні на порушення ІБ. В такому сенсі варто впроваджувати і заходи ЗІ від несанкціонованих дій, які носять незаконний характер і які призводять до збитків.

Досвід показав, що для здійснення аналізу множини джерел, об`єктів та дій варто здійснювати моделювання за допомогою існуючих методів, та створювати нові, за допомогою яких здійснюється імітація реальних ситуацій. Однак, варто враховувати той факт, що модель має певні припущення, яких не існує в реаліях. Однак, не зважаючи на це, модель повинна узагальнювати всі ключові фрагменти реальної картини, що в свою чергу дає можливість здійснити опис реальних заходів з урахуванням їх складності.

На рисунку 1.1 представлено концептуальну модель інформаційної безпеки. Дамо більш детальний зміст кожної компоненти даної моделі.

***Об`єкт загроз*** ІБ є дані про склад, стан та діяльність об`єкту захисту, а саме персоналу, матеріальних та фінансових активів та інформаційних ресурсів.

Загрози інформації - це намагання порушити цілісність її, отримати несанкціонований доступ до конфіденційної інформації, порушити її повноту та здійснити намагання її заблокувати.

Джерела загроз- це конкуренти, злодії, корупціонери, адміністративно-керуючі органи.

Метою джерел загроз ознайомлення з відомостями, їх модифікація з метою користі та знищення для нанесення прямого матеріального убутку.

Несанкціоноване заволодіння конфіденційної інформації, або отримати несанкціонований доступ до неї - спроможність за рахунок її розголошення, за рахунок витоку інформації через технічні канали та за рахунок несанкціонованого доступу до інормації, яка охороняється.

Джерелами конфіденційної інформації є люди, документи, публікації, технічні носії інформації, технічні засоби, які забезпечують виробничу та трудову діяльність, продукція та відходи від виробництва.

Основним вектором ЗІ є правовий, організаційний та інженерно-технічний ЗІ. Об`єднання цих трьох складових забезпечує комплексний підхід щодо забезпечення ІБ.

Засоби захисту інформації - це фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Криптографічні методи реалізуються як апаратними, програмними, а також комбіновано програмно-апаратними засобами.

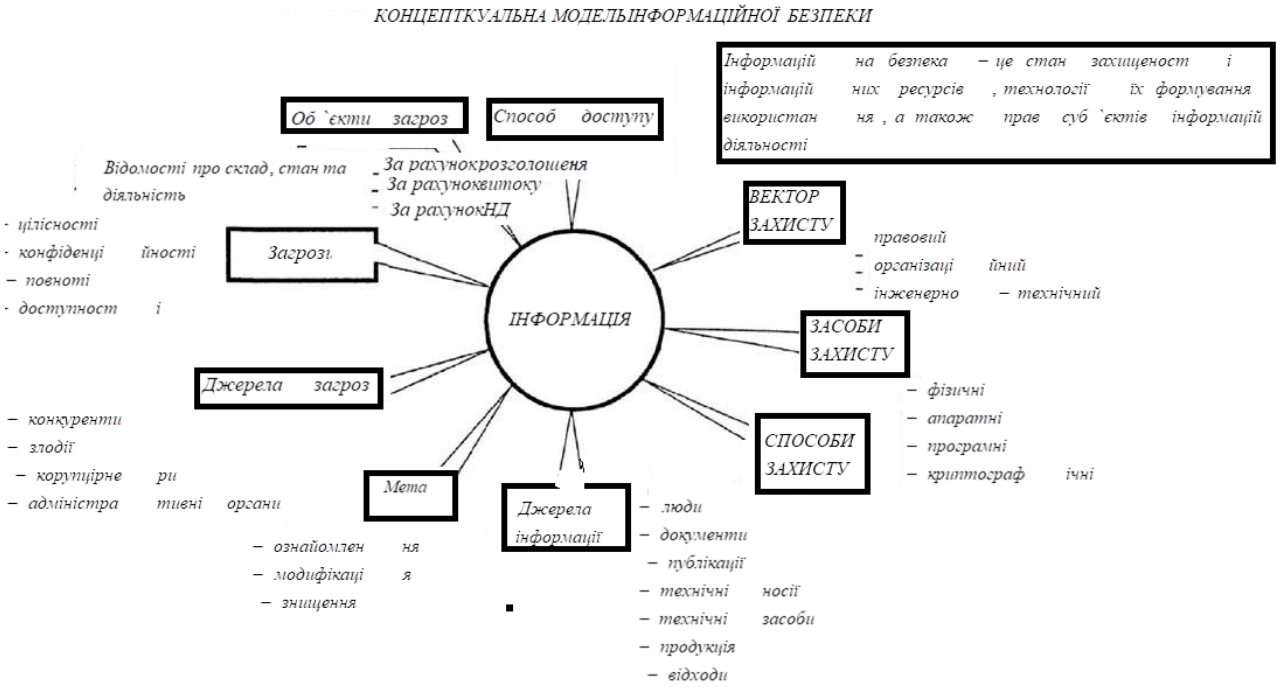


Рисунок 1.1. Концептуальна модель інформаційної безпеки

Способи захисту – це заходи, шляхи, способи та дії, які забезпечують запобіганню проти правових дій, їх запобіганню, перетин та протидія несанкціонованому доступу.

На теперішній час самим популярним способом передачі та прийому інформації є передача та прийом завдяки радіохвилям. Це пов`язано з тим, що такий спосіб зв`язку має властивість мобільності, має велику швидкість передачі та прийому інформації, та достатньо дешевий по відношенню до інших способів. При веденні бойових дій важливим критерієм зв`язку є мобільність. Це і є основним мотивом використовувати канали радіозв`язку.

При забезпеченні конфіденційного зв`язку в умовах бойових дій необхідно розглядати три зацікавлені сторони, а саме джерело передачі інформації, приймач інформації та сторона, яка зацікавлена в несанкціонованому доступі до цієї інформації. Такі системи радіозв`язку мають властивість асиметрії. На рисунку 1.2, представлено узагальнену організацію конфіденційного радіозв`язку.

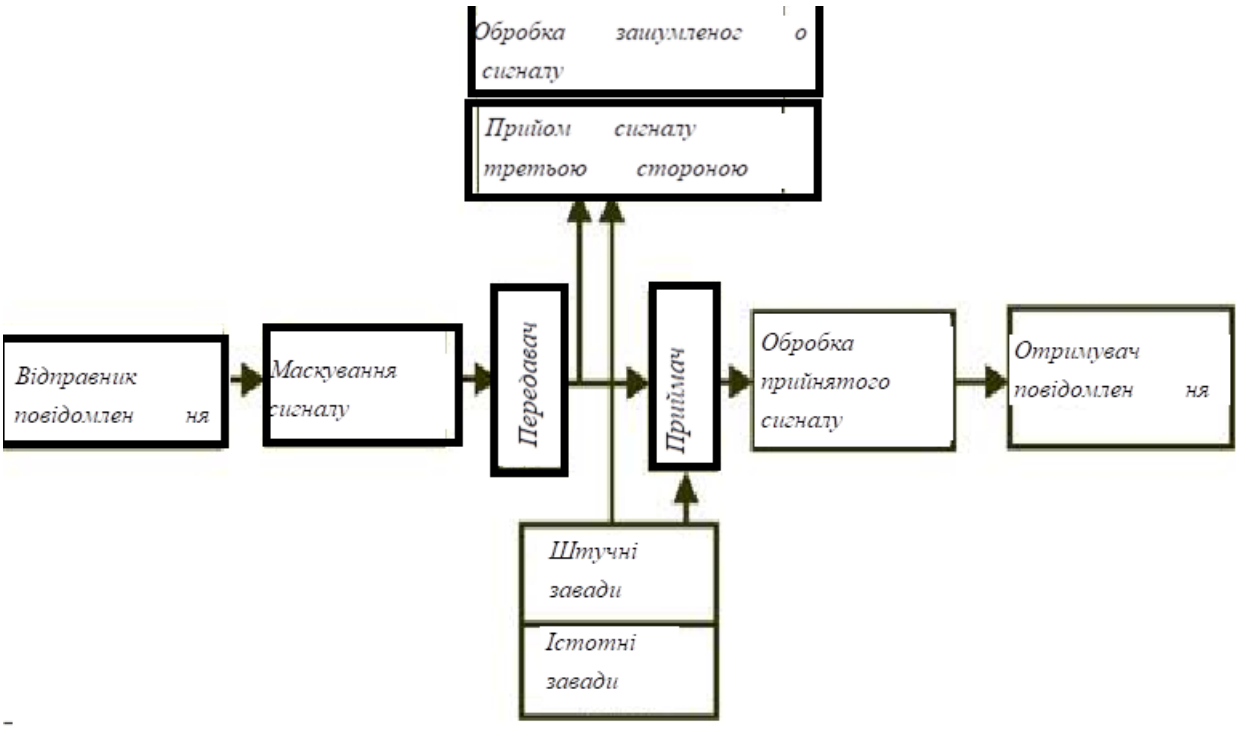


Рисунок 1.2. Структурна схема організації передачі конфіденційної інформації по каналу радіозв`язку.

З рисунку 1.2 видно, що відправник повідомлення за рахунок вибору каналу радіозв`язку обирає оптимальний спосіб передачі повідомлення. Якщо повідомлення, яке відправляється є конфіденціальним, то відправник здійснює додаткове шифрування цього повідомлення. В окремих випадках, щоб здійснити великі труднощі для перехоплення повідомлення, що відправляється, то здійснюється маскування штучними завадами. Способи, за якими здійснюється кодування, шифрування та маскування повідомлення, що відправляється, відомі отримувачу, який здійснює інверсію: виділення корисного сигналу з шуму, декодування та розшифрування.

Радіоелектронна боротьба (РЕБ) — це сукупність узгоджених за цілями, задачами, області та часу заходів та дій військ щодо визначення радіоелектронних засобів та систем керування військами та озброєнням противника, знищення його всіма видами озброєння або захоплення , а також щодо радіоелектронного захисту власних радіоелектронних об`єктів та систем керування військами та озброєнням. На рисунку 1.3 представлено структурну схему задач РЕБ.

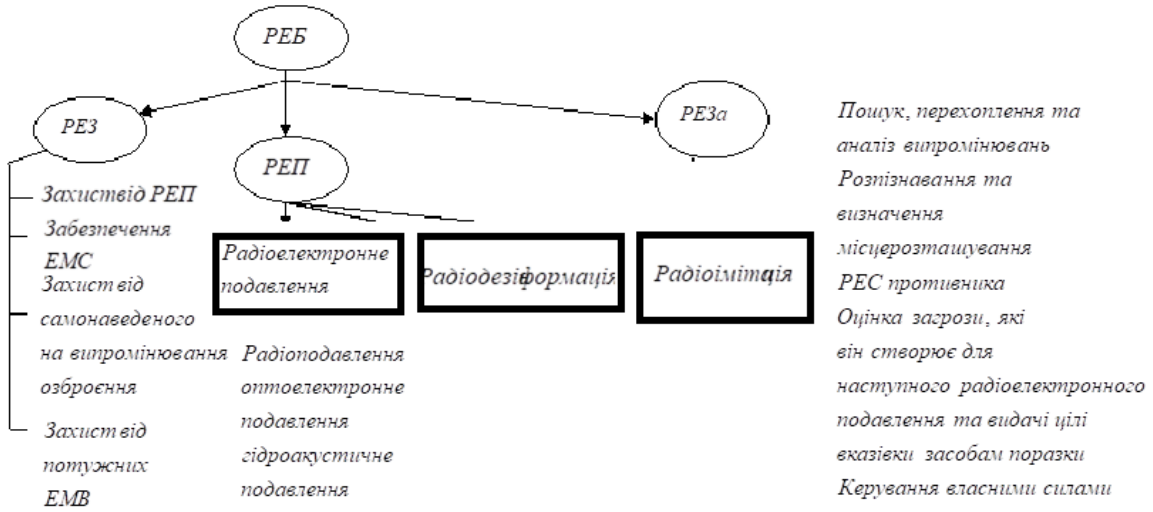


Рисунок 1.2. Схема задач радіоелектронної боротьби

1.2. Радіоелектронний захист в системах інформаційного захисту

Основним завданням радіоелектронного захисту є необхідною умовою для забезпечення стійкого керування власними військами та озброєнням. В РЕС входять чотири складові, які виконують свою функцію:

- захист від навмисних завад, які створює ворог;
- захист від ненавмисних власних завад та завад від ворога РЕС – забезпечення електромагнітної сумісності (ЕМС);
- захист від озброєння, яке от наводиться самостійно;
- захист від потужного електромагнітного випромінювання (ЕМВ).

Навмисні завади здійснюються для погіршення прийому сигналів з метою зробити складність його обробки. Крім того, вони призводять до того, що кінцева апаратура здійснює хибний вихід. Це призводить до того, що інформація, яка передається пошкоджується , або взагалі знищується інформація, яка зберігається в реєстрах та базах даних. Крім того, такі завади вводять в оману при здійсненні оцінки радіоелектронного оточення. Це призводить до прийняття хибних інформаційних рішень.

Завади можуть бути істотними та штучними. Істотні завади виникають за рахунок атмосферних змін, за рахунок впливу іоносфери, за рахунок космічного радіовипромінювання, за рахунок відбиття хвиль від предметів, що оточують, за рахунок геомагнітних умов в області функціонування інформаційно-телекомунікаційних систем (ІТС).

Штучні завади виникають за рахунок сторонніх передавачів або засобами електричного обладнання, які носять назву індустріальних завад, а також за рахунок навмисного наведення завад.

Навмисні завади розрізняють за способом їх створення. Існують активні завади, які виникають за рахунок генерації особливих передавачів, та пасивні, які виникають за рахунок відбиття хвиль, які випромінюються від РЕС, а також від різноманітних відбивачів або за рахунок штучної зміни електромагнітних властивостей середовища.

Активні завади. Передавачі завад адаптуються до частот, на яких здійснюється придушення радіоелектронними засобами інформаційно-комунікаційних систем. ***Завади, що пригнічують***, здійснюють вплив на ті підсистеми, які забезпечують обробку сигналів. Такі завади здійснюють руйнування важливої інформації, яку передають поточні сигнали радіоелектронними засобами, до моменту її надходження до систем обробки інформації. Завади, що пригнічують, мають спроможність досягти своє мети за рахунок більшої власної потужності над потужністю корисного сигналу, тобто виконується нерівність

$$\frac{P_{\text{int}\,reference}}{P_{useful}} > 1, \qquad (1.1)$$

де $P_{\text{int}\,reference}$ - потужність завади, P_{useful} - потужність корисного сигналу.

Імітаційні завади призначені для того, щоб в системі обробки інформації, за рахунок придушення радіоелектронними засобами вхідних сигналів, було вилучено зловмисником хибну інформацію. Такий вид завад в багатьох випадках імітує сигнали, які випромінюються радіоелектронними засобами. Ефективність цих перешкод тим більша, чим ближча форма спектру завади до форми спектру корисного сигналу.

Диверсійні завади, призводять до того, що в системах обробки інформації та в системах керування змінюються алгоритми обробки корисних сигналів та інформації. В таблиці 1.1 представлено множину всіх існуючих завад.

Таблиця 1.1. Види завад

Завади за способом впливу на канал зв`язку	- Імітаційні -Диверсійні -Завди що пригнічують
За структурою	- Імітаційні

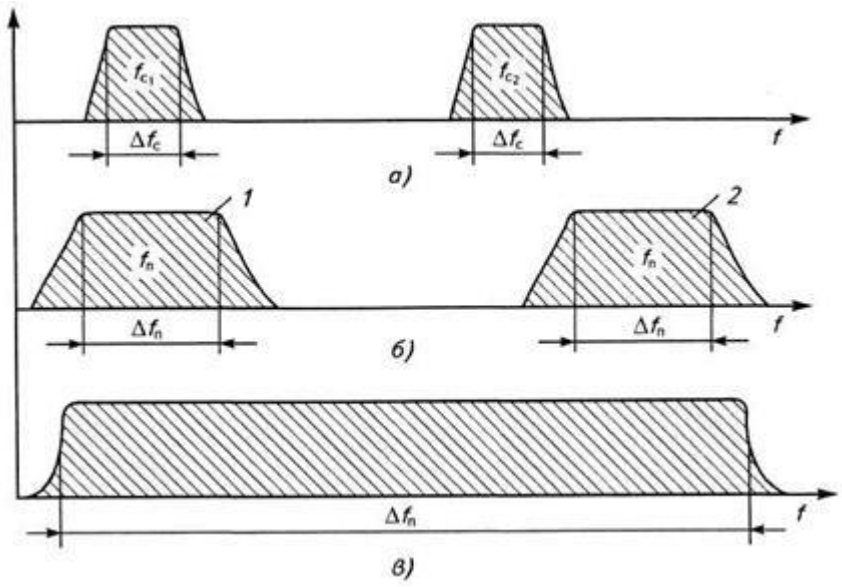
	- Шуми - завади, які корелюються з корисним сигналом
За часом	- Прицільні - Неперервні
За частотою	- Прицільні - Загороджувальні
За простором	- Прицільні - Загороджувальні - Зосереджені, тобто випромінювання здійснюється з однієї конкретної координати - Розподілені, тобто випромінювання здійснюється з різних координат простору
За принципом створення	- Ретрансляційні, тобто завади, які приймаються, підсилюються і яким притаманне отримання додаткової модуляції множиною завад - Генераторні – передавачі завад
За видом модуляції	- Прямий шум, тобто відбувається підсилення істотного шуму завдяки генератора завад - Модульовані шуми по амплітуді, фазі, частоті, поляризації - регульовані за модуляцією

Загороджувальні завади виникають в широкій смузі частот, яка в десятки та сотні разів перевищують смугу пропускання приймача, який

подавляється. Особливістю цих завад є те, що при незмінній потужності їх передавача спектральна щільність N_n потужності завад зменшується з розширенням спектру випромінювання, як показано на рисунку 1.3 в).

Прицільні завади виникають в достатньо вузькій смузі частот, яка не перевищує двох або трьох стійких смуг пропускання приймача. Ці завади мають властивість великої спектральної щільності завад, так як випромінюються в вузькому спектрі частот, як показано на рисунку 3.1 б).

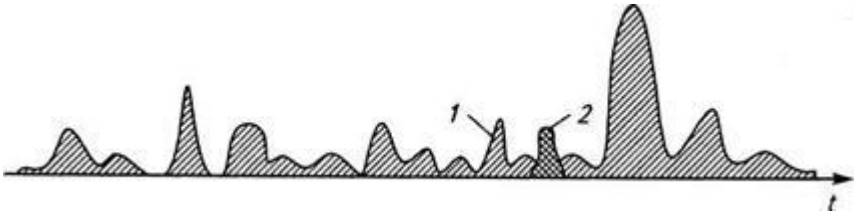
Шумові завади мають властивість хаотичної зміни амплітуди, частоти або фази виходу. Шум, характеристики якого зберігаються постійним в широкому діапазоні частот, і який носить назву білий шум. Так як вони за своєю структурою близькі з внутрішніми флуктуаційними шумами приймача, то іх в багатьох випадках буває важко виявити, що стає важким прийняти заходи щодо послаблення завад, як показано на рисунку 1.4.



а – сигнали, які подавляються; б – прицільна завада 1 збігається за частотою з корисним сигналом 2; в – загороджувальна завада.

Рисунок 1.3.Подавлення радіоелектронних засобів

Джерелом активних завад є спеціальні станції. Вони проектуються виходячи з їх призначення, діапазоном частот та місцем розташування. Станції завад як правило встановлюються в автівках, літаках, гвинтокрилах, а прилад для виконання функції таких станцій є переносним і розташовано як правило в кейсі. Також існують станції і одноразового використання. Передавачі завад, які закидають можуть бути принесені ракетами, артилерією, засобами нападу з повітря, а також диверсійно-розвідувальними групами, представниками організованої злочинності.

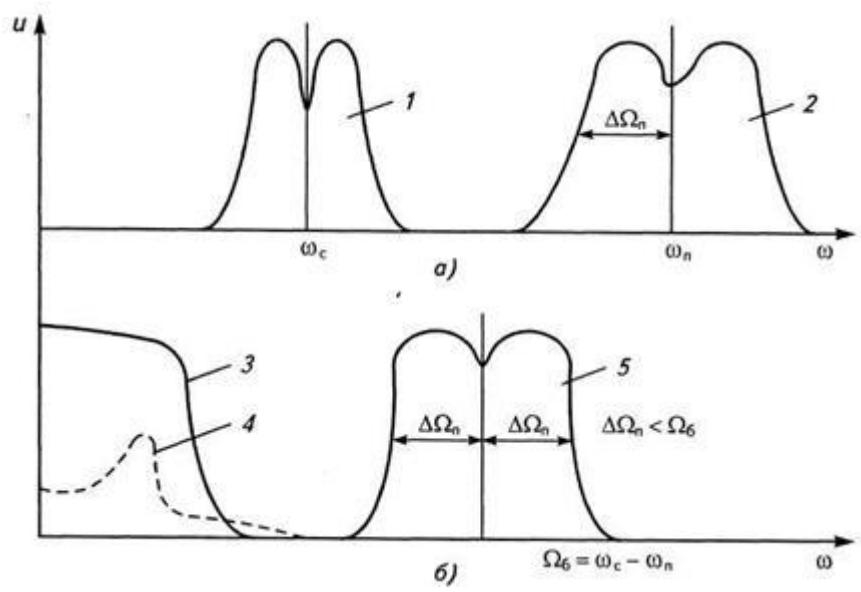


1 - завади; 2 – інформативні сигнали.

Рисунок 1.4. Шумові завади

Передавачі завад, які закидають, варто використовувати для локальної блокади вузлів зв`язку, спеціальних приміщень основного та другорядного призначення технічних засобів , охоронних систем.

На рисунку 1.5 представлено модуляцію завад за амплітудою. Створюється модуляція амплітуди напруги несучого коливання від передавача завад за рахунок гармонійних коливань Ω_n.



а – спектри інформативного сигналу 1 та завади 2 на вході приймача; б - результуючий спектр на виході детектора (3 - завада; 4 - інформативний сигнал; 5 - биття).

Рисунок 1.5. Вплив амплітудно-модульованої завади на радіо зв`язок.

За рахунок впливу напруги сигналу U_{Ω_c}, завади $U_{\Omega_п}$ виникає биття $U_{\Omega_б}$. Це призводить до спотворення інформативного сигналу в радіотехнічному обладнанні або маскуванню в обладнанні радіолокації інформативного сигналу.

З практичної точки зору при проектуванні систем та засобів радіозв`язку на теперішній час створені методи та обладнання технічного захисту тільки від маскуючих та структурних завад, які входять в групу пригнічених завад.

1.3. Захист від завад радіоелектронних засобів

Завада гасить приймальне обладнання РЕС тоді і тільки тоді, коли відношення потужності завади, яка виникає в його смузі пропускання, до потужності інформативного сигналу значно більше параметра, який характеризує даний тип завад та характеристик приймача.

Найменше необхідне відношення потужностей завад сигналу на вході приймача, в межах лінійної частини смуги пропускання, при якому досягається необхідний рівень пригнічення, є коефіцієнт пригнічення за потужністю, який має наступне представлення:

$$K_n = \min\left(\frac{P_n}{P_c}\right). \tag{1.2}$$

Досвід показав, що варто застосовувати коефіцієнт пригнічення за напругою, який має наступне представлення:

$$K_{пн} = \sqrt{\frac{E_n \cdot P_n}{\min(E_c) \cdot \min(P_c)}}. \tag{1.3}$$

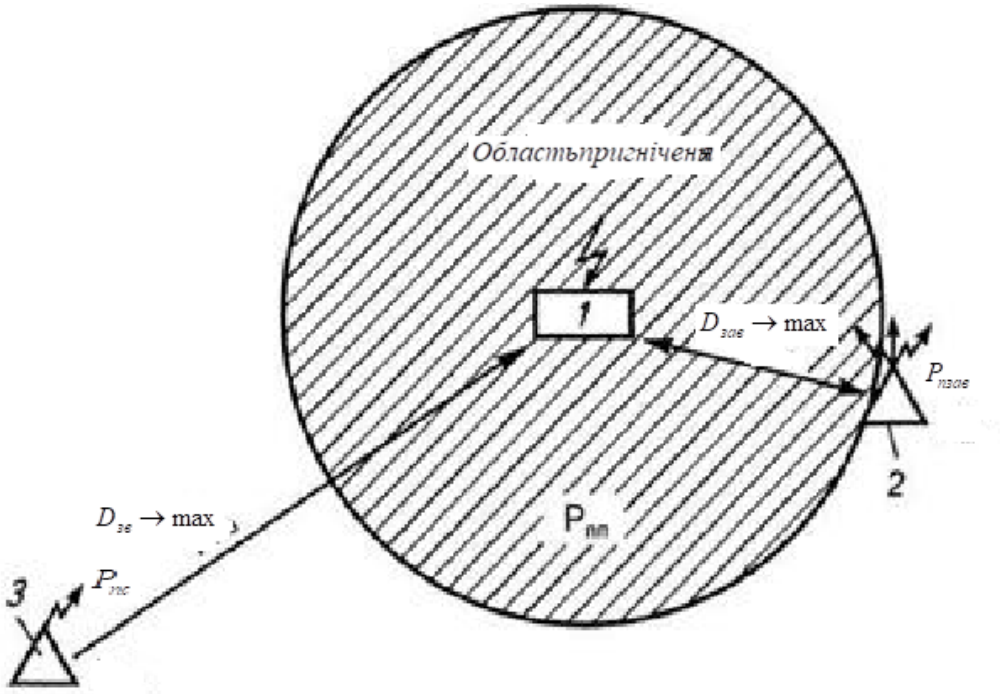
В загальному випадку коефіцієнт пригнічення для імпульсних та аналогових сигналів та завад обчислюють як відношення їх відповідних потужностей.

Заваду прийнято вважати якісною, якщо на вході приймача виконується нерівність

$$K_{пн} > K_n. \tag{1.4}$$

Області пригнічення каналів радіозв`язку в залежності від енергетичних параметрів та форм діаграм векторів антен, які розташовані на станціях радіозв`язку та завад, відрізняються одна від одної. Взагалі області пригнічення радіозв`язку уявляють собою фігуру, яка за своєю формою співпадає з діаграмою вектору антен приймача та з межею $M_n$, яка проведена з точки знаходження приймача, який пригнічується. При застосуванні багатовекторних антен в каналі радіозв`язку та в станціях завад ($G = 1$) область пригнічення уявлятиме круг, як представлено на рисунку 1.6. Для пониження якості завади, тобто ухилення від завади за рахунок застосування станціями радіозв`язку векторних антен,

необхідно щоб форма області пригнічення радіоелектронних засобів визначалась векторною діаграмою антени, яка приймає.



1 – приймач, який пригнічується; 2 - передавач завад; 3 - передавач інформативного сигналу; $D_{зв} \to \max$ - дистанція зв`язку, $D_{зав} \to \max$ - дистанція завади.

Рисунок 1.6. Область пригнічення радіозв`язку при застосуванні в приймачі багатовекторних антен.

Якщо переріз області подолання, який паралельний площині XoY декартової системи координат, має форму «петлі», тобто має аналітичне представлення $G_{прп}(\theta) = G_{пр} \cdot \cos^2(\theta)$ і графічне представлення зображено на рисунку 1.7,

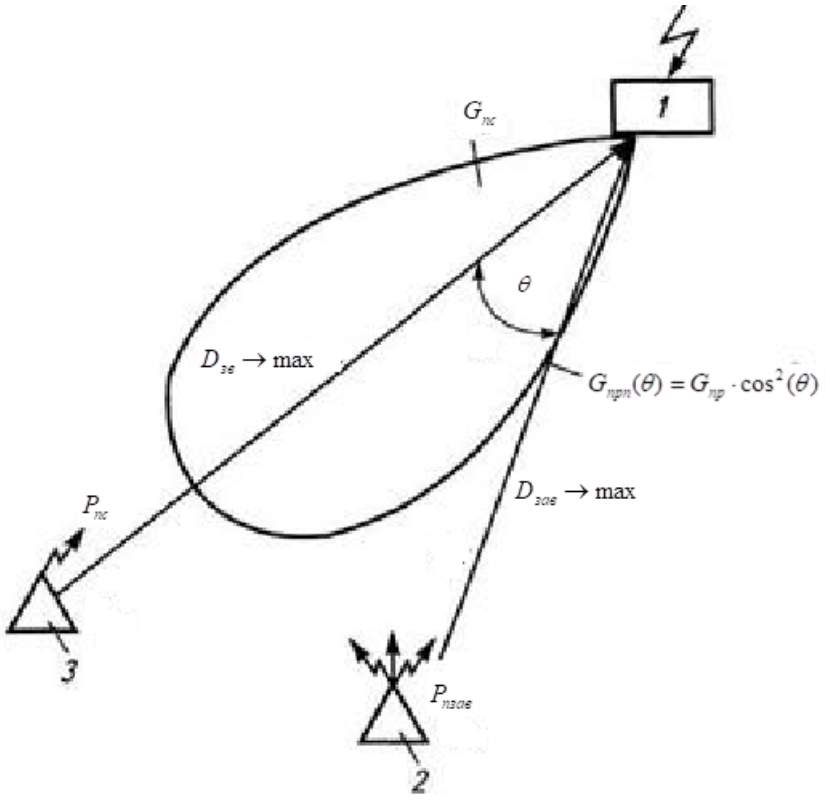


Рисунок 1.7. Область пригнічення радіозв`язку при застосуванні в приймачі гостро векторної антени.

1 – приймач, який пригнічується; 2 - передавач завад; 3 - передавач інформативного сигналу; $D_{зв} \to \max$ - дистанція зв`язку, $D_{зав} \to \max$ - дистанція завади.

Область пригнічення буде при цьому мати наступне представлення

$$D_n = D_{св} \sqrt{\frac{P_{пз} \cdot G_{пз} \cdot \Delta f_{пр} \cdot \gamma_{п(з/с)}}{P_{ic} \cdot K_n \cdot G_{пс} \cdot \Delta f_з}} \cdot \cos^2(\theta), \qquad (1.5)$$

де $P_{пз}$ - потужність передавача завад, P_{ic} - потужність передавача інформативного сигналу; $G_{пз}$ -коефіцієнт підсилення антени передавача завад, $G_{пс}$ - коефіцієнт підсилення антен передавача інформативного сигналу. Якщо виконується рівність $G_{пз} = G_{пс}$, то завади рухаються по основній пелюстці векторної діаграми антени приймача; $\Delta f_{пр}$ - смуга пропускання приймача, а $\Delta f_з$

ширина спектру завади; $\gamma_{п(з/с)}$- коефіцієнт відмінності поляризації завади та інформативного сигналу, який належить відрізку [0;1].

Найбільш допустима відстань між передавачем завад і приймачем, який пригнічується і при цьому здійснюється якісне порушення радіозв`язку, має наступне представлення:

$$D_{зав} \to \max = D_{зв} \to \max \cdot \sqrt{\frac{P_{пз} \cdot \Delta f_{пр} \cdot \gamma_{п(з/с)}}{P_{іс} \cdot K_{п} \cdot \Delta f_{з}}}. \quad (1.6)$$

В даному приведенні захищеність від завад засобів радіозв`язку забезпечується за рахунок оптимального вибору відстані зв`язку, яка менша за відстань від завад, самою антеною, забезпечення того, щоб потужність інформативного сигналу вища за потужність завади, тощо. Окремо варто зазначити, що якість завади, яка пригнічує, можна значно зменшити за рахунок організації прийому та передачі на розподілених частотах, та застосуванням систем радіозв`язку за рахунок зміни частоти за псевдовипадковому розподілу. Також використовуються засоби для пошуку станцій розповсюдження завад з подальшим фізичним їх знищенням. В існуючих джерелах визначається, що в розділах захисту радіоелектронних засобів від навмисних завад якісно вивчена та описано на рівні методів кількісних оцінок тільки дуже вузька сфера захисту від завад для окремих радіоелектронних засобів і тільки для одного виду серед трьох радіо завад.

1.4. Забезпечення електронної сумісності радіоелектронних каналів

В наслідок дії інтенсивних завад на радіоелектронний захист, відбувається перевантаження, і як наслідок приймач не спроможний реагувати на варіацію вхідного сигналу. Істотно, що при цьому приймач не може відтворювати

повідомлення. Перевантаження можуть виникати в довільній складовій приймача: у вхідних і вихідних підсилювальних каскадах, в підсилювачах проміжної частоти та у демодуляторах.

Один із найпростіших та ефективних способів уникнути перевантаження є - автоматичне регулювання посилення (АРП).

В процесі функціонування автоматичного регулювання підсилювання амплітуда напруги на виході, ультра низькі частоти (УНЧ) розпізнаються за допомогою детектору АРП, на який подається ще й напруга затримки $U_з$, посилюється і здійснюється процес середнього фільтром нижніх частот. Вихідна напруга, що регулюється, $U_Р$ підлягає керуванню значенням коефіцієнта посилення УНЧ приймача $k_{УПЧ} = k(U_Р)$ для того, щоб підтримувати сигнал на виході демодулятора на постійному прийнятному рівні

$U_{вих} = K(U_р) \cdot U_{вх}$, при умові виконання рівності $U_{вих} = U_з$.

Отже, час затримки спрацьовування залежить від значення $U_з$ яке чисельно визначає пороговий рівень вхідного сигналу, при перевищенні якого амплітудою вхідного сигналу спрацьовує система АРП. АРП "*вперед*". Таким чином, ми маємо якісний метод захисту від завад, що мають більшу тривалість, ніж імпульси сигналу $\tau_п > \tau_с$. Структурна схема такої системи АРП представлено на рисунку 1.8.

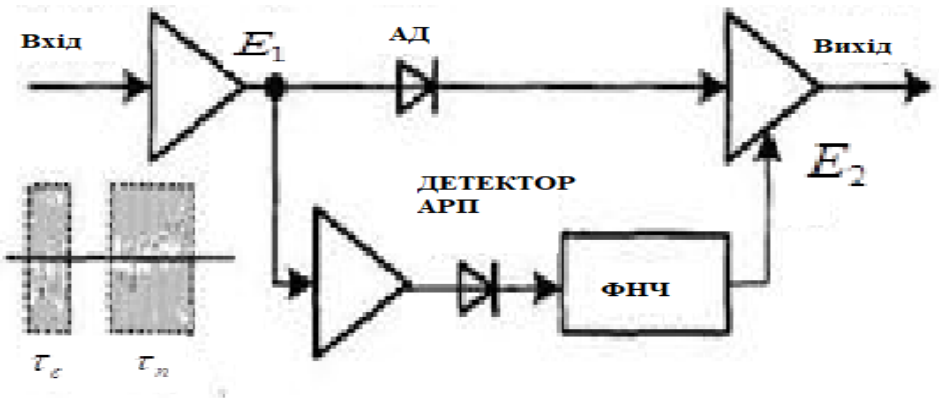


Рисунок 1.8. Структурна схема системи АРП "*вперед*".

В цьому випадку константа часу визначається наступним чином

$$\tau_{АРП} = \frac{1}{\Delta F_{ф}} > \tau_{c}\,. \tag{1.7}$$

В той момент часу, коли надходить імпульс сигналу час тривалості якого τ_c значення коефіцієнта посилення відео підсилювача $K(E_2)$ становиться максимальним, а протягом часу надходження довгого імпульсу завади, тобто при виконанні нерівності $\tau_n > \tau$, відбувається швидке зменшення цього значення і завада на виході послаблюється.

Автоматичне регулювання підсилювання "*за ближніми шумами*" уявляє собою швидке автоматичне регулювання посилення за шумовою завадою, що передує появі сигналу. Робота такої системи представлено осцилограмою на рисунку1.9.

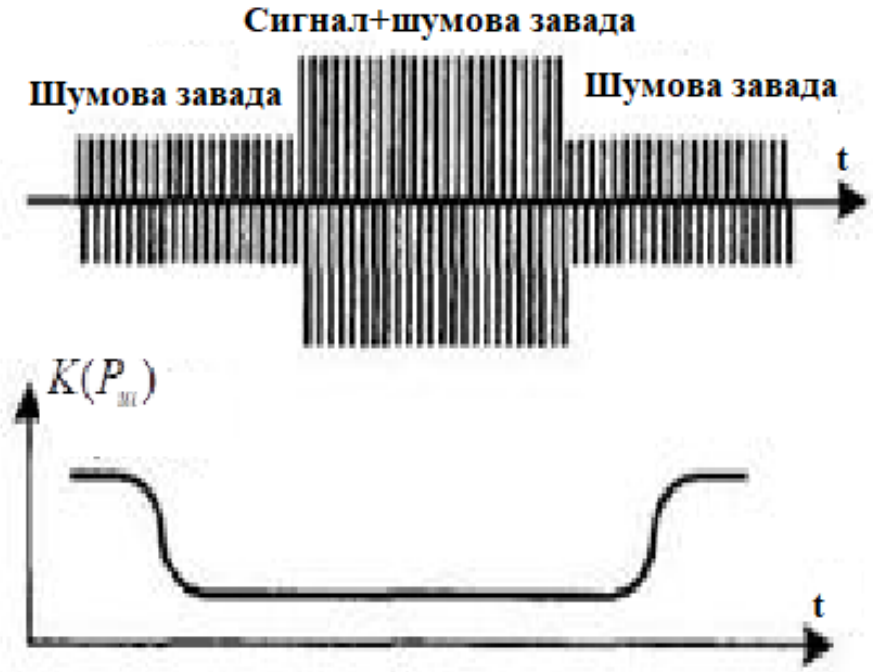


Рисунок 1.9. Осцилограма автоматичного регулювання підсилювання " *за ближніми шумами* ".

В цьому випадку, якщо прийнято потужний сигнал $q = \frac{P_c}{P_n} > 1$, а підсилення $K(P_ш)$ встановилося за шумовою завадою відносно нижчого рівня, то імпульс сигналу пройде на вихід. Якщо в аналогічній ситуації ухвалено сигнал малої потужності, тобто $q < 1$, то цей імпульс буде практично пригнічений, тобто завдяки роботі схеми автоматичного регулювання підсилення відрізок шумової перешкоди, що передує й іде за імпульсом сигналу, вирізають, підкреслюючи водночас корисний сигнал у разі $q > 1$.

Автоматизоване регулювання « *з пошуком провалу в спектрі завад* » виникає тоді, коли спектр завад на вході радіоприймального пристрою нерівномірний. Графічно це представлено на рисунку 1.10.

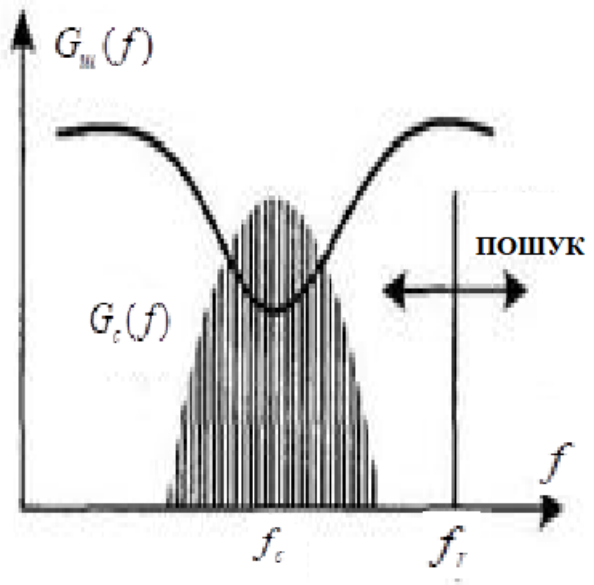


Рисунок 1.10. Автоматизоване регулювання «*з пошуком провалу в спектрі завад*»

Спектр сигналу зосереджений недалеко від провалу в спектрі завад, при здійсненні пошуку за частотою гетеродина $f_г$ за постійної смуги приймача $\Delta f_п$ можна домогтися максимального відношення *сигнал*/*шум*. Дана схема АРП поєднує в собі як властивості системи регулювання посилення, так і системи автоматичного підстроювання частоти. Але налаштування здійснюється не під якусь спектральну складову сигналу, а під частоту, на якій завада має мінімальну спектральну щільність. Налаштування під провал у спектрі перешкоди адаптує до завадової картини.

В наявності повільного автоматичного регулювання підсилення присутній постійний час $\tau_{АРП} \approx \tau_с$. За такої умови імпульс сигналу з мінливою за час $\tau_с$ амплітудою $E_с(t_с)$, $t \in [0, \tau_с]$ підтримується на виході постійним. Це захищає приймач від потужних імпульсних завад. Схема працює і при $\tau_{завад} \approx \tau_с$, тобто захищає приймач від довгих імпульсів завад .

Автоматизоване регулювання підсилювача «*з багаторазовими стробами*» забезпечує одержання постійного рівня вихідного сигналу приймача $E_{с\,вих} = const$ у широкому діапазоні амплітуд вхідних сигналів від $E_{с\,вих} = \min$ до $E_{с\,вих} = \max$ Для цього сигнал, який є керованим, обирають ступінчастим, тобто $U_{АРП} = k \cdot \Delta U_{АРП}$, $k = \text{var}$ і регулювання посилення проводять або до надходження імпульсного сигналу, або під час дії цього імпульсу, а також на максимальній дальності роботи радіолокаційної системи.

Детектор зі зворотним зміщенням уявляє собою особливий клас АРП, який забезпечує сталість амплітуди вихідного сигналу приймача, тобто $E_{с\,вих} = \max$ за будь-якого вхідного амплітудно-модульованого сигналу. Схема послаблює імпульсні завади з великою тривалістю, коли $\tau_п >> \tau_с$, тобто, наявність завад від

хмар дипольних відбивачів, аж до безперервних шумових завад.

Існує ще один спосіб зниження ризику перевантажень перешкодами, який полягає в залучені обмежувачів.

Обмежувачі сигналу уявляють собою окремий тип нелінійних пристроїв. Вони майже не дають придушення сигналу шумом, але при цьому спроможні успішно боротися з імпульсними завадами. Існує дуже багато різновидів схем, що використовують обмежувачі для зменшення впливу завад. В даній роботі здійснено коротке за відсутністю детального аналізу окремі схеми з цього класу.

Для боротьби з потужними імпульсними завадами, здійснюють обмеження зверху, тобто коли амплітуда завади значно перевершує амплітуду сигналу, тобто $E_n >> E_c$. В цьому випадку здійснюється обмеження зверху за рівнем E_c.

Унаслідок такого перетворення сумарний сигнал, який складається з інформативного сигналу та сигналу завади, потужні імпульси завади на вихід схеми обмежувача не надходять.

Наступним обмеженням є двопорогове, яке застосовується для захисту від завад каналу виявлення, схематично це представлено на рисунку 1.11.

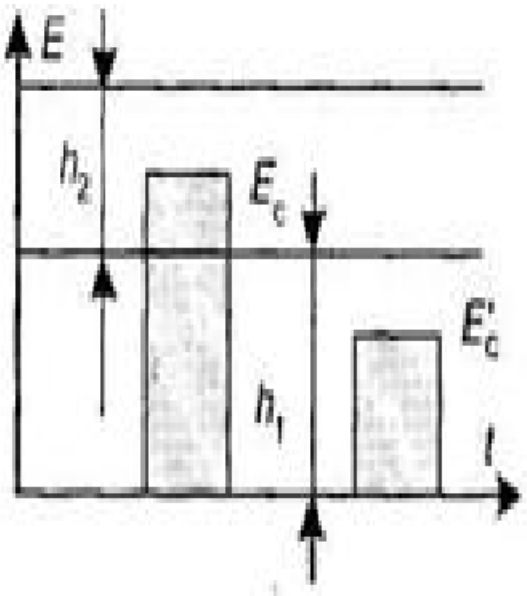


Рисунок 1.11. Двопорогове обмеження

В першому етапі функціонує каскад обмеження з першим пороговим рівнем h_1. Такий селектор пропускає сигнал з амплітудою E_c, який вилучає імпульси з $E_c < h_1$ і $E_c > h_1 + h_2$.

Що стосується обмеження знизу, то його можна застосовувати для придушення слабких завад. При застосуванні обмежувачів знизу, як це представлено на рисунку 1.12, на вихід проходять сигнали з $E_c > h_0$, а найбільш слабкі шумові імпульсні завади $x < h_0$ вилучаються.

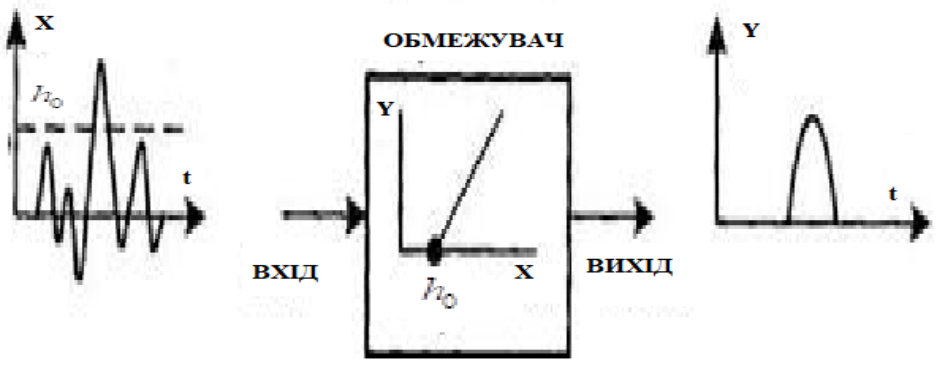


Рисунок 1.12. Обмеження знизу h_0

На рисунку 1.13 представлено схеми амплітудно-частоної селекції.

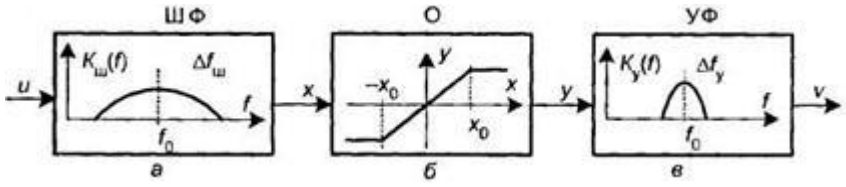


Рисунок 1.13. Амплітудно-частотна селекція з використанням схем «*Фільтр – Обмежувач – Фільтр*» , та «*Широкосмугова – Фільтр – Вузькосмугова*»

Смуги підсилювачів вибираються таким чином, щоб виконувалась умова $\Delta f_y \approx \Delta f_c$, $\Delta f_ш \approx k \cdot \Delta f_c$, $k >> 1$. Якщо на вхід схеми *Фільтр – Обмежувач – Фільтр* діє імпульс сигналу тривалості τ_c і завади з тривалістю $\tau_n << \tau_c$, то через вхідний підсилювач із широкою смугою обидва імпульси пройдуть без спотворень, як це показано на рисунку 1.13 а). Після обмеження прі рівні обмеження y_0 імпульсна завада буде зменшена за амплітудою до рівня $y_n = y_0$, як це представлено на рисунку 1.13 б). Фільтр із вузькою смугою, узгодженою з шириною спектра сигналу, імпульс сигналу не спотворить, а імпульс перешкоди розширить, зменшивши водночас його за амплітудою приблизно в k разів, як це представлено на рисунку 1.13 в). Отже, відношення *сигнал / шум* на виході буде визначатись наступним представленням

$$q_{вих} \approx \frac{1}{k^2} = \left(\frac{\Delta f_y}{\Delta f_ш} \right)^2 >> q_{вх} . \qquad (1.8)$$

Наступне призначення *Фільтр – Обмежувач – Фільтр* полягає в захисті від завад приймачів сигналів із кутовою модуляцією від шумових та інших широкосмугових завад. Також дана схема забезпечує стабілізацію ймовірності помилкових сирен радіоелектронного контролю на виході.

Варто зазначити, що обмеження не є єдиним спосібом нелінійного перетворення, що захищає від перевантажень. Серед нелінійних пристроїв придушення радіоперешкод отримали широкого застосування поширені різні модифікації приймачів із логарифмічними амплітудними характеристиками підсилювачів проміжної частоти, як це представлено на рисунку 1.14.

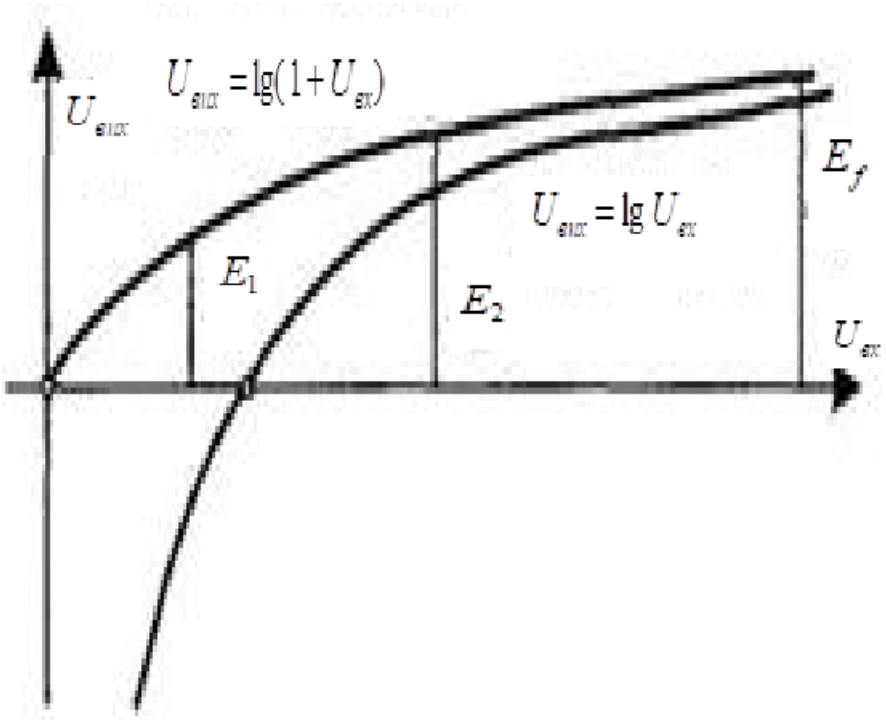


Рисунок 1.14. Логарифмічна характеристика приймача

Так як на інтервалі $U_{вх} < 1$ для довільного a виконується умова $\lim\limits_{x\to 0}(\log_a x) = -\infty$, для логарифмічних підсилювачів обирають характеристику, яку апроксимують функцією $\lg(1+x)$. В цьому випадку, значенню $x = 0$ за даною характеристикою, відповідає вихідний сигнал $y = 0$.

Логарифмічний приймач при малому значенні постійного часу стабілізує ймовірності хибних сирен радіолокаційної техніки та обмежує за протяжністю довгі завади $\tau_n >> \tau_c$. Структурну схему такого приймача представлено на рисунку 1.15. Особливістю такої схеми є застосування на виході логарифмічного підсилювача диференційного ланцюжка, що вкорочує вихідний імпульс сигналу та довгою перешкоди, коли $\tau_n >> \tau_c$. Практично не змінені диференціальним

ланцюжком імпульси сигналу та сильно укорочені ним імпульси завади посилюються вихідним відео підсилювачем.

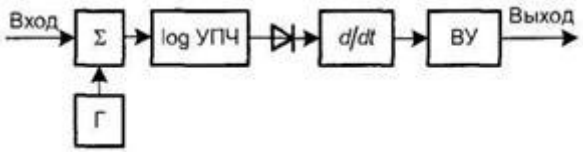


Рисунок 1.15. Логарифмічний приймач з малим значенням постійного часу

Висновки до розділу 1

1.Завдання захисту інформації, яка передається по радіотехнічному каналу є дуже важливою і в той же самий час достатньо складною.

2.Виявлення та нейтралізація завад, які виникають за рахунок потужних систем, які випромінюють електромагнітні поля потребує наявність потужних антен з підсилювачами, за допомогою яких здійснюється вилучення завад.

3.Методі, за допомогою яких здійснюється процес виявлення та нейтралізації завад на теперішній час отримали широкого застосування та дають можливість здійснювати надійний захист інформації, яка передається по радіотехнічному каналу.

4.Самим найкращим методом є метод передачі інформативного сигналу з обмеженнями.

РОЗДІЛ 2 МАСКУВАННЯ І НЕПОМІТНІСТЬ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ

2.1. Радіоелектронне маскування

Радіоелектронне маскування уявляє собою комплекс технічних та організаційних заходів, спрямованих на зниження якості засобів радіо, та радіотехнічної, радіолокаційної розвідки опонента. Об'єкти розвідки помітні остільки, оскільки приймачам засобів розвідки доступна інформація, за рахунок ПЕМВ. Інакше кажучи, помітність має місце завдяки тому, що приймачі засобів розвідки можуть виявити і виділити на тлі завад сигнали об'єктів розвідки, а мірою помітності є якість несанкціонованого приймання сигналів, що переносяться електромагнітним випромінюванням об'єктів розвідки в різних частотних діапазонах.

Найпростіший і в той же самий час наочний показник якості скритності сигналу радіоелектронної розвідки є P_p - імовірність несанкціонованого доступу засобів радіоелектронної розвідки до об`єкту і яка має наступне представлення

$$P_p = P_{EH} \cdot P_{CTP} \cdot P_{IHФ}, \qquad (2.1)$$

де

P_{EH} - показник енергетичної скритності, тобто умовна ймовірність виявлення сигналу, за умови, що він випромінюється;

P_{CTP} - показник структурної скритності, тобто умовна ймовірність виявлення розвідкою структури сигналу та ідентифікації радіоелектронної розвідки, що його випромінює. Так як структура визначається на підставі знання характеристик сигналу об'єкта розвідки, то ця ймовірність є ймовірністю визначення характеристик за умови, що сигнал виявлено;

$P_{IHФ}$ - показник інформаційної скритності, тобто умовна ймовірність виявлення, перехоплення та розшифрування радіоелектронною розвідкою повідомлень, що містяться в сигналі маскованого радіоелектронного засобу, за умови, що сигнал було випромінювано, виявлено та ідентифіковано.

Так як ймовірність правильного виявлення $P_{виявл}$ сигналу, що приймається на тлі завад, є монотонною функцією його енергії, тобто співвідношення енергії спостережуваної реалізації сигналу та спектральної густини завади. Такий показник називається характеристикою енергетичної прихованості $P_{ен} = P_{виявл}$. Фактори, що впливають на помітність об'єкта розвідки в радіодіапазоні, тобто на енергетичну скритність випромінювання, створюваного цим об'єктом, можна структурувати таким чином, як це показано на рисунку 2.1.

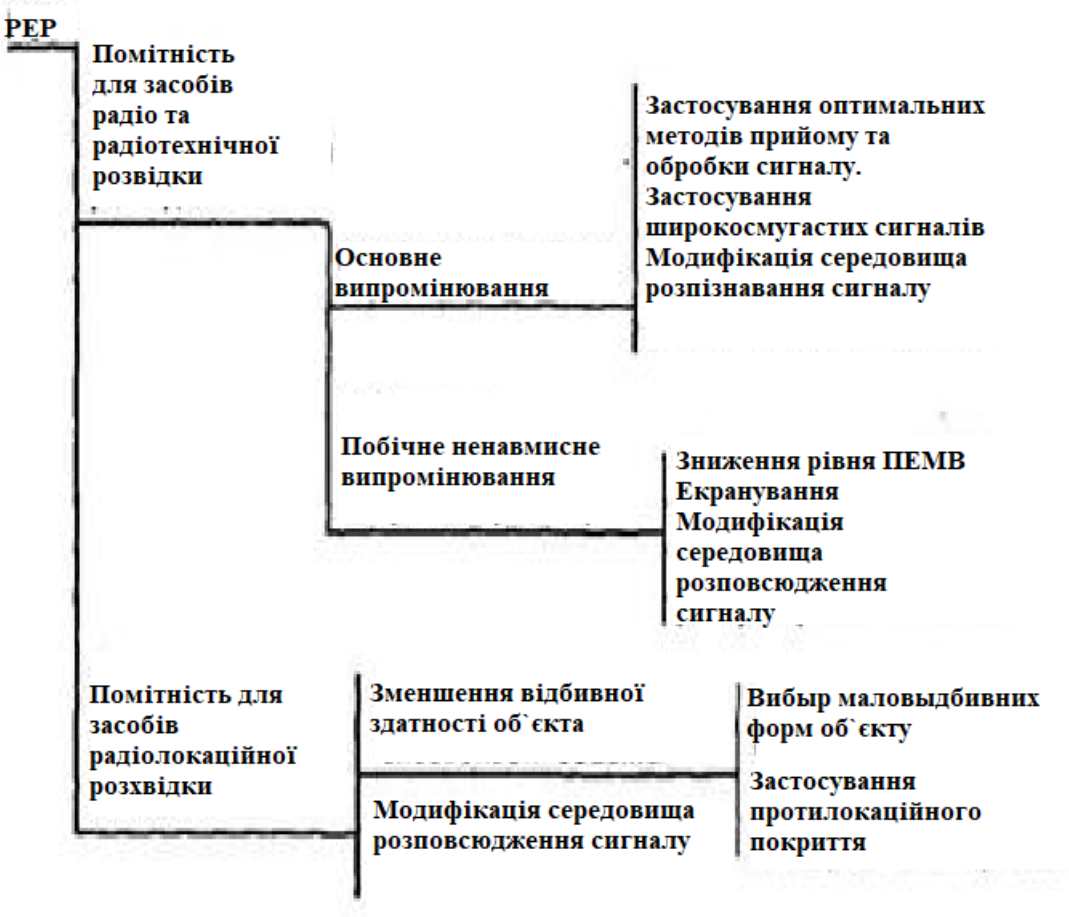


Рисунок 2.1. Завдання зниження помітності

Більшість радіоелектронних систем і засобів працюють із випромінюванням сигналів. Очевидно, що таке корисне для роботи випромінювання порушує їхню непомітність, демаскує об'єкт, що використовує радіоелектронні засоби. Для підвищення скритності всіляко знижують потужність основного випромінювання. Знижувати потужність сигналу можна

як завдяки раціональному вибору структури основного випромінюваного сигналу маскованих радіоелектронних засобів, так і завдяки організації його обробки на приймальній стороні. Таким чином, необхідний пошук і обґрунтування таких алгоритмів кодування і декодування повідомлень і таких способів модуляції і демодуляції несучих коливань, за яких на виході радіоканалу забезпечується найкраще відтворення повідомлень за заданої потужності сигналу, що передається, або потрібен сигнал мінімальної потужності для забезпечення заданої якості передавання або відтворення повідомлень. Методи вибору оптимальної структури сигналу і способу його оброблення відомі і розроблені теорією потенційної завадостійкості і теорією кодування.

Енергетична скритність основного випромінювання радіоелектронних засобів покращується у разі використання широкосмугових сигналів , тобто сигналів із великою базою, що мають дуже велике значення добутку ширини спектра на тривалість $B = \Delta f \cdot TR >> 1$. Завдяки збільшенню бази можна створювати сигнали з дуже малою спектральною густиною потужності і тим самим ускладнювати їхнє виявлення під час некогерентного оброблення в приймачі засобу розвідки. Також можна створювати сигнали з великою апріорною для розвідки невизначеністю параметрів.

Однак основне випромінювання маскованих радіоелектронних засобів аж ніяк не завжди доступне для прийому засобами радіоелектронних розвідок. Майже всі радіолокаційні системи і системи радіоуправління, а також багато систем передавання інформації концентрують потужність основного випромінювання у відносно вузькій ділянці простору, тобто використовують спрямоване випромінювання. Але і в цьому випадку радіоелектронні засоби демаскується своїми побічними і ненавмисними електромагнітними випромінюванням. Побічні і ненавмисні випромінювання розподілені за частотами поза основною смугою спектра сигналу і поза сектором простору, де локалізована головна пелюстка діаграми спрямованості антен. Ці випромінювання створюються пристроями формування і перетворення сигналів,

бічними пелюстками діаграм спрямованості антен, відсутність однорідності, що порушують безперервність екранів і фідерних трактів. Для зниження рівня побічних і ненавмисних випромінювання застосовують спеціальні конструктивні заходи і насамперед екранування елементів радіоелектронних засобів.

Важливий напрям у техніці зниження помітності радіоелектронних засобів є зменшення вторинного , тобто відбитого або розсіяного випромінювання радіолокаційних цілей. Це випромінювання не пов'язане з роботою власних радіоелектронних засобів об'єктів, що маскуються, і виникає завдяки взаємодії об'єктів із радіолокаційними полями. Коефіцієнт пропорційності між потужністю хвилі, що падає на поверхню маскованого об'єкта, і потужністю сигналу, випромінюваного в напрямку на антени приймальних пристроїв засобів радіолокаційної розвідки, має розмірність площі і називається ефективною поверхнею розсіювання. Тому методи зниження інтенсивності відбитого сигналу інакше називаються методами зменшення ефективної поверхні розсіювання. Для зменшення ефективної поверхні розсіювання існують два основні способи, що застосовуються як порізно, так і спільно, в комплексі. Перший спосіб полягає в виборі мало відбивної форми радіолокаційної цілі. Другий спосіб полягає в застосуванні спеціальних протирадіолокаційних покриттів, що зменшують енергію відбитого метою радіолокаційного сигналу.

2.2. Кодування в завадозахищенних системах передачі інформації

Для збереження достовірності передавання інформації в умовах дії завад застосовують спеціальні заходи, що зменшують імовірність появи помилок. Одним із таких заходів є застосування завадостійкого кодування. Кодування дає можливість збільшувати завадостійкість передавання інформації в обмін на збільшення надмірності та відповідно зниження швидкості передавання повідомлень. Але надмірність при кодуванні може вводитися і використовуватися по-різному. По-перше, за рахунок надмірності можна

створювати коди, здатні під час приймання і декодування виявляти і виправляти або коригувати помилки, обумовлені дією перешкод. Це коригувальні коди. По-друге, надлишкові символи можуть використовуватися для створення сигналів, що максимально відрізняються один від одного. Такі сигнали призначаються для приймання "*в цілому*". У складніших випадках інформаційну надмірність доповнюють апаратурною надмірністю, організовуючи передачу інформації зі зворотним зв'язком від одержувача повідомлень до їхнього джерела. Під час використання завадостійких кодів надмірність пов'язана з ускладненням структури кодованих повідомлень, що, зрештою, еквівалентно розширенню спектра сигналу або збільшенню часу передавання повідомлення. У разі використання складних сигналів, призначених для приймання "*загалом*", база збільшується також завдяки розширенню спектра. Крім того, підвищення завадозахищеності завжди пов'язане з деяким ускладненням систем передавання інформації, тобто зі збільшенням апаратурної надмірності. Завадостійка обстановка в середовищі, де працюють системи, може змінюватися. Відповідно можуть змінюватися і вимоги до завадозахисту: за меншої інтенсивності перешкод можна обійтися меншою надмірністю і, відповідно, забезпечити вищу швидкість передавання інформації. Але для такої адаптації швидкості передавання інформації до мінливих завадових умов необхідно мати зворотний канал передавання даних від приймача до передавача. Системи, що використовують такий канал, називаються системами передавання інформації зі зворотним зв'язком. Зазвичай використовують три основні варіанти здійснення зворотного зв'язку щодо переданої інформації.

За першого способу повідомлення, прийняте і запам'ятовуване одержувачем, ретранслюється джерелу інформації зворотним каналом. Передане і ретрансльоване повідомлення порівнюються. Якщо помилки під час передачі не сталося, передане повідомлення збігається з прийнятим зворотним каналом, передавач формує сигнал підтвердження правильності отриманих даних. У разі невідповідності повідомлення, прийнятого каналом зворотного зв'язку, тому, що раніше було передано прямим каналом, передавач фіксує помилку і формує

спеціальний сигнал стирання даних у пам'яті приймального пристрою. Після стирання передача повідомлення повторюється знову. І так доти, доки не буде зафіксовано факт неспотвореної передачі. Оскільки вся передана інформація ретранслюється зворотним каналом, подібний зворотний зв'язок називається інформаційним. Функціональну схему радіосистеми передавання сповіщень з інформаційним зворотним зв'язком наведено на рисунку 2.2.

Очевидно, що чим більшою є інтенсивність завад у прямому і зворотному каналах на рисунку 2.2 і відповідно ймовірність помилки під час передання, тим більше слід очікувати повторних передач і тим більшою є інформаційна надмірність.

Другий спосіб використання зворотного каналу - організація вирішального зворотного зв'язку. У радіосистемах із вирішальним зворотним зв'язком перевірка правильності приймання повідомлення та ухвалення рішення про необхідність повторного передавання здійснюються на приймальній стороні апаратурою одержувача інформації. Функціональна схема такої радіосистеми наведена на малюнку 2.3.

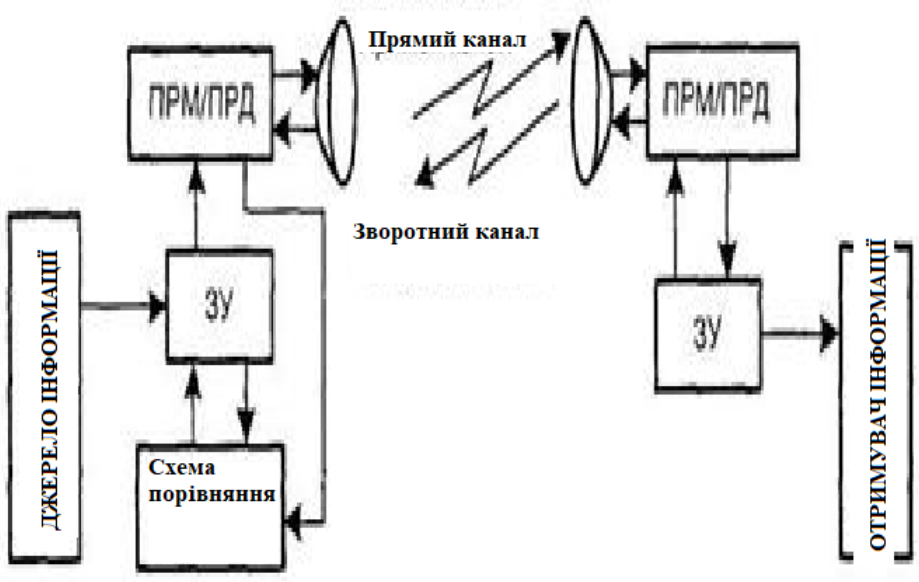


Рисунок 2.2. Радіосистема передачі повідомлення з оберненим зв`язком

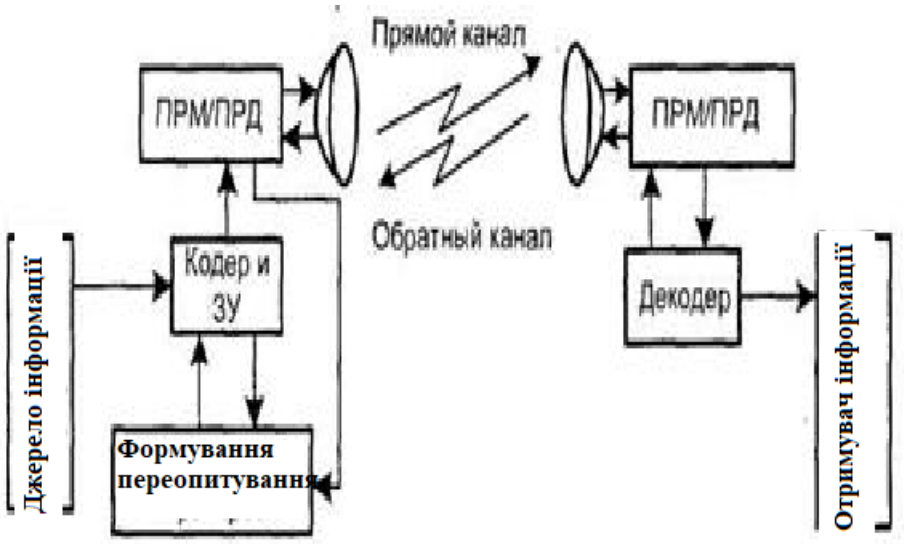


Рисунок 2.3. Радіосистема передачі повідомлення з вирішальним оберненим зв`язком

Аналіз прийнятої кодової комбінації виконується декодувальним пристроєм приймача. Очевидно, що для реалізації цієї можливості застосовується коригувальний код. У разі виявлення помилки прийняте повідомлення вважається спотвореним і зворотним каналом передається запит на повторну передачу. Якщо декодер не виявляє помилок у прийнятій кодовій комбінації, зворотним каналом передається підтвердження правильності прийому інформації. Отримавши квитанцію, що засвідчує правильність приймання, джерело повідомлень передає наступний блок інформації. В іншому разі воно повторює передачу попереднього спотвореного блоку. Таким чином, рішення про правильність прийнятого повідомлення виноситься в точці прийому, звідки назва "*вирішальний зворотний зв`язок*". Інша назва систем із вирішальним зворотним зв'язком - системи з переопитуванням. Природньо, що при використанні вирішального зворотного зв'язку зворотним каналом передається всього одна двійкова одиниця інформації на кожен інформаційний блок у прямому каналі.

Третій метод застосовує одночасно принципи як інформаційного, так і вирішального зворотного зв'язку. Це комбінований коригувальний зворотний зв'язок у системах передавання інформації. Наприклад, у разі рішення про помилку передавання повідомлення зворотним каналом надсилається квитанція-підтвердження, як у разі вирішального зворотного зв'язку. Якщо приймач виносить рішення про правильний прийом, зворотним каналом ретранслюється все прийняте повідомлення. При цьому з'являється можливість для усунення трансформації на прийомі однієї дозволеної кодової комбінації в іншу дозволену, але таку, що відрізняється від переданої.

Одна з найгостріших у радіоелектронному захисті проблема забезпечення радіоелектронних засобів зумовлена тією очевидною обставиною, що велика кількість екземплярів різнотипних радіоелектронних засобів працюють в обмеженому природою спектрі радіочастот.

Відповідно до рекомендацій Міжнародного союзу електрозв'язку, спектр електромагнітних коливань, частоти яких лежать у межах від $0{,}03 Гц$ до $3000 ГГц$, умовно розбитий на діапазони частот. Кожен діапазон має свою смугу частот і номер від одиниці до п`ятнадцяти.

Однією з особливостей радіочастотного спектра є його "*невитратність*" під час використання, тобто ділянка радіочастотного спектра, яку під час роботи займає деяка радіомережа або окремий радіоелектронний засіб, може бути використана іншою мережею або радіоелектронним засобом, розміщеними в тому ж місці, коли перші припиняють роботу. На умовах необхідного територіального розносу можлива робота на тій самій частоті за принципом "*спільного використання частот*".

Таке застосування частот можливе в тому разі, якщо рівень ненавмисних взаємних перешкод не призводить до неприпустимого зниження якості роботи радіоелектронних засобів.

Можливість багаторазового використання радіочастот залежить від умов поширення радіохвиль у тому чи іншому діапазоні частот, технічних характеристик приймально-передавальних і антенних пристроїв, типів сигналів, видів модуляції тощо.

В межах радіо служб останнім часом дедалі більше виділяються окремі "*застосування*". Так, наприклад, у рамках сухопутної рухомої служби виокремлюють такі застосування, як стільниковий, транкінговий радіозв'язок, бездротовий телефонний зв'язок тощо.

Відповідно до регламенту радіозв'язку, під час розгляду питань використання частот вживають такі терміни:

- розподіл смуги частот, коли йдеться про радіослужби;
- виділення радіочастоти або радіочастотного каналу, при наданні частоти або частотного каналу зонам або країнам;

- присвоєння радіочастоти або радіочастотного каналу, коли дозвіл на використання частоти або радіочастотного каналу отримує радіостанція.

Ефективне використання радіочастотних систем неможливе без добре налагодженої системи керування, яке повинно забезпечувати належне частотне територіальне планування та привласнення частот на основі забезпечення електромагнітної сумісності радіоелектронних засобів, як це представлено на рисунку 2.4.

Рисунок 2.4. Основні складові керування застосування радіочастотного контролю

Облік, створюваний сукупністю випромінювання радіоелектронних засобів, індустріальних та істотних завад, є необхідний елемент процедури керування використанням спектра.

Експлуатовані радіоелектронні засоби дуже нерівномірно розподілені за спектром частот і по поверхні Земної кулі. На завантаженість різних ділянок діапазону радіочастот вирішальний вплив чинять два фактори. Перший фактор уявляє собою технічне освоєння тієї чи іншої ділянки радіочастотної системи.

Другий фактор уявляє собою особливості поширення радіохвиль у різних ділянках радіочастотних систем, які не сумісні з кордонами держав і мають міжнародний характер.

Найбільш завантажені сьогодні метрова, дециметрова, сантиметрова, і, частково, гектометрова ділянки радіочастотних систем. Що стосується нерівномірності просторового розподілу радіоелектронних засобів, то потрібно враховувати, що сьогодні існує багато тисяч "*згустків*"радіоелектронних засобів навколо великих адміністративно-промислових центрів. У кожному такому угрупованні на обмеженій площі використовуються десятки і сотні тисяч примірників різноманітних радіоелектронних засобів. У таких угрупованнях і "*згустків*", коли відстані між радіоелектронними засобами менші за лінійні розміри зони, так званої, енергетичної доступності, радіоелектронні засоби створюють один одному перешкоди, які називають ненавмисними. Вплив ненавмисних завад на радіоелектронну систему розглядається як їхню електромагнітну несумісність, а заходи унеможливлення появи ненавмисних завад або послаблення їхнього впливу на ефективність роботи радіоелектронних систем визначено як забезпечення електромагнітної сумісності радіоелектронної системи.

Способи забезпечення електромагнітної сумісності радіоелектронних засобів поділяються на чотири групи:

- міжнародний і внутрішньодержавний розподіл ділянок діапазонів радіочастот між класами радіоелектронних засобів та службами;

- виділення частот для проектованих нових зразків радіоелектронних засобів;
- вдосконалення будови і функціонування радіоелектронних засобів під час їх проектування з метою виключення або ослаблення впливу ненавмисних завад;
- забезпечення електромагнітної сумісності радіоелектронних засобів в угрупованнях і на носіях, у межах об'єктів, що охороняються, вузлів зв'язку, центрів "*Р*", комплексного технічного та радіотехнічного контролю, зокрема в бойових діях.

Що стосується першої групи забезпечення електромагнітної сумісності радіоелектронних засобів, то ці способи на міждержавному рівні вирішує

міжнародний союз електрозв`язку, який розподіляє та періодично контролює розподіл смуг між районами земної кулі із зазначенням меж між ними. Усього таких районів три. На міжнародному рівні здійснюється розподіл смуг частот між службами, кожна з яких використовує свій клас радіоелектронних засобів. При цьому деякі частоти і смуги частот є загальними для всіх країн і заборонені для інших цілей.

Аналогічна за цілями і змістом регламентація використання смуг частот різними службами, класами і типами радіоелектронних засобів виконується в масштабах кожної держави. Така регламентація проводиться централізовано і децентралізовано. Централізовано призначаються частоти і смуги частот для роботи найпотужніших і найважливіших радіоелектронних засобів. Робочі частоти, призначені централізовано, забороняються для використання іншими радіоелектронними системами у межах територій, де можливі ненавмисні перешкоди таким важливим радіоелектронним системам. Децентралізовано розподіляються міністерствами та адміністраціями регіонів частоти для малопотужних радіоелектронних систем масового застосування.

2.3. Забезпечення електромагнітної сумісності радіоелектронних систем

Розвиток радіоелектронної розвідки дав змогу встановити, що, крім можливості прямого перехоплення інформації, що циркулює в каналах радіо, радіорелейного зв'язку, радіонавігації, локації, радіотелеуправління, є можливість отримання інформації каналами, утвореними під час роботи технічних засобів завдяки побічним електромагнітним випромінюванням і наведенням (ПЕМВ). ПЕМВ супроводжують роботу і фізичні процеси, що відбуваються як в основних розвідуваних технічних радіоелектронних засобах і системах, так і в різних допоміжних технічних системах, дротових, кабельних лініях зв'язку, металоконструкціях та інших спорудах.
Крім того, утворення інформативних побічних ефектів можливе завдяки

поданню на розвідувальний засіб спеціального розвідувального високочастотного або низькочастотного сигналу, що модулюється корисним інформативним сигналом, з подальшим прийомом і дешифруванням, тобто виділенням корисного сигналу. Найчастіше спеціальний розвідувальний сигнал, що подається, провокує самозбудження генераторів, гетеродинів, підсилювачів, що входять до складу технічних засобів.

Такі способи добування інформації в радіоелектронній розвідці класифікують як способи розвідки за технічними каналами витоку інформації (ТКВІ). Методи отримання інформації технічними каналами, як правило, використовують агентурна розвідка, спецслужби, що ведуть оперативно-розшукову діяльність, комерційна розвідка, а також групи організованої злочинності, зловмисники.

Класифікаційну схему основних технічних каналів витоку інформації представлено на рисунку 2.5.

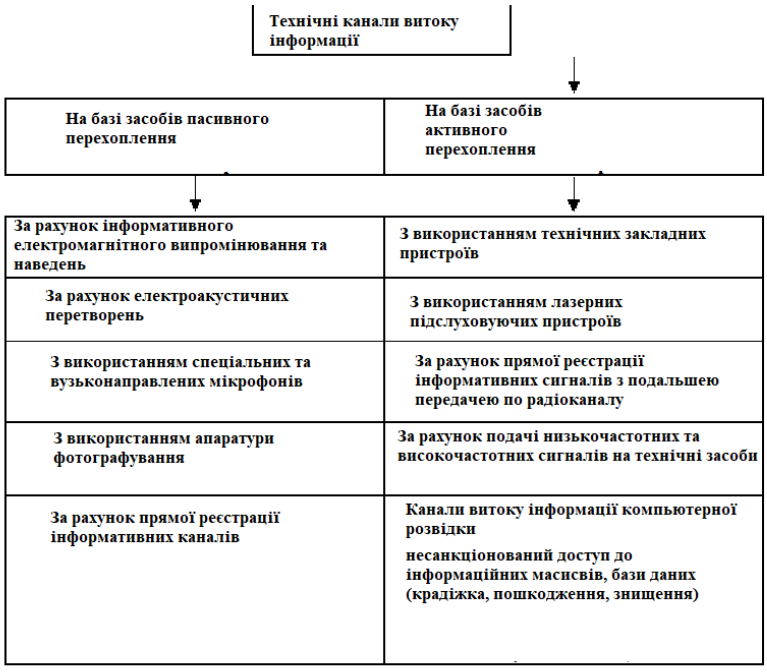


Рисунок 2.5. Технічні канали витоку інформації

Ці технічні канали витоку інформації згруповані за двома методами ведення розвідки, а саме за рахунок пасивного перехоплення і за рахунок активного перехоплення і відрізняються один від одного технічною реалізацією завдань розвідки.

Перша група каналів витоку інформації заснована на використанні ефектів розсіювання працюючих технічних засобів, мікрофонного ефекту, тобто за рахунок електроакустичних перетворень, а також прямої реєстрації інформаційних сигналів шляхом використання технічної апаратури приймання. Друга група каналів передбачає застосування технічних приймально-передавальних пристроїв .

Для отримання інформації, що обробляється, передається та зберігається за допомогою технічних засобів, можуть використовуватися і спеціальні технічні пристрої активного перехоплення, які, на відміну від засобів пасивного перехоплення, самі створюють електромагнітні розвідувальні сигнали, що впливають на технічний засіб , який розвідують. На них, своєю чергою, впливають сигнали, що циркулюють в інформаційних ланцюгах технічних засобів, або побічні інформативні сигнали, що виникають під час функціонування цих засобів. Утворений у результаті складніший інформативний сигнал фіксується, і за ним відновлюється інформація, переносником якої він є.

Висновки до розділу 2

1.Під час роботи деяких технічних засобів, поряд з електромагнітними полями "*розсіювання*", виникають інформативні акустичні, вібраційно акустичні, гідроакустичні та акустично електричні поля/сигнали;

2.Під час телефонної розмови електричний сигнал у лінії та різноманітні наведення і впливи;

3.Під час радіотелефонної розмови з'являється електромагнітний сигнал. 4.Акустична енергія, що виникає під час розмови, може викликати акустичні або механічні коливання елементів електронної апаратури, що призводить до появи електромагнітного випромінювання або до його зміни за певних обставин. 5.Найбільш чутливими елементами радіоелектронної апаратури до акустичних впливів є котушки індуктивності та конденсатори змінної ємності.

РОЗДІЛ3 РОЗВІДКА ЗА РАХУНОК СТВОРЕННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

3.1.Фізичний принцип ПЕМВ як фундамент створення каналів витоку інформації

У сучасних волоконно-оптичних системах (ВОС) у процесі передачі інформації використовується модуляція джерела світла за амплітудою, інтенсивністю та поляризацією. Зовнішній акустичний вплив на волоконно-оптичний дріт призводить до зміни його геометричних розмірів , тобто товщини, що спричиняє зміну шляху руху світла, тобто до зміни інтенсивності, причому пропорційно значенню цього тиску. У наявності - мікрофонний ефект у ВОС передачі інформації, тобто чутливість світловода до тиску визначається значенням співвідношення $Ч = \frac{\Delta\varphi}{\varphi\Delta p}$, де $\Delta\varphi$ - зсув фази, спричинений зміною тиску Δp.

Вивчення властивостей твердих діелектриків показало, що деякі з них поляризуються не тільки за допомогою електричного поля, а й у процесі деформації під час механічного впливу на них. Поляризація діелектрика під час механічного впливу на нього називається прямим п'єзоелектричним ефектом. Таким ефектом володіють кристали кварцу і всі сегнетоелектрики (під час стискання кварцу його протилежні грані заряджаються полярно і величина заряду пропорційна тиску, на вихідних контактах утворюється відповідний електричний сигнал). Кварцові пластини широко використовуються в

п'єзоелектричних мікрофонах, охоронних датчиках, стабілізаторах генераторів незатухаючих коливань.

Повітряні та вібраційні технічні канали витоку інформації досліджуються за допомогою спеціальних і вузько спрямованих мікрофонів. У повітряних укриттях середовищем поширення інформаційних сигналів є повітряне середовище, і для їхнього перехоплення використовують як приховані провідні лінії зв'язку, обладнані мініатюрними високочутливими мікрофонами, так і спеціальні вузько спрямовані мікрофони. За допомогою таких мікрофонів можна прослухати розмову на відстані до одного кілометру у межах прямої видимості. Простий спрямований мікрофон являє собою набір із семи алюмінієвих трубок діаметром до десяти міліметрів. Довжина трубок визначає резонансну частоту звукового сигналу. Мікрофон розташовується в параболічному уловлювачі. Посилення перехопленого сигналу здійснюється мікрофонним підсилювачем. Цей спрямований мікрофон перекриває весь спектр звукових речових коливань від трьохсот до три тисячі трьохсот герц. Розширення діапазону прийнятих частот з метою забезпечення високої якості прийнятих мовленнєвих сигналів здійснюється за рахунок збільшення кількості резонансних трубок і зміни їхньої довжини, для чого проводять спеціальні інженерні розрахунки система з тридцяти семи трубок, наприклад, забезпечує перекриття діапазону від ста восьмидесяти до вісім тисяч двісті герць.

У вібраційних укриттях середовищем поширення акустичних сигналів є конструкції будівель, споруд, труби водопостачання, системи опалення, каналізації та інші тверді тіла і поверхні. Для перехоплення акустичних коливань у цьому разі використовують контактні мікрофони стетоскопи. Контактні мікрофони, з'єднані з електронним підсилювачем, називають електронними стетоскопами.

Висновки до розділу 3

1.Ефект "*нав`язування*" полягає в подачі в телефонну лінію в бік приймального апарата, тобто спеціального пристрою для підслуховування розвідувального сигналу високих частот, низьких частот генератора або передавача з частотою сто п`ятдесят кілогерц і вище на один дріт телефонної лінії, до другого дроту під'єднується вхід приймача.

2.Земля передавача і приймача з'єднані між собою або із загальною землею, наприклад, водопровідною мережею.

3.Ці коливання за рахунок нелінійності елементів телефонного апарата модулюються мовними сигналами під час розмови при піднятій телефонній слухавці або електро рушійної сили мікрофонного ефекту дзвінка при покладеній телефонній слухавці.

4.Сумарний звуковий і високо частотний-розвідувальний сигнал є складним сигналом, що змінюється за законом мовних коливань. У результаті отримаємо квазі телефонний закладний пристрій, в якій і передавач, і приймач винесено за межі контрольованої зони, а нелінійність телефонного апарата виконує роль модулятора. Сумарний сигнал детектором приймача перетворюється на мовний інформативний.

ВИСНОВКИ

1.У загальному комплексі заходів із ведення розвідки важливе місце відводиться технічній розвідці, яку нині вважають основним засобом отримання розвідувальної інформації.

2.Вважається, що на частку технічної розвідки припадає понад половини всієї отриманої інформації. Тому проблема захисту від технічної розвідки набуває особливої актуальності.

3.Захист від технічних засобів захисту інформації є невід'ємною і складовою частиною наукової та виробничої діяльності підприємств, установ і організацій усіх форм власності.

4.Необхідно зазначити також, що на сучасному етапі значного поширення набуває економічне та промислове шпигунство, яке не пов'язане безпосередньо з міждержавними, політичними та військовими протиріччями.

5.Головною причиною виникнення промислового шпигунства є конкуренція між фірмами, компаніями та підприємствами. Промислове шпигунство охоплює сьогодні всі сфери ринкової економіки і в умовах запеклої конкурентної боротьби його масштаби різко зростають.

6.При веденні промислового шпигунства користуються тими ж технічними засобами і способами. Тому матеріал пропонованої книжки, безумовно, є корисним для широкого кола осіб, до обов'язків яких входять питання забезпечення безпеки інформації.

7.Невід'ємною частиною захисту приховуваних об'єктів та інформації від розвідки є технічний контроль, що призначений для оцінки ефективності та надійності вжитих заходів захисту. Без якісного технічного контролю неможливо реалізувати надійне закриття каналів витоку інформації.

8.Технічний захист інформації в системах оброблення та передавання даних має здійснюватися в суворій відповідності з нормативними документами. Тому в роботі належну увагу приділено питанням правового забезпечення

комплексної системи технічних засобів захисту інформації, а також передачі інформації в телекомунікаційних системах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.

18. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – Москва, 2006. – 197 с.