МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Захист інформації
в телекомунікаційних системах

Київ 2009

УДК 629.735.05 (076.5)
ББК 3811р
К 338

Рецензенти: д-р техн.. наук, проф. В.П. Вінницький,
д-р техн.. наук, проф. В.О. Хорошко

Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн,
О.О. Горбунов
К 338 Захист інформації в телекомунікаційних системах: Навчальний посібник.(лист МОНУ №1.4/18 – Г – 183 від 02.06.2009р.). –К.: НАУ,2009. – 380с.

Захист інформації в телекомунікаційних системах.
Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, О.О. Горбунов

В посібнику розглянуто основні проблеми захисту інформації, які виникають в відомчих системах зв’язку та передачі даних, радіотехнічних системах та системах зв’язку загального користування. Приведено досить повний аналіз каналів витоку інформації, методів та засобів несанкціонованого отримання інформації , засобів захисту інформації та проаналізовано особливості функціонування відомчих телекомунікаційних систем.

Посібник буде корисним студентам відповідних спеціальностей та спеціалістам в області телекомунікацій та захисту інформації.

Зміст

Вступ 5
1. Загальні проблеми безпеки авіаційних інформаційно-комунікаційних систем. 6
1.1. Основні поняття й визначення 6
1.2. Стандарти інформаційної безпеки 17
1.3. Сучасні методи й засоби оцінки стану безпеки 21
Розділ 2. Інформаційні характеристики мовних повідомлень 27
2.1. Структурна схема системи зв'язку та її елементи 27
2.2. Характеристики безперервних джерел та одержувачів повідомлень 28
2.3. Компресія мовних сигналів 39
2.4. Статистичні характеристики мовних повідомлень 49
2.5. Параметрична компресія мовних сигналів 52
Розділ 3. Характеристика каналів витоку інформації в телекомунікаційних системах588
3.1 Класифікація каналів витоку інформації 588
3.2 Моделі електромагнитних каналів витоку інформації 75
3.3 Застосування моделі Хата для моделювання технічних каналів витоку інформації в службових приміщеннях. 94
Розділ 4. Пристрої і системи технічної розвідки 103
4.1. Загальна інформація 103
4.2. Радіомікрофони 105
4.3. Пристрої перехоплення телефонних повідомлень 1177
4.4. Спеціальні пристрої прослуховування 1299
4.5. Системи і пристрої відеоконтролю 1499
4.6. Нелінійні радіолокатори 1522
Питання для самоперевірки: 1522
Розділ 5. Методи захисту інформації в системах зв′язку та передавання даних 1533
5.1. Класифікація засобів технічного захисту інформації в каналах загального користування. 1533
5.2 Пристрої захисту інформації в телекомунікаційних системах 1644
5.3. Індикатори поля 1800
5.4. Скануючі приймачі 1911
5.6 Випалювачі телефонних заставних пристроїв 2155
5.7. Виявлювачі та придушувачі диктофонів і ВЧ електронних пристроїв 2166
5.8 Системи віброакустичного зашумлення 2233
4.9 Нелінійні радіолокатори 2366

Розділ 6. Основи криптографії та шифрування. 23939
6.1. Основні принципи криптографії 23939
6.2. Класифікація шифрів. 2400
6.3. Симетрична криптографія. 2444
6.4 Асиметрична криптографія та цифровий підпис. 2733
Питання для самоперевірки 2800
Розділ 7. Методи закриття мовних сигналів 2811
7.1. Загальні положення 2811
7.2. Аналогове скремблювання 2844
7.3. Дискретизація мови з наступним шифруванням 2944
7.4. Статистичний аналіз кодерів CELP 3122
7.5. Багатопозиційні фазова та амплітудно-фазова модуляція 3166
7.6. Критерії оцінки систем закриття мови 3222
Розділ 8. Дослідження особливостей технічного захисту інформації в процесах експлуатації відомчої телекомунікаційної мережі цивільної авіації україни. 3300
8.1. Аналіз сучасного стану об'єкта досліджень – мережі ATN. 3300
8.2. Аналіз особливостей використання в АНЕЗ ЦА ліній передачі мереж загального користування з сучасними технологіями 3411
8. 3 Класифікація атак на ресурси інформаційно-комунікаційних систем 3611
8.4. Вимоги до комплексної системи захисту інформації в авіаційних інформаційно-комунікаційних системах 36969
Список літератури 3800

Вступ

Досягнення у розвитку сучасних засобів передачі інформації знайшли своє застосування і в авіації. Це привело до інтенсивного розвитку авіаційних телекомунікаційних систем та обчислювальної техніки. Досягнення сучасних технологій дають можливість у наш час передавати інформацію на будь-які відстані.

Авіаційні телекомунікаційні системи базуються на використанні електронно-обчислювальних машин, каналів зв'язку та модемів і є складовою частиною сучасної телекомунікації.

Широкий розвиток цифрових методів передачі інформації створив умови для організації більшої кількості служб у рамках єдиної мережі, ніж це було можливо при використанні аналогових мереж, а також для запровадження в авіації електронної пошти, телексу, факсу, відеотексту тощо.

Інтенсивний розвиток засобів та систем передачі інформації в авіації вимагає забезпечення інформаційної безпеки, яка полягає у використанні спеціальних засобів, методів та заходів, щоб запобігти втраті інформації. Заходи безпеки спрямовані на запобігання несанкціонованому одержанню інформації, фізичному знищенню або модифікації інформації, яка захищається.

Враховуючи те, що втрата інформації в авіаційній галузі може призвести не тільки до економічних збитків авіакомпаній, аеропортів, а й до зниження безпеки польотів та людських жертв, збереження її є актуальною проблемою.

Можливість зловживань інформацією, яка передається каналами телекомунікацій, розвивається та вдосконалюється не менш інтенсивно, ніж засоби їх попередження. Тому проблема захисту інформації потребує організації цілого комплексу спеціальних заходів захисту з метою попередження втрати інформації, яка міститься в каналах телекомунікацій.

Комплексний підхід до інформаційної безпеки передбачає комплексний розвиток усіх методів та засобів захисту інформації.

Таким чином, нині існує сучасна технологія захисту інформації, яка передається каналами телекомунікацій і в сферу впливу якої потрапляють не тільки канали зв'язку, але й центри комутації, периферійні пристрої, термінали, адміністратори зв'язку, локальні комп'ютерні мережі тощо.

1. Загальні проблеми безпеки авіаційних інформаційно-комунікаційних систем.

1.1. Основні поняття й визначення

Проблема безпеки інформаційно-комунікаційних систем (ІКС), будучи відносно новою, поступово загострювалася в міру розвитку інформаційних технологій і тотального використання ІКС і мереж у всіх областях народного господарства. На сьогодні в сфері захисту сформувалася досить потужна індустрія (яка об'єднала в собі науку й виробництво), орієнтована на рішення основних питань безпеки, які можна розділити на три групи: фізичні (зв'язані здебільшого з об'єктивними факторами); логічні (пов'язані із суб'єктивними факторами); соціальні [17].

З фізичною безпекою зв'язані питання захисту від пожеж, затоплень, землетрусів, ураганів, вибухів, промислових хімічних речовин, різних магнітних полів, збоїв устаткування, гризунів і т.п.

Логічна безпека відображає питання захисту від несанкціонованого доступу (НСД), помилок у діях персоналу й програм, які негативно впливають на інформацію й т.п.

До соціальної безпеки належать засоби юридичного, організаційного й адміністративного захисту, питання підготовки кадрів, виховної роботи, спрямованої на формування певної дисципліни й етичних норм, обов'язкових для тих, хто взаємодіє в інформаційному контурі й т.п.

До базових характеристик безпеки інформації відносять конфіденційність (Confidential), цілісність (Integrity) і доступність (Accessibility) [17].

Конфіденційність - характеристика безпеки інформації, що відображає її властивість нерозкритості й доступності без відповідних повноважень. Фактично, інформація не може бути доступна або розкрита неавторизованій стороні, тобто для неї її нібито немає. У свою чергу, авторська сторона (наприклад, персонал що обслуговує, користувачі, програми й т.п.), якій надані відповідні повноваження, має повний доступ до інформації.

Цілісність - характеристика безпеки інформації (даних), що відображає її властивість протистояти несанкціонованій модифікації. Наприклад, користувач, що накопичує інформацію, має право очікувати, що зміст його файлів залишиться незмінним, незважаючи на цілеспрямовані впливи, відмову програмних або апаратних засобів. По цій характеристиці інформація не піддається ніякому впливу з боку неавторизованої сторони.

Доступність - характеристика безпеки інформації, яка відображає її властивість, що складається в можливості використання відповідних ресурсів у заданий момент часу відповідно до пред'явлених повноважень. Фактично авторська сторона по першій потребі одержує необмежений доступ до потрібної інформації.

Взагалі дані характеристики можна використати для відображення зазначених властивостей цілих систем або будь-яких компонентів ІКС, під якими мають на увазі сукупності програмних засобів, апаратури, різні фізичні носії інформації, дані й навіть обслуговуючий персонал.

Під доступом (access) мають на увазі взаємодію між ресурсами ІКС, що забезпечує передачу інформації між ними, а в процесі доступу до інформації (access to information) зокрема реалізується її копіювання, модифікація, знищення, ініціалізація й т.п. Розрізняють несанкціонований і санкціонований доступ. Якщо доступ до ресурсів системи здійснюється з порушенням правил розмежування доступу, то такий доступ є несанкціонованим. Однією з базових дій, що породжує НСД, є перехоплення (intercept), під яким мають на увазі несанкціоноване одержання інформації незаконним підключенням до каналів зв'язку (наприклад, пряме перехоплення), візуально (наприклад, підглядання), або за допомогою радіотехнічних засобів (наприклад, непряме перехоплення).

Перехоплення по дії на інформацію можна розділити на активне і пасивне, а по типі підключення - на прямій і непрямий.

Активне перехоплення (active eavesdropping). Перехоплення, під час якого в супротивника є можливість не тільки перехоплювати повідомлення, але й впливати на нього, наприклад, затримувати або видаляти сигнали, які передаються каналами зв'язку.

Пасивне перехоплення (passive tapping). Одержання інформації з можливістю тільки спостерігати за обміном повідомленнями (наприклад, з метою виявлення різної системної інформації) в обчислювальній мережі, при цьому не роблячи на неї ніякого впливу.

Пряме перехоплення (direct eavesdropping). Перехоплення інформації шляхом безпосереднього підключення (наприклад, додаткового термінала) до лінії зв'язку. Пряме перехоплення можна виявити перевіркою лінії зв'язку.

Непряме перехоплення (indirect eavesdropping). Перехоплення інформації (наприклад, індуктивних хвиль) без використання безпосереднього підключення до лінії зв'язку. Пасивне перехоплення важко виявити, оскільки немає безпосереднього приєднання термінального обладнання до лінії зв'язку.

Стан безпеки інформації щодо його базових характеристик залежить від успішності реалізації тієї або іншої погрози, під якою розуміють потенційну можливість порушення безпеки.

Під час побудови комплексних систем захисту аналіз погроз є одним з обов'язкових етапів. На цьому етапі формується найбільш повна безліч погроз із урахуванням фактора ризику і їхніх властивостей. Ґрунтуючись на публікаціях закордонних і вітчизняних авторів [22-24, 28], класифікацію погроз можна виконати по таких базових ознаках.

1. По дії на характеристики безпеки інформації:

К-тип (погроза конфіденційності);

Ц-тип (погроза цілісності);

Д-тип (погроза доступності);

Кц-тип (погроза конфіденційності й цілісності);

Кд-тип (погроза конфіденційності й доступності);

Цд-тип (погроза цілісності й доступності);

Кцд-тип (погроза конфіденційності, цілісності й доступності).

2. По природі джерела:

об'єктивна (погроза, виникнення якої не залежить від прямої діяльності людини й пов'язана з різними стихійними природними явищами, такими, як пожежі, блискавки, землетруси, радіоактивне випромінювання, напади гризунів і т.п.);

суб'єктивна (погроза, виникнення якої залежить від діяльності людини).

Суб'єктивну погрозу, у свою чергу, за мотивом розділяють на активну й пасивну. Активна пов'язана з діями людини спрямованими на одержання певної вигоди, а пасивна виключає зазначену складову й пов'язана з помилками людини, недбалістю, проектно-технологічними недоліками в програмному й апаратному забезпеченні й т.п.

Можна вводити додаткові ознаки класифікації (наприклад, за частотою появи погрози, наслідками її реалізації, можливістю виявлення й запобігання й т.п.), які допоможуть формалізувати хід ідентифікації й аналізу погроз і підвищити ефективність процесу побудови систем ЗІ.

Розглянемо приклади найбільш типових погроз [17] інформаційним ресурсам (ІР) і визначимо деякі їхні властивості відповідно до ознак вищенаведеної класифікації.

Апаратні збої й відмови. Суб'єктивна пасивна погроза Кцд-типа, запобігти яку майже неможливо, частота її появи висока, для оцінки використається показник наробітку на відмову, виявити в окремих випадках нескладно, але іноді необхідна спеціальні апаратури, можливі потенційно більші наслідки. Для інформації, оброблюваної в ІКС, особливо небезпечні збої (відмови) жорсткого диска, внаслідок яких можуть бути ушкоджені записи, що впливає на цілісність; неможливість виконати завантаження є погрозою доступності; у фірмі по обслуговуванню дисків може виникнути витік даних, що порушить конфіденційність.

Диверсії. Суб'єктивна активна погроза Цд-типа, з'являється не дуже часто, запобігти її дуже важко, складність виявлення - різна, наслідки потенційно дуже великі. Найчастіше проявляється у фізичному (підпал, пробій, розукомплектовування, ушкодження живлення й т.п.) або логічному (зміна імен файлів, дисків, підміна програм, даних і т.п.) ушкодженні.

Випромінювання й наведення. Суб'єктивна пасивна погроза К-типу. Виявити зняття інформації з каналів побічних електромагнітних випромінювань і наведень (ПЕВН) майже неможливо, частота такого доступу невідома, запобігти цьому явищу досить складно (для цього потрібно застосовувати спеціальні засоби захисту), наслідки потенційно великі. Такі погрози є одним зі слабких місць у комп'ютерному захисті, оскільки кабелі, з'єднання й пристрої (відеотермінали, принтери, модеми, клавіатура, конекторы, заземлення й т.п.), випромінюють певні сигнали, які навіть при незначному рівні можуть бути перехоплені чутливою антеною.

Комп'ютерні віруси. Суб'єктивна активна погроза Цд-типа, запобігання при нових формах може бути складним, вплив як правило очевидний, частота появи відносно висока, наслідки потенційно дуже великі, але на практиці менш загрозливі. Віруси по різному впливають на ІР, наприклад, знищують файли, псують записи, змінюють таблицю розподіл файлів і т.п.

Крадіжки. Суб'єктивна активна погроза Кцд-типа, запобігти й виявити яку досить складно; частота появи невідома, а наслідки потенційно дуже великі. Під вплив погрози може підпадати, наприклад, як апаратури, так і файли, при цьому крадіжка останніх, як правило, залишається непоміченої. Цілісність і доступність у цьому випадку порушується зі зникненням єдиних екземплярів певних ІР. Крадіжка також може бути пов'язана з підміною даних перед їхнім уведенням або в процесі використання.

Хакери. Суб'єктивна активна погроза Ц-типа, запобігти яку досить складно; виявити вплив дуже просто або складно; частота появи невідома, але швидше, досить висока; наслідки потенційно великі. За допомогою крекерів здійснюється злом різних систем захисту через модифікацію захисного механізму в самому ПО. Крекери - вузькоспрямовані програми, внаслідок впливу яких з'являється можливість не тільки безперешкодно входити в систему, але й вільно використати різні комерційні (захищені) версії програм. Після дії крекеру, як правило, відкривається доступ іншим погрозам, які порушують основні характеристики безпеки окремих ІР.

Логічні бомби. Суб'єктивна активна погроза Кцд-типа, запобігти й часто виявити яку досить складно; частота появи точно невідома (швидше невисока), наслідки потенційно великі. Логічні бомби ініціюються з виникненням різних подій (наприклад, відкриття якого-небудь файлу, обробка певних записів й інших дій) з метою знищення, перекручування або модифікування даних. Використаються, наприклад, для розкрадання за допомогою зміни певним чином (у свою користь) коду програми, що реалізує фінансові операції, а також для нанесення збитку або шантажу.

Недбалість. Суб'єктивна пасивна погроза Кцд-типа, що дуже важко запобігти; різна складність виявлення, з'являється часто, наслідки потенційно великі. Така погроза, як

правило, пов'язана з різними помилками людини, випадками, необачністю, проявами некомпетентності й, по оцінках експертів, 50-60 % втрат здійснюється саме через неї.

Неможливість використання. Залежно від мотиву, суб'єктивна активна або пасивна погроза Д-типа, що пов'язана з падінням продуктивності функціонування систем внаслідок невикористання з будь-якої причини наявних програмних й апаратних засобів. Запобігти погрозі важко, виникає з невідомою частотою, виявити іноді буває досить складно, а наслідки потенційно великі.

Неправильна маршрутизація. Суб'єктивна пасивна погроза До-типу, запобігти яку досить складно, виявити можна просто, частота появи можливо висока, але точно не відома, а наслідки потенційно великі. Порушення конфіденційності здійснюються через пересилання повідомлень, файлів й іншої інформації до неправильної адреси, сформованої здебільшого внаслідок ненавмисної помилки.

Неточна або застаріла інформація. Суб'єктивна пасивна погроза Ц-типа, запобігання й виявлення якої може бути важким, трапляється досить часто, а наслідки потенційно дуже великі. Повідомлення, записи, файли й інша інформація може стати недоброякісною, через її випадкове перекручування, неповноту або старіння, обумовлене одержанням нових даних. Для запобігання несприятливих наслідків таку інформацію необхідно вчасно видаляти.

Помилки програмування. Суб'єктивна пасивна погроза Кцд-типа, запобігти яку майже неможливо, виникає постійно, виявлення буває досить складним, а наслідки потенційно дуже великі. У процесі створення програм у вихідному неналагодженому тексті, як правило, на 50 рядків, зустрічається не менше однієї помилки. Під час налагодження більшість із них виправляється, однак певна частина залишається й виявляється, як правило, у позаштатних ситуаціях, наприклад, під час зміни форматів параметрів, оточення й т.п.

Перевантаження. Залежно від мотиву суб'єктивна активна або пасивна погроза Д-типа, виявити яку просто, запобігти складно, виникає з невідомою частотою (як правило висока в нових рідко використовуваних системах), а наслідки потенційно дуже великі. Будь-яке програмне або апаратне забезпечення, що дає збої під час його тестування в критичних режимах, як правило, показує подібні результати й у випадку його перевантаження. Наприклад, за допомогою автоматичного номеронабирача з декількох комп'ютерів можна здійснити атаку типу “відмова в обслуговуванні” всіх телефонних номерів авіакомпанії, які використаються для продажу квитків. Для цього після відповіді абонента здійснюється відключення лінії й знову виконується виклик. Внаслідок реалізації такої суб'єктивної активної погрози Д-типа доступність до мережі продажу квитків буде дуже обмежена, і від цього постраждає не тільки компанія, але й клієнти.

Перехоплення. Залежно від дії, суб'єктивна активна погроза К- або Кц-типа, запобігти яку майже неможливо, виявити досить складно або навіть неможливо. Частоту такої погрози

не встановлено, а наслідки потенційно великі. Перехоплення інформації здійснюється переважно через несанкціоноване підключення додаткового термінала або, наприклад, через спостереження за побічними електромагнітними випромінюваннями й наведеннями. Для захисту від зазначеної погрози використають криптографічні методи, стеганографію, екранування, фільтри, радіоущільнювачі, генератори шумів і т.п.

Пиггибекинг. Суб'єктивна активна погроза Кцд-типа, запобігти й виявити яку досить важко, частота появи, швидше за все висока, а наслідки потенційно великі. За допомогою пиггибекинга здійснюється несанкціоноване проникнення в систему через одержання доступу в результаті тимчасової відсутності або некоректного завершення сеансу роботи легального користувача. Запобігти погрозі можна за допомогою охоронних систем, спеціальних програм захисного екрана й т.п.

Підробка. Суб'єктивна активна погроза Ц-типа, запобігання й виявлення якої може бути важким, частота появи невідома, а наслідки потенційно дуже великі. Підробка пов'язана з навмисним перекручуванням ІР, спрямованим, наприклад, на протизаконне виготовлення документів, записів, файлів і т.п. з метою використати їх замість дійсних.

Навмисне ушкодження даних або програм. Суб'єктивна активна погроза Ц-типа, запобігання й виявлення якої досить складне, частота появи невідома, але швидше невисока, а наслідки потенційно дуже великі. Ця погроза супроводжується зловмисним руйнуванням суб'єктом таких ІР, як файли, записи, різні дані й т.п.

Перешкоджання використанню. Суб'єктивна активна погроза Д-типа, запобігти яку досить важко, виявити легко. Частота появи невідома, а наслідки потенційно дуже великі. Ця погроза пов'язана з уповільненням роботи в системі, наприклад, за рахунок вилучення важливих ключових файлів, зміни їхніх імен, несанкціонованого захоплення ресурсів і т.п.

Програми розкриття паролів. Суб'єктивна активна погроза К-типу, запобігання й виявлення якої може бути дуже складним, частота появи невідома, а наслідки потенційно дуже великі. Такі програми, як правило, призначені для вгадування паролів (наприклад, архівіруваних файлів) через перебір варіантів, можливих для використання символів або проникнення в систему за допомогою словників. Програми, які засновані на останньому методі, здійснюють злом системи парольного захисту через перебір елементів одного або декількох словникових файлів, складених спеціально або взятих із серверів або жорстких дисків локальних станцій.

Різні версії. Суб'єктивна пасивна погроза Ц-типа, запобігти й виявити яку складно, виникає досить часто, а наслідки потенційно великі. Використання різних версій, наприклад, однієї й тієї ж програми, часто приводить до різних непорозумінь, які пов'язані з тим, що нові версії можуть інакше редагувати або створювати файли, а також містити помилки, які не дозволяють нормально її експлуатувати. У цьому випадку доводиться повертатися до старих

версій, тому не треба поспішати їх знищувати. Досить часто виникають випадки, коли файл із однаковим ім'ям зберігається (наприклад, коли немає доступу до диска з файлом і доводиться використати (редагувати) резервну копію, або коли остання версія перенесена в інший каталог) у різних частинах диска або дискового простору й нерідко помилково використається інформація (файл) не самої останньої редакції. Після її зміни (доповнення) вона подається як останній варіант, при цьому попередня модифікація не враховується. Таким чином, жодна версія не буде достовірною, що порушить цілісність даних і може привести до серйозних наслідків.

Самозванство. Суб'єктивна активна погроза Кцд-типа, запобігти й виявити яку досить складно, частота появи невідома, а наслідки потенційно великі. Самозванство, як правило, пов'язане з використанням чужого ідентифікатора для проникнення в систему з метою вивчення й копіювання даних, використання робочих станцій і серверів, ініціалізації програм, заміни імен і т.п.

Збір сміття. Суб'єктивна активна погроза К-типу, запобігти й виявити яку досить складно, частота появи невідома, а наслідки потенційно дуже великі. Під збором сміття мають на увазі спосіб одержання інформації через відновлення й перегляд вилучених (з інформаційних носіїв) файлів використаних дисків, стрічок, листингов, копірок й інших відходів інформаційної діяльності.

Мережні аналізатори. Суб'єктивна активна погроза К-типу, запобігання й виявлення якої майже неможливе або дуже складне; частота появи невідома й прогресує, а наслідки потенційно дуже великі. Зазначені аналізатори будують на базі програмно-апаратних засобів (в окремих випадках у вигляді програмних, що запускають на робочій станції, підключеної до мережі), призначених для зчитування будь-яких параметрів потоку даних.

Соціальний інжиніринг. Суб'єктивна, активна погроза К-типу, запобігти й виявити яку досить складно, частота появи невідома, а наслідки потенційно дуже великі. Ця погроза пов'язана з одержанням певних даних (наприклад, імен користувачів, паролів, номерів телефонів вилученого доступу й ін.) від різних людей, що атакують за допомогою інформаційного обміну.

Стихійні лиха. Об'єктивна погроза Цд-типа, запобігти яку досить складно, вплив, як правило, очевидно, зустрічається з невідомою частотою, а наслідки потенційно дуже великі. До цієї погрози можна віднести пожежі, які приводять до значних фінансових втрат, а також землетруси, повені, урагани, затоплення, навали гризунів і комах і т.п.

Суперзаппинг. Суб'єктивна активна погроза Кцд-типа, запобігти й виявити яку досить складно, частота появи невідома, а наслідки потенційно дуже великі. Фактично, ця погроза пов'язана з несанкціонованим застосуванням утиліт для модифікації, знищення, копіювання, розкриття, вставки, використання або заборони використання комп'ютерних даних.

Таємні ходи. Залежно від мотиву, суб'єктивна активна або пасивна погроза Кцд-типа, запобігти й виявити яку дуже складно, частота появи невідома, а наслідки потенційно великі. Таємний хід, спеціально створений розроблювачем або виниклий випадково, фактично є додатковим способом проникнення в систему.

Троянські коні. Суб'єктивна активна погроза Кцд-типа, запобігти яку майже неможливо або дуже складно, виявити досить важко, частота появи невідома, а наслідки потенційно дуже великі. Фактично троянський кінь це спеціальна програма, що дозволяє дії, відмінні від певних у специфікації, використовуваного ПЗ.

Із прикладів зазначених погроз бачимо, що природа їхнього походження й властивості різнобічні. Це обставина потрібно враховувати під час побудови моделей і систем ЗИ.

Інформаційна безпека галузі є складовою частиною безпеки держави в цілому, тому питанням інформаційної безпеки в авіації приділяється підвищеної увага. Як й у будь-якій іншій галузі, в авіації здійснюється передача різної інформації. До неї ставляться передача мовних повідомлень, радіолокаційної, радіонавігаційної й метеорологічної інформації, цифрових даних, текстових повідомлень тощо.

Існують системи обміну інформацією типу «земля-земля», «повітря-земля», «повітря-повітря», а також космічні технології зв'язку. У всіх цих системах широко застосовується обчислювальна техніка, що дозволяє створювати комп'ютеризовані мережі зв'язку типу ATN (Aeronautical Telecommunication Network - авіаційна телекомунікаційна мережа). Тому тут доречно розглядати безпеку в информационно-комуникационных системах.

Інформація, що циркулює в мережах ATN й інших авіаційних службах має комерційну цінність, а в деяких випадках є закритою інформацією, тому необхідно розробляти методи й засоби захисту цієї інформації. Система безпеки спрямована на запобігання несанкціонованого одержання інформації, фізичного знищення або модифікації інформації, що захищається.

Можливість зловживання інформацією, що передається в мережі АТ розвивається й удосконалиться не менш інтенсивно, чим засобу їхнього попередження.

Тому проблема захисту інформації вимагає організації цілого комплексу спеціальних заходів з метою попередження втрати інформації, що втримується в каналах телекомунікацій. Під інформаційною безпекою(information system security) будемо розуміти властивість информационно-телекомуникационной системи протистояти спробам несанкціонованого доступу.

Комплексний підхід до інформаційної безпеки передбачає розвиток всіх методів і засобів захисту інформації.

До методів забезпечення інформаційної безпеки відносять:

- перешкода - складається у фізичному перешкоджанні на шляху зловмисникові до інформації, що захищається;
- керування доступом до інформації - охоплює ідентифікацію користувачів персоналу й об'єкта по ідентифікаторі, що він представляє; перевірку повноважень; дозвіл і створення умов роботи в рамках установленого регламенту; реєстрацію звертань до захищених ресурсів, реагування на несанкціоновані дії;
- маскирование - пов'язане з користуванням способів криптографічного захисту;
- регламентація - пов'язаної зі створенням таких умов автоматизованої обробки зберігання й передачі захищає информации, що, при яких несанкціонований доступ зводиться до мінімуму;
- примус - користувачі й персонал системи змушені дотримуватися правил обробки, передачі й використання захищає информации, що, під погрозою матеріальної адміністративної або кримінальної відповідальності;
- спонукання - спонукує користувача й персонал системи не порушувати норм моралі й етики, які зложилися в суспільстві.

Ці методи забезпечення інформаційної безпеки реалізуються на практиці за допомогою різних засобів захисту – апаратні, програмні, програмно-апаратні, криптографічні, стеганографические, організаційні, законодавчі й морально-етичні [17].

Апаратні засоби - різноманітні механічні, електричні, електромеханічні, електронні, механічні та інші пристрої й системи (наприклад, джерела безперебійного харчування, криптографічні обчислювачі й Сбис-процессоры, електронні ідентифікатори й ключі, пристрої для виявлення жучків, генератори шумів і т.п.), які функціонують автономно, а також можуть вбудовуватися або з'єднуватися з іншими апаратурами для блокування дій дестабілізуючих факторів і рішення інших завдань захисту інформації (ЗІ).

Програмні засоби - спеціальні програми (наприклад, антивіруси, шифрувальники даних, що реалізують алгоритми цифрового підпису, що розділяють доступ, що оцінюють ризики, що визначають рівень безпеки, супроводу експертиз і т.п.), які функціонують у межах комп'ютерної системи для рішення завдань ЗІ.

Програмно-апаратні засоби- взаємозалежні апаратні й програмні засоби (наприклад, банківські системи захисту електронних платежів, комплексні ІКС конфіденційного зв'язку, автоматизовані системи контролю доступу персоналу й транспортних засобів у режимних зонах і т.п.), які функціонують автономно або в складі інших систем з метою рішення завдань ЗІ.

Криптографічні засоби - засобу, призначені для ЗІ шляхом криптографічного перетворення інформації (шифрування, дешифрування), що реалізується за допомогою асиметричних або симетричних криптографічних систем. Асиметричні криптографічні системи ґрунтуються на криптографії з відкритим ключем. Наприклад, найбільш відомими практичними реалізаціями цього типу є системи Диффи-Хеллмана, RSA й Ель-Гамаля.

Симетричні криптографічні системи ґрунтуються на криптографії із секретним ключем, найбільш відомими практичними реалізаціями яких є, наприклад, DES, ГОСТ 28147-89 і т.п. Практичне використання сучасних криптографічних засобів тісно пов'язане з фундаментальними дослідженнями в цій області й здійснюється через відповідні апаратні, програмні й апаратно-програмні засоби, побудовані на їхній основі. До таких засобів ставляться, наприклад, системи Криптон, Тессера, Клиппер і т.п. Слід зазначити, що із цим класом засобів тісно зв'язаний криптоанализ, що ефективно використається для випробування надійності криптографічних систем.

Останнім часом інтенсивно розвиваються стеганографические засобу (стеганография (приховання інформації в такій формі, коли сам факт наявності інформації не очевидне, наприклад приховання даних у звукових або графічних файлах, що входять до складу ОС Windows 95), але широкого практичного застосування (особливо на державному рівні) вони поки не одержали.

Організаційні засоби - організаційно-технічні й організаційно-правові заходи (наприклад, організація розробки й використання систем ЗІ, контроль за знищенням носіїв й інформації з обмеженим доступом, планування заходів щодо відновлення потеряной інформації, аудит систем захисту, експертизи й т.п.), які здійснюються протягом всіх технологічних етапів (проектування, виготовлення, модифікація, експлуатація, утилізація й т.п.) існування ІКС із метою рішення завдань ЗІ. Розробляючи організаційні засоби, необхідно враховувати, щоб у загальній безлічі механізмів захисту вони могли самостійно або в комплексі з іншими засобами вирішувати завдання захисту, забезпечувати ефективне використання засобів інших класів, а також раціонально поєднувати всі засоби в єдину цілісну систему захисту. Слід зазначити, що безліч всіх потрібних і потенційно можливих організаційних засобів невизначене й не існує формальних методів формування їхнього переліку й змісту. Виходячи із цього можна вважати, що основними методами формування організаційних засобів є неформальн-евристичні.

Законодавчі засоби - нормативно-правові акти (конвенції, закони, укази, постанови, нормативні документи й т.п.) призначені для забезпечення юридичної підтримки для рішення завдань ЗІ. Наприклад, одним з ефективних засобів захисту від несанкціонованого копіювання ПО може стати відповідний закон про захист авторських прав. Загалом, за допомогою законодавчих засобів визначаються права, обов'язки й відповідальність відносно правил взаємодії з інформацією, порушення яких може вплинути на стан її захищеності. У світовій практиці основу зазначених засобів становлять патентне й авторське право, національні закони про державну таємницю й обробку інформації в ІКС, ліцензування, страхування, сертифікація, класифікаційні нормативні документи й т.п.

Морально-етичні засоби - моральні норми й етичні правила, які зложилися в суспільстві, колективі й об'єкті інформаційної діяльності (наприклад, BBS), порушення яких ототожнюється з недотриманням загальноприйнятих дисциплінарних правил і професійних ідеалів. Прикладом таких засобів може бути кодекс професійного поводження членів Association for Computing Machinery [17] нетикет , етика хакера [17] і т.п.

Отже, інформаційна безпека це комплекс заходів, що забезпечує для охоплюваної їм інформації наступні фактори [17]:

- конфіденційність - можливість ознайомиться з інформацією мають у своєму розпорядженні тільки ті особи, хто володіє відповідними повноваженнями;
- цілісність - можливість внести зміни в інформацію повинні мати тільки ті особи, хто на це вповноважені;
- доступність - можливість одержання авторизованого доступу до інформації з боку уповноважених осіб у відповідний санкціонований для роботи період часу;
- облік - означає, що всі значимі дії особи, виконувані нею у рамках, контрольованих системою безпеки, повинні бути зафіксовані й проаналізовані;
- відмовність або апеляйність - означає, що особу, що направила інформацію іншій особі, не може відректися від факту посилання інформації, а особа, що одержала інформацію, не може відректися від факту її одержання.

Зазначені цілі інформаційної безпеки забезпечуються застосуванням наступних механізмів або принципів:

- політики - набір формальних правил, які регламентують функціонування механізму інформаційної безпеки;
- ідентифікація - розпізнавання кожного учасника процесу інформаційної взаємодії перед тим, як до нього будуть застосовані які б то не було поняття інформаційної безпеки;
- аутентифікація - забезпечення впевненості в тім, що учасник процесу обміну інформацією ідентифікований вірно, тобто дійсно є тим, чий ідентифікатор він пред'явив;
- контроль доступу - створення й підтримка набору правил, що визначають кожному учасникові процесу інформаційного обміну дозвіл на доступ до ресурсів і рівень цього доступу;
- авторизація - формування профілю прав для конкретного учасника процесу інформаційного обміну з набору правил контролю доступу;
- аудит і моніторинг - регулярне відстеження подій, що відбуваються в процесі обміну інформацією в процесі з реєстрацією й аналізом значимих або підозрілих подій;
- реагування на інциденти - сукупність процедур або заходів, які виробляються при порушення або підозрі на порушення інформаційної безпеки;
- керування конфігурацією - створення й підтримка функціонування середовища інформаційного обміну в працездатному стан і відповідно до вимог інформаційної безпеки;
- керування користувачем - забезпечення умов роботи користувачів у середовищі інформаційного обміну відповідно до вимог інформаційної безпеки;

- керування ризиками - забезпечення відповідності можливих втрат від порушення інформаційної безпеки потужності захисних засобів;
- забезпечення стійкості - підтримка середовища інформаційного обміну в мінімально припустимому працездатному стані й відповідності вимогам інформаційної безпеки в умовах деструктивних зовнішніх і внутрішніх впливів.

1.2. Стандарти інформаційної безпеки

Важливим елементом оцінювання стану безпеки є експертиза як технічне підтвердження того, що заходи безпеки й контролю, підібрані для певного ЗЗІ, відповідають стандартам і нормально функціонують. Стандарти інформаційної безпеки - найважливіший критериальний засіб, використовуваний для рішення прикладних завдань захисту.

Найбільш відомі у світовій практиці такі стандарти: “Критерії безпеки комп'ютерних систем Міністерства оборони США”, що керують документи які управляють Гостехкомисією при Президентові Російської Федерації, “Європейські критерії”, “Федеральні критерії безпеки інформаційних технологій”, “Канадські критерії безпеки комп'ютерних систем”, а також “Єдині критерії безпеки інформаційних технологій”.

Це не повний перелік, однак він містить найважливіші аспекти як з погляду розвитку цих документів, так і рішення завдань захисту інформації в Україні.

Приведемо основні висновки аналізу стандартів щодо їхнього використання.

В “Критеріях безпеки комп'ютерних систем Міністерства оборони США”; які називають “Жовтогарячою книгою”, запропоновані такі категорії вимог безпеки: політика безпеки, аудит, коректність. Тут, зокрема, є також вимоги до документаційного забезпечення (ДЗ). Передбачено чотири групи критеріїв: D (клас D1), C (класи C1, C2), B (класи B1, B2, B3) і A (клас A1), які характеризують ступінь захищеності, починаючи від мінімальної й закінчуючи формально доведеною.

Варто сказати, що в цьому документі критерієм оцінки фактично є відповідність безлічі засобів захисту даної системи безлічі, зазначеному в одному із класів оцінки й у випадку, коли набір засобів недостатній, то систему захисту відносять до першого нижчого класу, а для перевірки її приналежності до вищого необхідно застосовувати спеціальні й трудомісткі методики, що практично нездійсненно для реальних систем.

В “Критеріях безпеки інформаційних технологій”, розроблених країнами Європи (звідси назва “Європейські критерії”), загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту й рівня адекватності їхньої реалізації. У цьому стандарті виявляється тісний зв'язок з американськими, але головна відмінність “Європейських критеріїв” полягає в тому, що тут уперше введено поняття адекватності засобів захисту й спеціальна шкала критеріїв, причому адекватності приділяється значно

більше уваги, чим функціональним вимогам. Під час перевірки адекватності аналізується весь життєвий цикл системи від початкової стадії проектування до експлуатації й супроводу. У документі визначається сім рівнів адекватності – Ei ($i = \overline{0,6}$). Рівень E0 - мінімальний (аналог рівня D "Жовтогарячої книги"), на рівні E1 аналізується лише загальна архітектура системи, а адекватність засобів захисту підтверджується функціональним тестуванням, на рівні E3 до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення, а на E6 уже необхідно формальний опис функцій безпеки, загальної архітектури й політики безпеки. Ступінь безпеки визначається найбільш слабким із критично важливих механізмів захисту.

Укажемо, що важливим недоліком документа Європейських критеріїв є те, що в ньому немає чіткого взаємозв'язку між процесом проектування системи й оцінкою її безпеки, що може ввести додаткові витрати під час доробки КС із метою підвищення рівня захищеності. Також зізнається можливість наявності недоліків у сертифікованих системах. Тим самим засвідчує їхню недосконаліть, а для виявлення й класифікації цих недоліків у конкретних функціонуючих системах необхідні розробка й застосування спеціальних методик.

Гостехкоміссія при Президенті Російської Федерації прийняла ряд керівних документів, де пропонується дві групи критеріїв безпеки: 1) показники захищеності від НСД (дає можливість оцінювати ступінь захищеності окремих компонентів автоматизованих систем (АС)) і 2) критерії захищеності АС обробки даних (для оцінки всефункціональних систем). Показники захищеності містять вимоги захищеності зазначених засобів від НСД до інформації й застосовуються в загальносистемних програмних засобах й операційних системах. Конкретні переліки показників визначають класи захищеності засобів обчислювальної техніки й описуються сукупністю вимог, які зокрема пред'являються до керівництва користувача, посібнику з комплексу засобів захисту, текстової документації, конструкторської (проектної) документації й ін. Установлено сім класів захищеності засобів обчислювальної техніки від НСД до інформації, а також дев'ять класів для оцінки рівня захищеності АС від НСД.

Недоліком цього стандарту є те, що засоби захисту спрямовані тільки на протидію зовнішнім погрозам, а до внутрішньої структури системи, її функціонування не висуваються ніякі вимоги. До того ж, у порівнянні з іншими стандартами ранжирування вимог по класах захищеності дуже спрощене й визначається наявністю або відсутністю певної безлічі захисних механізмів. Це обставина значно зменшує гнучкість вимог й у багатьох випадках ускладнює можливість практичного використання документів.

В “Федеральних критеріях безпеки інформаційних технологій” запропонована концепція профілю захисту, що містить вимоги до проектування й технології розробки, а також кваліфікаційний аналіз продукту інформаційних технологій (Іт-продукта). Документування процесу розробки - одне з обов'язкових вимог до технології розробки Іт-продуктов і надалі до проведення кваліфікаційного аналізу. Вимоги до документування визначають склад і зміст технологічного документационного забезпечення (ДЗ) і містять:

- документування функцій ядра безпеки;
- повну документацію на Іт-продукт;
- документування, тестування й аналіз Іт-продукта, що містить документування процесу тестування функцій, аналізу можливостей порушення безпеки й аналізу схованих каналів;
- документування середовища й процесу розробки.

У свою чергу, вимоги до супроводу Іт-продукта регламентують склад користувальницької й адміністративної документації, процедуру відновлення версій і виправлення помилок, а також інсталяцію продукту. У вимогах до класифікаційного аналізу Іт-продукта описана процедура проведення тестування функцій ядра безпеки як самим розроблювачем Іт-продукта, так і незалежним експертом.

Недоліком цього стандарту є те, що в ньому викладені лише загальні вимоги (наприклад, до ДЗ) не передбачають їхній розподіл на рівні або градації й, тому, в експерта можуть виникнути труднощі під час здійснення оцінювання, оскільки він не має належного інструмента для якісної оцінки продукту.

Перевагою цих критеріїв є те, що замість узагальненої універсальної шкали класів безпеки й твердих вказівок, цей документ містить погоджений з попередніми стандартами ранжируваний перелік функціональних вимог, що дозволяє розроблювачам і користувачам підбирати найбільш підходящі вимоги для конкретного Іт-продукта й середовища його експлуатації.

В “Канадських критеріях безпеки комп'ютерних систем”, уведене незалежне ранжирування вимог за окремо взятим розділом, у результаті чого визначиться безліч окремих критеріїв, що характеризують роботу окремих підсистем, які забезпечують безпеку. У цьому документі, крім функціональних критеріїв, уведені критерії адекватності реалізації, що відображають рівень коректності реалізації політики безпеки й визначають вимоги до процесу проектування, розробки й реалізації ІКС.

Цей документ має такий же недолік, як й “Федеральні критерії”, оскільки, наприклад, відсутність градацій в оцінюванні документів не дозволяє якісно виконати цю процедуру.

“Єдині критерії безпеки інформаційних технологій” [21] стали продуктом об'єднання канадських, федеральних й європейських критеріїв [21] у єдиний погоджений документ. Ці критерії регламентують всі стадії розробки, кваліфікаційного аналізу й експлуатації Іт-

продуктов. Вони визначають безліч типових вимог, уводять частково впорядковані шкали, які дозволяють споживачам створювати окремі вимоги, що відповідають їхнім потребам. Основними документами, які описують всі аспекти безпеки Іт-продукта (з погляду користувачів і розроблювачів), є відповідно профіль захисту й проект захисту.

В Україні також прийнятий ряд документів, які регламентують порядок захисту інформації. Вони засновані на Законі України «Про захист інформації в автоматизованих системах», що був пізніше змінений на Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», а також на «Положенні про технічний захист інформації».

Тут також уведені в дію нормативні документи (НД) системи технічного захисту інформації (СТЗІ) [20] "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", а також НД по технічному захисті інформації (ТЗІ) на програмно-керованих АТС загального користування.

В українських критеріях [20] у процесі оцінювання здатності ІКС забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги до функцій захисту (послугам безпеки) і до гарантій. Якщо розглянути, як приклад, вимоги до експлуатаційного ДЗ, то відзначається, що у вигляді окремих документів або розділів (підрозділів) інших документів розроблювач повинен надати опис послуг безпеки, реалізованого комплексу засобів захисту, керівництва адміністратора й користувача щодо послуг безпеки.

Тут, зокрема, робиться застереження, що в описі функцій безпеки повинні бути викладені основні (необхідні для правильного використання послуг безпеки) принципи політики безпеки, що реалізується комплексом засобів захисту, оцінюваної ІКС, а також самі послуги. Перелік складових для опису політики безпеки інформації перебуває в НД ТЗІ 3.7–001–99 "Методичні вказівки по розробці технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі" [20]. Наприклад, керівництво адміністратора по послугах безпеки повинне містити:

- опис засобів інсталяції, генерації й запуску ИКС;
- опис всіх можливих параметрів конфігурації, які можна використати в процесі інсталяції, генерації й запуску ИКС;
- опис властивостей ИКС, які можна використати для періодичного оцінювання правильності функціонування комплексу засобів захисту;
- інструкції з використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує ИКС.

У посібнику користувача по послугах безпеки повинні бути інструкції щодо використання функцій безпеки звичайним користувачем.

У "Критеріях оцінки" також зазначено, що керівництво адміністратора й посібник користувача можуть бути об'єднані в керівництві з установки й експлуатації. Відповідно цих стандартів ПЗ може бути сертифіковане при наявності повного набору перерахованих документів.

У методичних вказівках відзначається, що повний перелік такого необхідного ПЗ визначається розроблювачем СЗІ й узгоджується із замовником, а на етапі їхніх випробувань і здачі в експлуатацію, якщо необхідно розробку спеціальних апаратур і ПЗ, може також знадобитися розробка відповідного ПЗ.

Для підвищення гнучкості при реалізації процедури оцінювання варто трохи розширити встановлені вимоги за допомогою використання додаткових критеріїв. Важливо вказати, що, наприклад, при оцінюванні ПЗ потрібно враховувати зручність і можливість його відновлення й своєчасного доповнення, наявність навчальних систем, а також виклад матеріалу в загальноприйнятих термінах.

Комплекс засобів захисту на предмет відповідності зазначеним критеріям оцінює експертна комісія. Для того щоб експертна комісія привласнила ІКС певний клас, повинні бути визначені рівні реалізованих послуг в об'єднанні з рівнем гарантій (РГ). Однак у нормативному документі передбачається, що вимоги, наприклад до ПЗ, є загальними для всіх РГ, тобто тут не оцінене якість матеріалу, що надається на експертизу, а кількісна його оцінка недостатня для повноцінної сертифікації ІКС, оскільки наявність відповідного вичерпні ПЗ є одним з важливих факторів, що впливає на ефективність використання інструментальної СЗІ.

Найчастіше експерти, які оцінюють певну ІКС, не завжди можуть чітко визначити рівень захищеності її СЗІ, оскільки в існуючих стандартах не до кінця визначені параметри, які вносять в оцінювання елементи нечіткості, розмитості. Головна функція стандартів - узгодження позицій і запитів виробників, споживачів й експертів. При цьому останні хочуть мати такі документи, де б докладно була наведена процедура кваліфікаційного аналізу, а також надавалися прості, однозначні й легко застосовні критерії. Очевидно, що практично такий стандарт створити складно й у реальності завжди прийде прибігати до певних компромісів для оцінювання захищеності КС.

Аналіз закордонних і сучасних вітчизняних стандартів в області безпеки інформації показав [20], що їхнє успішне застосування вимагає додаткових спеціальних методик оцінювання (наприклад, ПЗ) враховуючі різні кількісні і якісні показники.

1.3. Сучасні методи й засоби оцінки стану безпеки

Стан безпеки інформації - найважливіша характеристика ІКС, від якої значною мірою залежить рівень довіри (РД) користувача до наданих системою функціям і ресурсам.

Забезпечення потрібного рівня такого стану нерозривно пов'язане з реалізацією ряду заходів, які можна поділити на чотири основні групи [21]: 1 (аналіз погроз; 2 (розробка, вибір і застосування заходів і засобів безпеки, адекватних погрозам; 3 (їхня сертифікація й акредитація; 4 (планування й організація дій у непередбачених обставинах. Розробка методів і засобів, які забезпечують ефективність цих заходів, пов'язана з реалізацією різного виду оцінок, наприклад, для виміру рівня ризику, захищеності, гарантій або вибору оптимального варіанта системи захисту й т.п.

Розглянемо методи й засоби, які використаються в теорії й практиці інформаційної безпеки для рішення деяких завдань такого класу.

Відома узагальнена послідовність виміру безпеки [20], що включає узагальнені нижчеподані кроки.

Крок 1. Формулювання вимог і підходів, включаючи вимоги забезпечення необхідного рівня безпеки.

Крок 2. Використання обраних методів виміру.

Крок 3. Інтерпретація результатів.

Крок 4. Визначення відповідності обмірюваного рівня безпеки необхідному.

З наведених кроків видно, що дана послідовність не орієнтована на використання конкретних методів, моделей і пристроїв.

Відома також модель поводження потенційного порушника, що здійснює НСД до будь-якої частини зберігаємої, оброблюваної і переданої в ІКС інформації якій потрібен захист. У моделі передбачається шість найнебезпечніших ситуацій, щодо яких можна встановити набори вихідних даних (ВД), необхідних для створення системи захисту, а також визначити основні способи її побудови.

Далі для оцінки рівня захищеності інформації, що обробляється в конкретній (з урахуванням специфіки) ІКС, пропонується послідовно вирішити заданий набір завдань. Для цього попередньо треба визначитися з початковими умовами, що містять моделі очікуваного поводження порушника, вибір яких впливає на кінцевий результат оцінювання захищеності. Під час побудови моделей розглядаються еталонний і диференційований підходи, які відповідно орієнтовані тільки на професіонала й на заздалегідь певну кваліфікацію порушника.

При диференційованому підході порушників розділяють на чотири класи (висококваліфікований, кваліфікований, некваліфікований і недисциплінований користувач), кожному з яких у комплексі засобів обробки даних в ИКС буде відповідати певний набір можливих каналів НСД.

Виходячи з моделі поводження потенційного порушника і його класу, автор пропонує взяти за основу чотири класи безпеки, а для забезпечення кожного з них необхідно

забезпечити ІКС набором відповідних засобів захисту, які перекривають заздалегідь відомі безлічі можливих каналів НСД. Після цього вважається, що побудовано закритий захисний контур. Рівень захищеності в границях класу визначається кількісними показниками "міцності" окремих фрагментів захисту й контуру в цілому.

Нижчеподані показники захищеності носять імовірнісний характер, а їх величини залежать від "міцності" найбільш слабкої ланки. Імовірність неподолання порушником перешкоди з урахуванням можливої відмови системи (Р) визначають за формулою

$$P = P_{в.\,бл}(1 - P_{отк}) \wedge (1 - P_{обх}1) \wedge (1 - P_{обх}2) \wedge \ldots \wedge (1 - P_{обх}j),$$

де Рв. бл = (1 – Рпр) – імовірність виявлення й блокування несанкціонованих дій порушника, Ротк(t) = e-λt – імовірність відмови системи, Робх – імовірність обходу перешкоди порушником, j – кількість шляхів обходу перешкоди, Рпр – імовірність подолання перешкоди порушником.

Для неконтрольованих можливих каналів НСД розрахунок здійснюється за виразом

$$P_{СЗИ} = (1 - P_{пр}) \wedge (1 - P_{обх}1) \wedge (1 - P_{обх}2) \wedge \ldots \wedge (1 - P_{обх}j).$$

У випадку, коли канали закриті двома й більше засобами захисту, розрахунок виконують за формулою

$$P_{\Sigma} = 1 - \prod_{i=1}^{m} (1 - P_i) \ ,$$

де і – порядковий номер перешкоди; m – кількість дублюючих перешкод; P_i – "міцність" і-го перешкоди.

Слід зазначити, що вищеописаний підхід до оцінювання захищеності, запропонований у роботі [21], передбачає початкові умови, які задаються в технічному завданні на КС обробки даних, де й обмовляється модель порушника, тобто засобу захисту від порушників певного класу вже визначені на етапі проектування й фактично виконується оцінювання їх "міцності". У такому підході не передбачений випадок, коли оцінювання необхідно виконувати у вже функціонуючих системах й, тим більше, в умовах невизначеності. Наприклад, якщо заздалегідь невідомо як буде організований захист, які засоби будуть використатися і як буде здійснюватися обробка параметрів, що надходять у нечіткій формі.

У роботі [21] запропонований метод експертних оцінок безпеки, у якому розглядається система, що забезпечує захист відносно n-го числа характеристик. Ці характеристики є перетинанням набору засобів захисту. Якщо ці засоби використаються спільно, то збільшується ступінь забезпечення безпеки КС. Для кількісного оцінювання цього ступеня вводиться деяка "гарна міра" Gi характеристики Fi. Уважається, що якщо Gi=0, то характеристики Fi система не має.

Далі використається суб'єктивний ваговий коефіцієнт важливості (КВ) Wi, привласнений характеристиці Fi деяким експертом (експертами). При цьому повинні витримуватись умови 0≤□Gi≤□□□i Wi >□□ для 1≤i≤n.

Для визначення ступеня безпеки (SR) КС на підставі вже певних параметрів використається лінійний метод “зважування й підрахунку”, що представляється рівнянням

$$SR = \frac{1}{n}\sum_{i=1}^{n} W_i G_i .$$

У методі заздалегідь обумовлюється, що наведена формула деякою мірою суперечить положенню про визначення “міцності системи захисту міцністю її найбільш слабкої ланки”, і показано, що для ідеально безпечної системи SR=1, а для цілком незахищеної SR=0.

Далі зазначено, що експертні оцінювання безпеки можуть бути дуже корисними, а визначення КВ й якості характеристик, мабуть, завжди залишиться суб'єктивним.

У роботі [21] як засіб визначення стану безпеки запропонована експертна система для оцінювання рівня інформаційної захищеності об'єктів. Указується, що вона дозволяє в діалоговому режимі визначити характеристики об'єкта, у границях якого інформація повинна бути захищена. Система містить базу знань, на основі якої можна оцінити погрозу інформації й вибрати організаційні й технічні засоби, які підвищують ефективність захисту до потрібного рівня. У процесі розробки системи були побудовані алгоритми оцінки рівня погроз і реалізоване відповідне ПЗ, але нічого не сказано про те, які методи й моделі були використані.

Існує набір інструментальних програмних засобів аналізу ступеня ризику на підставі попередньо зібраної інформації [20]. Ці засоби аналізують відносини між цінностями, погрозами, уразливими місцями, захисними засобами, заходами, імовірностями різних подій і т.п. з метою визначення потенційних втрат. Автори цих розробок тільки вказують, що вимір втрат заснований на методах послідовних наближень, НЛ, а також використання дерева подій і помилок.

У відомих програмних продуктах, таких як @RISK, ALRAM (Automated Livermore Risk Analysis Methodology), BDSS (Bayesian Desicion Support System), LRAM (Livermore Risk Analysis Methodology) і інших, для оцінки ризику застосовують традиційні кількісні методи, які використають для знаходження очікуваного річного збитку. Його пошук здійснюється через оцінювання для всіх компонентів ИКС частоти подій, які порушують характеристики безпеки.

Відзначається, що частина інструментальних засобів орієнтована на оцінювання збитку від одиночної погрози, а інша ґрунтується на інформації про безпеку, що використається для точних й умоглядних висновків.

Далі сказано, що такі інструментальні засоби аналізу ступеня ризику, як BUDDY SYSTEM, CONTROL-IT, CRAMM і т.п., ґрунтуються на якісному підході й ефективно застосовуються у випадку, коли потенційна втрата непомітна, а ризик не можна виразити в грошовому еквіваленті. При такому підході результати ризику виражаються в лінгвістичній формі, наприклад, “немає ризику” або “дуже великий ризик”.

Відзначимо, що прихильники кількісного підходу, аналізуючи ступінь ризику, дотримуються тієї позиції, що ефективність засобів захисту щодо втрат не можна оцінити, якщо немає кількісних показників ступеня ризику. Прихильники ж якісного підходу затверджують, що кількісні методи вимагають виконання точних оцінок, навіть у тому випадку, коли інформація неповна, розмита або навіть не цілком достовірна.

Слід зазначити, що в роботі [21] не наведено конкретних методологій, моделей і математичних викладень, які є основою побудови описаних систем оцінки ризику, але досить добре описані деякі методи, які знайшли своє застосування в теорії інформаційної безпеки, наприклад, ранжирування погроз на підставі дельфийских списків, під якими мається на увазі група експертів, що збирає інформацію в межах проблемної області.

Дельфийска команда - це основа комп'ютеризованих експертних систем, оскільки на базі їхніх знань формуються продукційні правила, які моделюють ухвалення рішення людиною. Команди формуються виходячи з компетентності в досліджуваній області знань конкретної системи, рівня информированности про стан справ, практичного досвіду й ін. з метою об'єднання суджень експертів для досягнення певного консенсусу.

Для оцінювання ризику команда визначає безліч погроз із метою їхнього ранжирування по ступені небезпеки. Далі судження членів команди інтегруються й генерується колективне рішення про небезпеку погроз, відображуване в упорядкованому по зменьшенню списку. В основу формування такого списку можуть бути покладені різні принципи, наприклад, найбільший ризик, рівень таємності, вартість, трудомісткість, наслідки, збитки, імовірність виникнення й т.п. Часто впорядкування робить одна особа, діючи при цьому як дельфийская команда.

Далі в роботі описуються просте, кардинальне й відносне ранжирування ризику.

По методу простого ранжирування всі можливі погрози, уразливі місця та інші характеристики, які становлять основу критеріїв при прийнятті рішень, розставляються в зменьшувальний ряд, тобто найнебезпечніші або найбільш важливі елементи перебувають на початку списку, а менш значущі наприкінці.

Метод кардинального ранжирування ґрунтується на тім, що кожній погрозі в результаті її впливу привласнюється конкретне числове значення, певне сумою збитку. Такий метод, як правило, використає категорії високого, середнього й низького ризиків.

При відносному ранжируванні будь-який список заносять у таблицю, по якій будують трикутну матрицю. Після цього переходять до простого ранжирування, а отримана матриця стає моделлю рішення.

Такий метод істотно спрощує консолідацію суджень завдяки можливості порівняння окремо взятої погрози з тими, які залишилися. Для полегшення ухвалення рішення корисної виявляється можливість порівняння двох погроз, ігноруючи всі інших.

Важлива перевага методу відносного ранжирування ризику полягає в тому, що немає потреби в ухваленні єдиного рішення, тобто експерт групи може віддати голос за одну із двох погроз або розділити його, наприклад, на рівнозначні частини (0,5 голосу на погрозу).

У роботі [21] автор, розкриваючи поняття захищеної системи, дотримується позиції, що безпека є якісною характеристикою системи, у результаті чого виникають труднощі щодо її виміру в будь-яких одиницях і потім порівняння безпеки, наприклад, двох систем.

Не можна також не враховувати той факт, що ухвалення рішення при експертизі залежить від суб'єктивних суджень експерта, його знань і досвіду. Зменшити негативний вплив цього фактора можна за рахунок розвитку відповідного методичного й наукового забезпечення. Із проведеного аналізу також випливає, що в області інформаційної безпеки недостатня теоретична база, яку можна застосовувати для рішення завдань якісної оцінки. Це особливо важливо тоді, коли немає повної інформації про систему, а ІД, які підлягають обробці, задані нечітко (розмито) і часто пов'язані із судженнями й інтуїцією людини.

Для роботи з нечітко детермінованими величинами, як правило, застосовують апарат теорії НМ, що оперує такими поняттями, як НМ, нечіткі (НП) або лінгвістичні змінні (ЛП), нечіткі відносини й ін.

Розділ 2. Інформаційні характеристики мовних повідомлень

2.1. Структурна схема системи зв'язку та її елементи

У процесі людської діяльності виникає потреба в передачі відомостей з місця їх виникнення до деякої віддаленої точки. Сукупність відомостей, або інформацію, яка повинна бути передана, називають повідомленням, а саме джерело виникнення – джерелом повідомлення (ДП).

Залежно від характеру повідомлення (кількості станів, в якому воно може знаходитись) розрізняють безперервні та дискретні повідомлення.

Для передачі повідомлення по лінії зв'язку використовують деякий фізичний процес як матеріальний носій інформації. Фізична величина, яка змінюється та відтворює стан джерела повідомлення, називається сигналом. Прикладом сигналів можуть бути струм у проводі, акустична хвиля в повітрі, електромагнітне поле і ін.

Будь-який сигнал можна подати у вигляді функції $x(t)$, де $x \in X$, $t \in T$. Якщо множини X та T мають нескінченну кількість елементів, то такі сигнали називають аналоговими. Якщо тільки множина T має кінцеву кількість елементів, то сигнали називають дискретними. У разі, коли X та T мають фіксовану кількість елементів, сигнали називають цифровими. Пристрої, які перетворюють повідомлення в сигнал, називають перетворювачами повідомлень (ПП). В якості ПП виступають мікрофони або ларингофони.

Середовище, в якому поширюється сигнал від передавача до приймача, називають лінією зв'язку. Лінії зв'язку (ЛЗ) бувають акустичні та електричні і в свою чергу поділяються на радіолінії та провідні лінії зв'язку.

В системах радіозв'язку для передачі сигналів за допомогою радіоліній використовують радіопередавачі (РПД) та радіоприймачі (РПМ).

Сукупність пристроїв, які забезпечують незалежну передачу та прийом інформації від джерела повідомлень до одержувача повідомлення (ОП), називають каналом зв'язку (КЗ).

Система зв'язку (СЗ) – це впорядкована сукупність каналу зв'язку, джерела та одержувача повідомлень, яка характеризується заданими правилами перетворення повідомлення в сигнал і відновлення повідомлення за прийнятим сигналом. Основним призначенням системи зв'язку є передача із заданою якістю інформації від джерела до одержувача повідомлення [1].

Структурна схема системи зв'язку показана на рис. 2.1.

Рис.2.1. Структурна схема системи зв’язку

Крім вищезгаданих скорочень, на рис. 2.1:

З – джерело завад;

СЧ – синтезатор частот;

ПС – перетворювач сигналу в повідомлення.

Системи зв’язку можна класифікувати за такими ознаками:

за призначенням:

– системи радіомовлення та телебачення;
– системи професійного зв’язку;

за видом джерела повідомлення:

– СЗ для передачі безперервних повідомлень;
– СЗ для передачі дискретних повідомлень;

за видом сигналу:

– аналогові СЗ;
– дискретні СЗ;
– цифрові СЗ;

за видом модуляції:

– системи з амплітудною модуляцією;
– системи з частотною модуляцією;
– системи з фазовою модуляцією;
– системи з імпульсною модуляцією;
– системи з шумоподібними сигналами;

за частотами, що використовуються;

за кількістю повідомлень, які передаються одночасно:

– одно канальні СЗ;
– багатоканальні СЗ;

за порядком обміну повідомленнями і т. ін.

2.2. Характеристики безперервних джерел та одержувачів повідомлень

Джерелом безперервних повідомлень є голосовий апарат людини, а мова вважається самим повідомленням. Одержувачем мовного повідомлення є слуховий апарат людини.

Системи зв’язку, в яких використовуються мовні повідомлення, ще називають телефонними системами.

Характерною особливістю систем передачі мовних повідомлень вважають наявність у них акустичних елементів (голосовий та слуховий апарати людини, мікрофон та телефон).

Розглянемо основні характеристики джерела звуків та слуху. Складовими елементами мовних повідомлень є слова та фрази. Слова, в свою чергу, складаються з більш простих елементів мови – складів та звуків, характерних для тієї чи іншої мови. Точного визначення терміна „звук мови” не існує. Його можна порівняти з великою літерою. Залежно від мови, місця наголосу кожний звук може мати різні відтінки. Так, нараховується декілька тисяч звуків, які відрізняються за суб’єктивним сприйняттям один від одного. Проте, все ж вдається класифікувати всі звуки та їх варіанти. А якщо ще й виділити типові ознаки звуків, то їх кількість вдається скоротити до 40...42. Такі типізовані звуки мови носять назву фонем. Кожна фонема має свої характерні ознаки, які легко розрізнити на слух. Але під час навіть найточнішого наголосу її в послідовній мові внаслідок впливу сусідніх звуків вона може набувати тих чи інших відтінків. Це будуть варіанти фонеми за місцем у слові або так звані фоноїди. [1]

Структура звуку досить складна та характеризується цілою низкою складових звукових частот. При цьому розрізняють голосні та приголосні звуки.

Спектр голосних звуків має дискретний характер і складається з основного тону та його гармонік. Математичне очікування частоти основного тону F_{OT} для чоловічого голосу складає 120 Гц, а для жіночого – 240 Гц. Під час промови повідомлень різними особами відбувається зміна частоти основного тону $\left(\frac{\partial F_{OT}}{\partial t}\right)$ навколо математичного очікування, що й визначає особу, яка веде розмову. Таким чином, кожна людина розмовляє з характерною для неї частотою основного тону F_{OT} та похідною $\frac{\partial F_{OT}}{\partial t}$.

Для глухих приголосних та мови пошепки характерний суцільний спектр звуків. Частотні спектри дзвінких приголосних звуків мають комбінований дискретний та суцільний вигляд.

Типова осцилограма голосного звуку показана на рис.2.2.

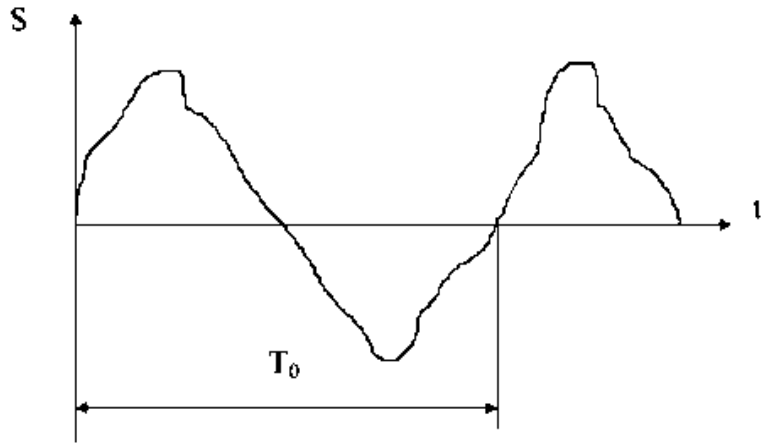


Рис.2.2. Осцилограма голосного звуку

В спектрі звуків утворюються області концентрації енергії, які носять назву формант. Іншими словами, формантою називають групу суміжних частотних складових спектра звуку, рівні яких більші, ніж у сусідніх складових. Для голосних звуків характерно до трьох яскраво виражених формант, які знаходяться в діапазонах: 300...1000 Гц (це перша форманта), 1000...2000 Гц (друга форманта) та 2000...3500 Гц (третя форманта) (рис. 2.3). Глухі приголосні мають лише одну форманту з досить розмитим екстремумом у діапазоні частот понад 1200 Гц. Слід зазначити, що кожній фонемі відповідає свій формантний рисунок. Це означає, що мозок людини аналізує розташування формант та їхню інтенсивність, отримує інформацію з мовного повідомлення.

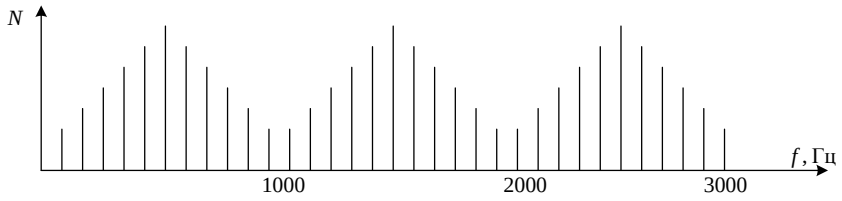


Рис.2.3. Спектр голосного звуку

Так звані вибухові звуки (п, к, т) не мають особистого формантного рисунку, а являють собою ту чи іншу зміну попередніх та наступних звуків.

Таким чином, діапазон частот, в якому розташовані форманти, які несуть інформацію про звуки, що промовляються, досить вузький. Він складає від 300 до 3500 Гц і носить назву телефонного каналу. Хоч під час розмови утворюються звуки в смузі частот від 100 до 9000 Гц, з точки зору отримання інформації немає ніякого сенсу робити телефонний канал ширше від 300....3500 Гц.

Все це стосується професійних систем зв’язку. В системах же радіомовлення та телебачення намагаються передати всі частоти, які утворюються під час розмови, співу, музичного супроводження тощо.

У професійному зв’язку завжди визначають темп мови, він складає близько $10\ \frac{\text{фонем}}{\text{с}}$. У разі такого темпу (швидкості проголошення фонем) інтервал існування звуків складає 20...300 мс, при цьому у голосних він більший, ніж у приголосних. Найкоротші звуки – це вибухові, вони звучать 20...30 мс.

Під час розмови утворюється звукова хвиля, яка зумовлює відповідний звуковий тиск. Його позначають літерою *P* та вимірюють у паскалях (Па). Відчуття гучності пов’язано з силою_звуку, яку позначають літерою *I* та вимірюють у $\text{Вт}/\text{м}^2$. Сила звуку еквівалентна потужності, а звуковий тиск – напрузі електричних коливань, тому можна записати, що $I \equiv P^2$.

Рівень інтенсивності звуків мови (*N*) вимірюють у децибелах (дБ). При цьому за одиницю, з якою порівнюють звукові коливання, приймають мінімальну силу I_0 звукових коливань, що відчуває вухо людини з середнім слухом. Ця сила на середніх частотах (600...800) Гц дорівнює $I_0 = 10^{-2}\ \text{Вт}/\text{м}^2$ або $P_0 = 2 \cdot 10^{-5}$ Па [1].

Тоді рівень будь-якого звукового коливання силою *I* та звуковим тиском *P* буде дорівнювати:

$$N = 10 \lg \frac{I}{I_0} = 20 \lg \frac{P}{P_0}.$$

Діапазон зміни рівнів звуків мови називають динамічним діапазоном мови. Вухо людини не відчуває звуків нижче 0 дБ, а поріг відчуття болю лежить у межах 120...125 дБ.

Рівні чутності звуків виражають у фонах та позначають літерою *L*. Рівень чутності *L* визначає число децибел рівня тону з частотою 1000 Гц, який рівнозначний зі звуком, що досліджується. Він також залежить від частоти (рис. 2.4). Виміри рівня чутності виконують за допомогою шумоміра.

Рівень різних частотних складових мови неоднаковий. Залежність усереднених за великий термін часу рівнів мови від частоти називають спектром мови. На рис. 2.5 наведено спектр української мови, звідки видно, що найбільші рівні мають складові мови в діапазоні 200...600 Гц, і тут зосереджена основна частка енергії мови.

Цікавою особливістю спектра мови є те, що в цьому частотному діапазоні можна отримати тільки інформацію про частоту основного тону та про першу форманту. Тому, у разі аналізу слухового апарату людини слід звернути увагу на те, яким чином компенсується такий невдалий розподіл енергії в спектрі мови.

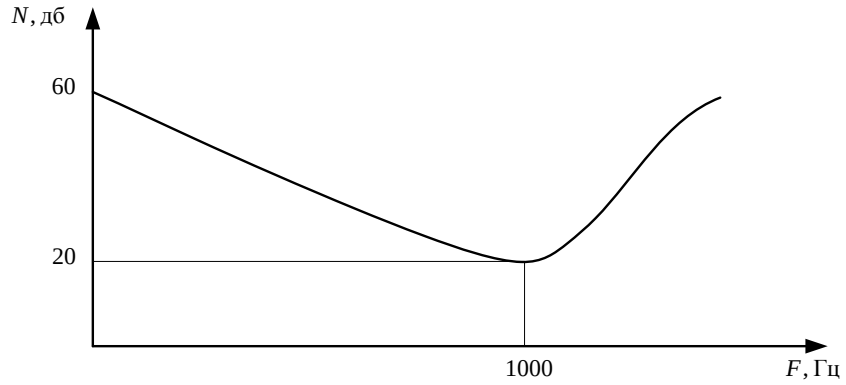


Рис.2.4. Залежність гучності від частоти

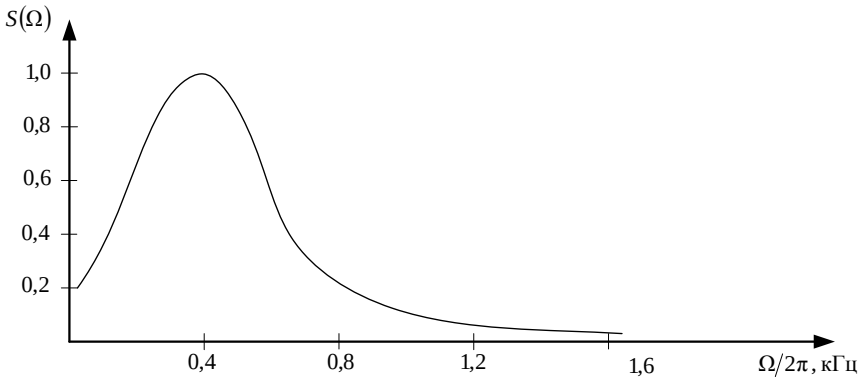


Рис.2.5. Спектр української мови

Досить часто в літературі доводиться зустрічатися з такими термінами, як пікфактор та рівень спектра звука. Під пікфактором мови (Пр) розуміють відношення пікового тиску до середнього ефективного: $\text{Пр} = 20\lg\frac{P_{\text{пік}}}{P}$.

Рівень спектра звуку (B) є тим же рівнем інтенсивності звуку, приведеним до 1 Гц:

$$B = 10\lg\frac{I}{I_0\Delta f_E},$$

де f_E – значення еквівалентної смуги частот, в якій вимірювали рівень інтенсивності.

Для пояснення процесу слухового сприйняття мови користуються так званою резонансною теорією слуху. Відповідно до цієї теорії модель вуха уявляють у вигляді набору резонаторів, які настроєні на різні частоти та мають смугу пропускання, що звуться критичними смугами слуху для тієї чи іншої частоти. Вухо здатне інтегрувати частотні складові звукового спектра, які знаходяться у межах критичної смуги. Критична смуга слуху залежить від частоти (рис. 2.6).

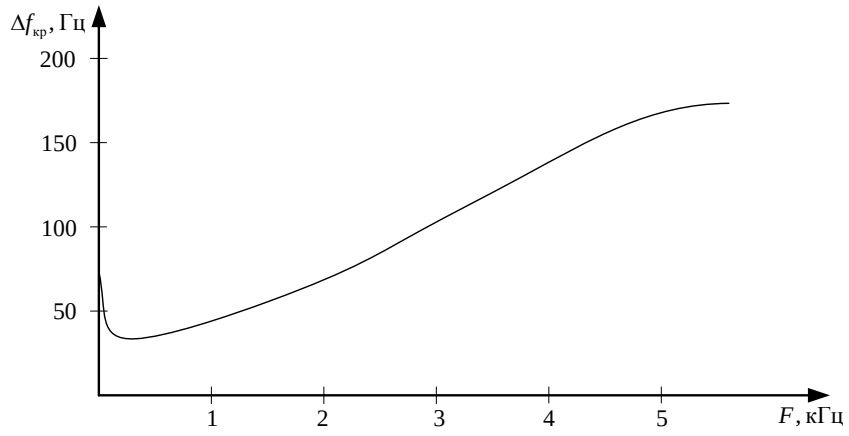


Рис 2.6. Залежність критичної смуги слуху від частоти

Існує деякий мінімальний рівень звуку, який сприймається вухом. Він зветься порогом чутливості, а також є функцією частоти. Так, звуки на різних частотах вухо людини починає чути з неоднаковим рівнем.

На рис.2.7 показано залежність порога чутливості від частоти. З рис. 2.7 видно, що звуки з частотою 200 Гц починають бути чутними при рівні інтенсивності 30 дБ. В той же час для звуків на частоті 3000 Гц досить навіть 0 дБ, щоб бути почутими вухом людини.

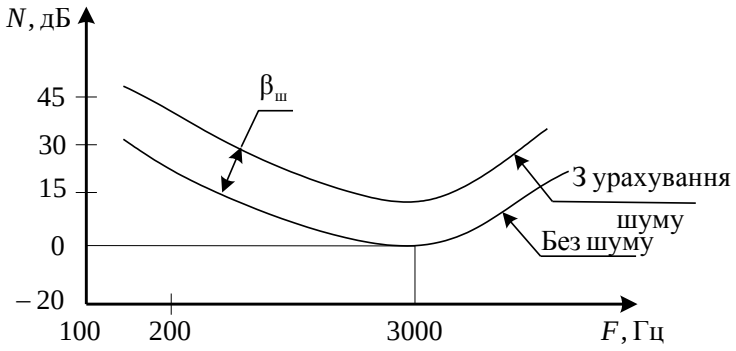


Рис. 2.7. Залежність порога чутливості від частоти

Таким чином, вухо людини, немовби, компенсує недоліки розподілу енергії в спектрі мови. Тобто звуки мови, які мають багато енергії, починають бути чутними при високому рівні інтенсивності (звуки в смузі 200...600 Гц), а звуки з малою енергією – відповідно чутні з низьким рівнем (звуки в смузі від 1000 до 4000 Гц).

Зрозуміло, що поріг чутності в тиші відрізняється від порога під час дії шуму на відповідний рівень інтенсивності шуму, який оцінюють як $\beta_ш = 10 \lg \frac{I_ш}{I_0}$.

Слід відзначити, що шум стає відчутним, коли його рівень перевищує 80 дБ. Рівень шуму в 90 дБ потребує вести розмову з напругою, а при рівні в 115 дБ розмова взагалі не можлива.

2.2.1. Теорія розбірливості мови

Якість зв'язку під час передачі не перетворених мовних повідомлень оцінюється розбірливістю мови, названою також артикуляцією. Під артикуляцією розуміють відсоток правильно прийнятих елементів мови із загальної кількості елементів, переданих у даному повідомленні. Як передані елементи мови можуть бути фрази, слова, склади, звуки, форманти. Тоді якість зв’язку оцінюють артикуляцією фраз *I*, слів *W*, складів *S*, звуків *D*, формант *A*.

Сприйняття звуку залежить від рівнів формант над порогом чутності. Під час передачі окремого звуку приймання його достовірний тільки у тому випадку, коли усі форманти даного звуку, істотні для розуміння, сприймаються слухачем, у разі передачі ряду послідовних звуків мови ця вимога не є обов’язковою. У цьому випадку звук з неповно прийнятими формантами може бути прийнятий вірно, якщо достатня кількість інших звуків була прийнята правильно. Звичайно, розбірливість звуків *D* певним чином пов’язують з розбірливістю формант *A*.

Індивідуальні розрізнення частот формант та їхнє взаємне розташування у різних людей виявляється значним, тому у разі аналізу прийнятого повідомлення мозок слухача виконує величезну роботу щодо порівняння прийнятого сигналу із “еталонами” комбінацій даного звуку, що зберігаються в “чарунках пам’яті”, причому відповідність прийнятого сигналу “еталона” встановлюється не тільки з урахуванням відхилення сигналу від “еталона”, але й імовірності появи даного звуку за попередніми звуками.

Кількісне значення артикуляції визначається експериментальним шляхом. При цьому звичайно користуються артикуляційними таблицями, що містять набір тих чи інших елементів мови. У більшості випадків артикуляційні таблиці складають зі складів чи звукових сполучень, що не мають суттєвого значення.

Приклад кількісної оцінки якості зв’язку за допомогою артикуляції проілюструємо за допомогою табл. 2.1, що містить значення розбірливості елементів мови для оцінки якості зв’язку.

З табл. 2.1 видно, що абсолютні зміни форматної розбірливості за своїм значенням значно більші, ніж для звукової, складової і словесної розбірливості. Це означає, що точність вимірів за формантною розбірливістю буде значно вище, ніж за іншими видами розбірливості.

Під час оцінки однієї з основних експлуатаційних характеристик трактів передачі мови – пропускної здатності (чи часу, необхідного для передачі повідомлення) необхідно враховувати, що чим нижче якість переданої мови, тим більше часу потрібно для її повного розуміння.

Таблиця 2.1

Вид розбірливості, %	Якість зв'язку				
	зрив зв'язку	мінімально допустима	задовільна	добра	**відмінна**
A	36	42	46	52	60
D	60	70	77	85	91
S	20	32	45	60	75
W	65	73	80	90	95
I	–	60	70	80	90

Дослідження показали, що значення розбірливості формант A обернено пропорційно значенню часу T, необхідного для повного розуміння змісту мови $\left(A = \frac{K}{T}\right)$. Отже, розбірливість формант – це відносне значення гранично можливої швидкості передачі, тобто формантна розбірливість є найбільш показовим видом розбірливості.

Значення формантної розбірливості за умови практики з достатнім ступенем точності визначається добутком ширини частотного діапазону (у герцах) і середнього значення ефективного динамічного діапазону мови (у децибелах)

$$A = K_1 D_{\text{ср}} F ,$$

де $D_{\text{ср}}$ – середнє значення ефективного динамічного діапазону мови по входу тракту; F – ширина частотного діапазону мови, що пропускається трактом $\frac{1}{K_1} = N_0 F_0 = 1{,}05 \cdot 10^5$ дБ·Гц, тут $F_0 = 3500$ Гц і $N_0 = 30$ дБ.

У роботі [8] зроблено цікавий висновок про те, що кількість прийнятої інформації прямо пропорційна добутку частоти, яка пропускається трактом F, середнього динамічного діапазону D і часу передачі T:

$$I \approx K_1 D_{\text{ср}} FT ,$$

тобто пропорційна добутку формантної розбірливості на час передачі.

Теорія розбірливості мови заснована на статистичному процесі сприйняття формант за умов дії шуму. За цих умов має місце маскування мови шумами, тому велике значення в теорії розбірливості мови має визначення залежності ефекту маскування від рівнів і спектрів шумів.

Для широкополосних рівномірних флуктуаційних шумів низьких і середніх рівнів поріг чутності в критичній смузі слуху $\Delta f_{кр}$ визначається виразом

$$N_{ш} = \beta + K_{с} + 10\lg\left[1 + 10^{-0,1}\left(\beta + K_{с} - N_{0}\right)\right],$$

де β – рівень спектра шуму; $K_{с}$ – логарифмічна ширина критичної смуги слуху, $K_{с} = 10\lg \Delta f_{кр}$; N_{0} – рівень порога чутності в тиші.

$$\text{при} \begin{array}{l} \beta + K_{с} - N_{0} > 10, \\ N_{ш} = \beta + K_{с}. \end{array} \qquad (2.1)$$

Із виразу (2.1) випливає, що в кожній ділянці частотного діапазону флуктуаційних шумів рівень порога чутності визначається рівнем спектра шуму і шириною критичної смуги слуху і як би не залежить від маскуючої дії складових на інших ділянках. Насправді маскуючий ефект на кожній такій ділянці визначається сумарною дією всіх складових шуму, причому частка кожної з них тим менше, чим далі він знаходиться від розглянутої області частот. При цьому маскуюча дія більш помітно позначається на частотах, що лежать вище частоти маскуючого тону чи шуму.

Вираз (2.1) показує, що тон може бути почутий, якщо його рівень інтенсивності дорівнює рівню шуму в критичній смузі. Для рівномірного шуму з діапазоном частот 100...4000 Гц це означає, що тон може бути почутий, якщо його рівень на $10\lg 3900 / \Delta f_{кр}$ нижче рівня шуму. Для частоти 1000 Гц $\Delta f_{кр} = 65$Гц, отже, загальний рівень шуму може бути на 18 дБ вище рівня тону. Це пояснюється високою вибірковістю слуху.

2.2.2. Розбірливість мови при радіозв'язку

Розбірливість мови в системі радіозв'язку є функцією багатьох перемінних, з яких найбільше значення мають:

- відношення сигнал/завада на вході приймача;
- перетворення цього відношення в приймальному пристрої;
- спектральне відношення сигнал/завада на вході демодулятора;
- низькочастотна характеристика радіолінії;
- наявність зовнішніх завад (наприклад, акустичного шуму).

Під завадостійкістю радіолінії розуміють таку сукупність її властивостей, яка забезпечує визначену розбірливість мови при заданому відношенні сигнал/завада на вході приймача для даного типу завад і заданому акустичному шумі на приймальному і передавальному кінцях.

Як критерій розбірливості зручніше використовувати величину *A*, оскільки ймовірність правильного приймання елементів повідомлення виражається залежністю

$R_{\text{пр}} = A/100$ і відповідно $R_{\text{вик}} = 1 - A/100$; $R_{\text{пр}} = \varphi\left(\frac{P_{\text{с}}}{P_{\text{п}}}\right)_{\text{вх}}$. Чи залежність $R_{\text{пр}} = \psi\left(\frac{P_{\text{с}}}{P_{\text{п}}}\right)_{\text{вх}}$ буде цілком характеризувати роботу радіолінії (тут $P_{\text{с}}$ – потужність сигналу; $P_{\text{п}}$ – потужність завади).

Оскільки розбірливість у системах радіозв'язку в основному залежить від спектрального відношення $\frac{P_{\text{с}}}{P_{\text{п}}}$, розглянемо, як це відношення змінюється під час проходження через різні елементи системи зв'язку.

Наявність істотно нелінійних елементів зумовлює серйозні зміни спектрального відношення сигнал/завада в різних елементах лінії зв'язку. Перетворювач частоти не змінює відношення спектральних складових сигналу і завади в радіоприймальному пристрої. Тут має місце зміна спектрів сигналу і завади – придушення модуляції шумом і збільшення шуму у разі впливу несучої.

Рівні спектра сигналу під час детектування збільшуються, оскільки відбувається додавання симетричних бічних, тому

$$N_1 = N_2 + 6\,\text{дБ},$$

де N_1 – рівень сигналу після детектора; N_2 – рівень сигналу до детектора.

Рівні спектра завади зростають менше, оскільки відбувається додавання компонентів з випадковими фазами й амплітудами. Можна вважати, що це зростання відбувається на 3 дБ. Однак одночасно (в силу специфіки проходження завади через детектор) відбувається зменшення рівнів спектра завади, тому

$$N_3 = N_4 + (3 - X)\,\text{дБ},$$

де N_3 – рівень завади після детектора; N_4 – рівень завади до детектора; X – розрахунковий рівень.

Для розрахунків розбірливості мови звичайно X приймають рівним 6 дБ. Таким чином, зміна спектрального відношення сигнал/завада виявляється в процесі демодуляції.

У разі постійного рівня шуму зміна смуги підсилювача проміжної частоти (ППЧ) не викликає зростання рівня спектра шуму N_4 і не збільшує придушення частоти модуляції. Разом з тим артикуляційні виміри показують зменшення розбірливості передачі, якщо при сталості відношення потужності несучої до потужності завади в смузі частот приймача смуга ППЧ звужується. Це свідчить про те, що при передачі мови в лінії з амплітудною модуляцією (АМ) заважають лише компоненти шуму, розташовані в області складових сигналу, що визначають розбірливість мови.

Розширення смуги пропускання приймача по проміжній частоті не буде впливати на розбірливість мови. А розширення смуги пропускання підсилювача низької частоти (ПНЧ)

не впливає на розбірливість мови при помірних рівнях акустичного шуму. У разі великих рівнів шуму розширення цієї смуги може викликати перевантаження вуха і зниження розбірливості мови через зростання рівня інтенсивності шуму.

Заважаюча дія високих рівнів шуму може виявлятися не тільки в маскуванні складових мови, але й у змушеному зниженні рівня її відтворення. Це зниження може відбуватися за рахунок таких складових спектра шуму, що безпосередньо маскуючої дії не виконують і тому, здавалося б, нешкідливе. Саме так позначаються шкідливі впливи потужних низькочастотних компонентів шуму з частотою до 250 Гц. Не впливаючи на розбірливість мови по прямому маскуванню, вони в значній мірі визначають загальний рівень інтенсивності шуму і тим самим можуть знижувати можливий рівень відтворення мови.

Для одержання найбільшої завадостійкості і розбірливості мови в системі радіозв'язку низькочастотні характеристики модулятора і каналу в цілому повинні вибиратися таким чином, щоб на граничній дальності зв'язку забезпечувалося найвигідніше формантне перевищення. Це перевищення буде здійснюватися у разі максимальної модуляції передавача, якщо максимальній модулюючій напрузі відповідає найвигідніший для розбірливості розподіл частотних складових мови під час впливу даних завад. Такому найвигіднішому розподілу складових мови відповідають цілком визначені викривлення частотного і динамічного діапазонів мови, тобто маємо визначену структуру мови, що є оптимальною для зв'язку у разі наявності завад заданого виду. Одержання такої структури мови можливо тільки при використанні модулятора з оптимальною низькочастотною характеристикою. Ця характеристика буде різною для різних співвідношень сигналу завади на вході приймача. Дослідження показали, що оптимальна характеристика модулятора повинна мати підйом порядку 6 дб/окт, починаючи з частоти 500...600 Гц. Якщо говорити про оптимальну смугу пропускання модулятора, то необхідно врахувати ряд суперечливих факторів. Так, збільшення смуги пропускання модулятора дає підвищення розбірливості мови в процесі роботи за умов сильного шуму. Однак це зумовлює зменшення завадостійкості. Тому розширення смуги модулятора не слід робити більшим, ніж це потрібно для забезпечення заданої максимальної розбірливості, оскільки при цьому зменшуються формантні перевищення для даного значення відношення $P_{\text{с}}/P_{\text{п}}$ і дальність зв'язку падає.

Звичайно в службових системах радіозв'язку смуга пропускання модулятора не перевищує 300...3500 Гц.

У роботі [8] показано, що вибір оптимальних низькочастотних характеристик каналу зв'язку і введення невеликого амплітудного обмеження дозволяє збільшувати дальність зв'язку на 30...40 %.

Це рівноцінно майже шестиразовому виграшу в потужності.

2.3. Компресія мовних сигналів

2.3.1. Елементи теорії інформації в застосуванні до мовного сигналу

Кількісною мірою мовного повідомлення є кількість відомостей, що містяться в ньому. Так, наприклад, у телеграфному повідомленні кількість відомостей може бути легко визначена з кількості відомостей, що містяться в кожному знакові. Під час аналізу мовних повідомлень на перший погляд здається, що мову, як неперервний процес, можна представити тільки нескінченно великим числом елементів. Однак із теореми Котельникова відомо, що сигнал, у який перетворюється будь-яке неперервне повідомлення, можна представити з наперед заданою точністю кінцевим числом елементів, тобто передаються тільки ординати безупинного сигналу, розташовані на інтервалах $1/2F_{в}c$, де $F_{в}$ – верхня частота діапазону.

У системах авіаційного радіозв'язку – це звичайно сигнали обмеженої тривалості T і смугою спектра F. Процес передачі повідомлення в цьому випадку цілком визначається числом параметрів, рівним [8]

$$n = 2FT .$$

Цими параметрами можуть бути або миттєві значення сигналу, розташовані на інтервалах $1/2Fc$, або спектральні коефіцієнти розкладання в ряд Фур'є і т. ін.

Отже, безупинний сигнал кінцевої тривалості і з обмеженим спектром точно описується кінцевим числом значень цього процесу.

Крім квантування в часі, може бути квантування за рівнем (рівнями) миттєвих значень сигналу, при якому відбувається викривлення форми сигналу, однак ці викривлення не перевищують значень викривлень, викликаних завадою. Можна вважати, що ніякого викривлення сигналу під час квантування за рівнем не відбувається, а лише з'являється завада зі ступінчатою зміною свого рівня.

Під час розгляду процесу квантування за рівнем необхідно запам'ятати, що поняття рівня миттєвого значення сигналу не слід змішувати з поняттям рівня потужності сигналу, що часто скорочено називають також рівнем сигналу.

Таким чином, сигнал можна замінити послідовністю імпульсів, розташованих на дискретних інтервалах і дискретних значеннях рівнів. У будь-якому вигляді мовного повідомлення (звук, склад, слово і т. ін.) кількість відомостей буде тим більше, чим більше загальне число знаків, з яких даний знак обраний. Якщо всіх можливих знаків *m*, а число

знаків у повідомленні n, то число можливих сполучень буде $N = m^n$, звідси число знаків у повідомленні

$$n = \frac{\log_2 N}{\log_2 m}$$

і максимальне число відомостей (інформації) пропорційне числу знаків у повідомленні:

$$I = \log_2 N = n \log_2 m .$$

Максимальна кількість відомостей, що приходяться на один знак повідомлення, тобто змістовність повідомлення, оцінюють у бінарних одиницях (біт):

$$I = \log_2 m .$$

Розглянемо взаємозв'язок між основними параметрами сигналу і кількістю відомостей, що містяться в ньому. Як відомо, сигнал визначається тривалістю, частотним і динамічним діапазонами. Нижня границя динамічного діапазону і точність його передачі визначаються рівнем завад. Звичайно вважають, що динамічний діапазон сигналу характеризується відношенням середніх потужностей сигналу $P_{\text{с}}$ і завади $P_{\text{п}}$ чи різницею їхніх рівнів:

$$D = \log \frac{P_{\text{с}}}{P_{\text{п}}} = \log P_{\text{с}} - \log P_{\text{п}} . \qquad (2.2)$$

Добуток трьох вимірів сигналу називають обсягом сигналу і записують у такий спосіб:

$$V = FTD$$

чи з урахуванням виразу (2.2)

$$V = FT \log \frac{P_{\text{с}}}{P_{\text{п}}} . \qquad (2.3)$$

Вираз для кількості відомостей, вважаючи, що кількість знаків у неперервному сигналі $n = 2FT$ і $m^2 = a\frac{P_{\text{с}}}{P_{\text{п}}}$, запишемо в такий спосіб:

$$I = FT \log a \frac{P_{\text{с}}}{P_{\text{п}}} , \qquad (2.4)$$

де a визначається кодом сигналу.

Таким чином, порівнюючи вирази (2.3) і (2.4), знаходимо, що кількість відомостей і обсяг сигналу розрізняються тільки на постійну величину $\log a$. Якщо врахувати, що кількість відомостей у заданому повідомленні – величина незмінна, то, змінюючи основу коду m, можна відповідно змінювати число елементів сигналу n. Це означає, що, наприклад, змінюючи число переданих рівнів, можна відповідно змінювати ширину частотного

діапазону $\left(n = \frac{T}{\Delta t} = 2FT \right)$. Таким чином, шляхом кодування можна змінювати кожний з трьох вимірів сигналу за рахунок іншого (інших). У цьому випадку обсяг сигналу також залишається незмінним.

В процесі передачі інформації з каналу зв'язку в реальному масштабі часу лише час повідомлення *T* залишається незмінним, смуга ж частот *F* і відношення $\frac{P_{\text{с}}}{P_{\text{п}}}$ зменшуються. Таким чином, обсяг прийнятого сигналу завжди менше обсягу переданого. Для більш повного використання ліній зв'язку та їхнього спрощення обсяг переданого сигналу бажано зменшувати, однак це часто суперечить вимогам підвищення завадостійкості передачі. У таких випадках необхідно шукати компромісне рішення, обумовлене призначенням лінії зв'язку. При цьому необхідно мати на увазі, що відношення $\frac{P_{\text{с}}}{P_{\text{п}}}$ у виразі (2.3) є інтегральним, і йому відповідає нескінченність комбінацій спектральних відношень $\frac{P_{\text{с}}}{P_{\text{п}}}$ у кожній точці площини *TF*, і тільки цілком визначені сполучення відношень дають найбільшу завадостійкість передачі при даному відношенні $\frac{P_{\text{с}}}{P_{\text{п}}}$. Отже, при передачі мови має значення не тільки обсяг сигналу, але і його конфігурація. Тому перетворення обсягу сигналу, вироблене для підвищення ефективності роботи лінії зв'язку, може бути здійснено всілякими способами.

Дослідження показали, що обсяг інформації, перенесеної мовним сигналом, виявляється майже на порядок менше обсягу мовного сигналу. Тому зменшення обсягу сигналу не призводить до скорочення інформації, перенесеної цим сигналом. Зменшення обсягу мовного сигналу чи його стиснення (компресія) досягається за допомогою відповідних перетворень мовного сигналу. Розрізняють методи безпосередньої і параметричної компресій (компресія з функціональним перетворенням мови). Класифікація методів компресії мови показана на рис.2.8.

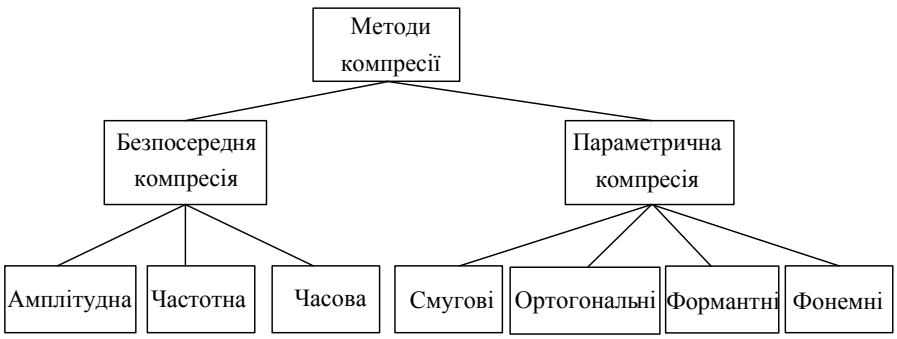


Рис. 2.8. Класифікація методів компресії мови

2.3.2. Методи безпосередньої компресії

Компресією мовних сигналів називається зменшення обсягу сигналів за рахунок стиснення одного чи декількох параметрів сигналу (динамічний діапазон, спектр частот, тривалість). Ці методи відрізняються тим, що виробляються тільки деформації обсягу сигналу, а мікроструктура сигналу цілком не знищується. Під час деформації об'єму сигнал частково викривляється, однак ці викривлення відіграють роль завад. Тут сигнал у відповідному вимірі "деформується", тобто стискається на передавальному кінці з відповідним розширенням його на приймальному кінці.

Отже, після обмеження сигналу по динамічному, частотному діапазону чи в часі відновити сигнал цілком на приймальному кінці не вдається.

Розгляд методів безпосередньої компресії почнемо з амплітудної компресії. У динамічному діапазоні сигналу міститься переважно інформація про якість звучання й у значно меншому ступені – інформація про розбірливість звуків, тобто скомпресований за рівнем мовний сигнал має розбірливість, що мало відрізняється від вихідного сигналу. Таким чином, компресія дозволяє підвищувати завадостійкість передачі.

Стиснення динамічного діапазону мови виробляється або методом автоматичного регулювання фонетичного рівня мови, або миттєвою компресією сигналу. При першому способі стиснення рівні звуків мови так чи інакше зближаються один з одним. У результаті піковий і мінімальний рівні скомпресованої мови також зближаються. Перехідні процеси, що залежать від сталої часу компресуючого пристрою, дуже спотворюють деякі звуки мови (б, п, д, т). В цілому динамічне компаундування мови, крім корисного ефекту, має недолік – поява викривлень через наявність перехідних процесів. Корисна дія компандування виявляється в тому, що при заданій піковій потужності передавача, незважаючи на викривлення, розбірливість мови підвищується навіть при наявності завад. У цьому випадку максимальний рівень мови на виході компресора буде таким же, як і на вході, а більш низькі рівні будуть піднятими.

Внаслідок "підтягування" слабких складових мови збільшується її розбірливість на тлі завад. Крім того, стиснення динамічного діапазону при заданій піковій потужності генератора забезпечує краще використання вихідних каскадів. Більш ефективним є спосіб стиснення динамічного діапазону шляхом миттєвої компресії (амплітудного обмеження). Цей спосіб є без інерційним. Розрізняють обмеження по максимуму (рис.2.9, *а*, *в*) і по мінімуму (рис.2.9, *б*, *г*).

Під ступенем обмеження зверху розуміють величину $\gamma_{\text{В}} = 20\lg\dfrac{U_{\max}}{U_{\text{обм}}}$, а при обмеженні знизу – $\gamma_{\text{Н}} = 20\lg\dfrac{U_{\max}}{U_{\max} - U_{\text{обм}}}$, де $U_{\max}$ – максимальне значення напруги на вході обмежувача; $U_{\text{обм}}$ – напруга початку обмеження.

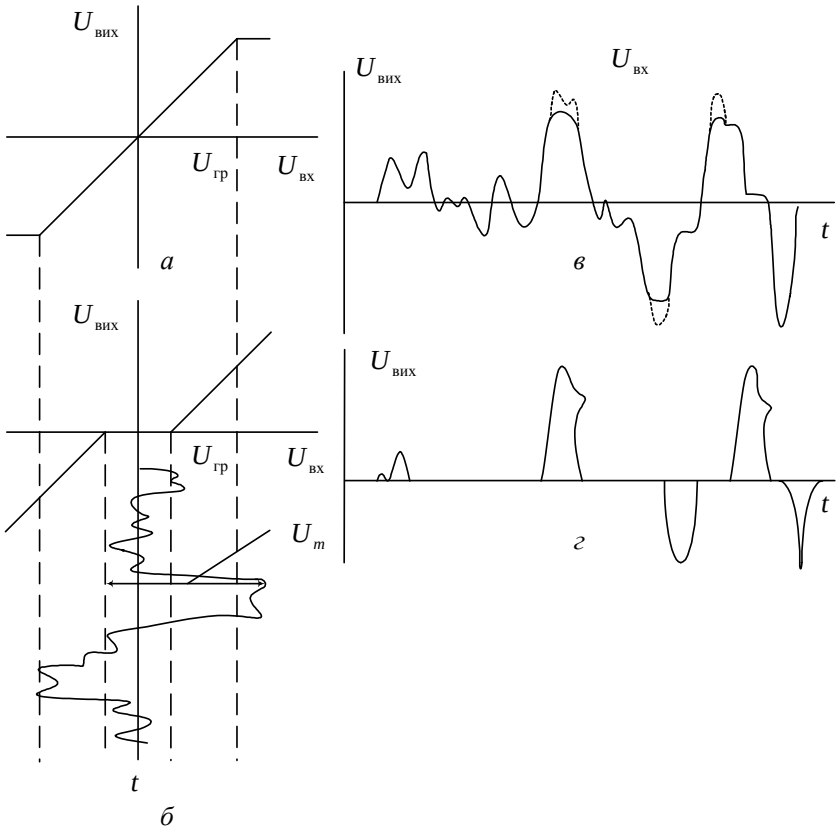


Рис. 2.9. Епюри напруг, що пояснюють принцип обмеження по максимуму і мінімуму

Вплив обмеження знизу і зверху на розбірливість мови різний (рис. 2.10). Незначне обмеження знизу викликає істотне зниження розбірливості мови, а навіть при сильному обмеженні зверху розбірливість мови неістотно падає. Встановлено, що висока розбірливість мови зберігається навіть при граничному обмеженні, що називається кліпуванням. Кліпована мова має вигляд прямокутних імпульсів різної тривалості (рис. 2.11). При цьому єдиною інформацією про первісну мову є послідовність нульових переходів. Виходячи з високої розбірливості процесу кліпування, випливає, що ті чи інші властивості розташування нулів (рис. 2.11) містять велику кількість інформації про мовне повідомлення.

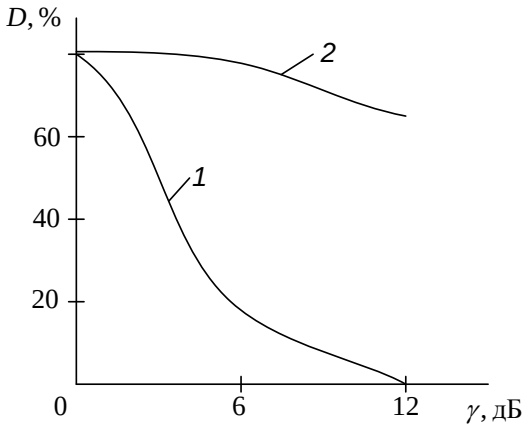


Рис. 2.10. Вплив на розбірливість обмеження зверху (*2*), і знизу (*1*)

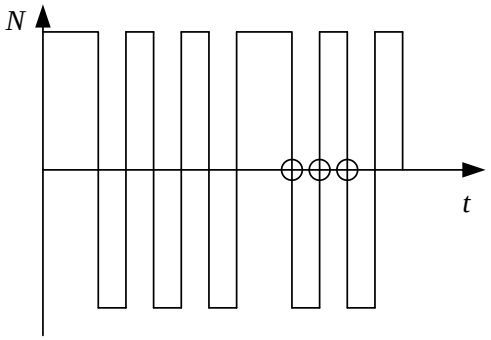


Рис. 2.11. Осцилограма кліпованої мови

Ще краща розбірливість, якщо мову попередньо диференціюють, а потім обмежують похідну мовного процесу. У цьому випадку зберігається положення не нульових, а екстремальних значень мовного повідомлення. Більш висока розбірливість мови для цього випадку пояснюється тим, що число екстремальних значень у мовному повідомленні більше числа нульових значень. Експериментально встановлено, що для чоловічих голосів нульові значення випливають з частотою 2780 Гц, а екстремальні – з частотою 4700 Гц. Таким чином, при збереженні положень екстремальних значень за допомогою диференціювання зберігається і передається в лінію зв'язку більш повна інформація про структуру сигналу.

Мовний сигнал у разі дотримання деяких умов може бути записаний як

$$F(t) = U_F(t)\cos\varphi(t).$$

При цьому функції $UF(t)$ і $\varphi(t)$ визначені у такий спосіб:

$$U_F(t) = \sqrt{F^2(t) + V^2(t)}\ ;\ \varphi(t) = \operatorname{arctg}\frac{V(t)}{F(t)},$$

де вихідна функція $F(t)$ і сполучена функція $V(t)$ однозначно пов'язані між собою інтегральними перетвореннями Гільберта:

$$V(t) = -\frac{1}{\pi}\int_{-\infty}^{+\infty}\frac{F(\tau)}{\tau - t}d\tau\,;\; F(t) = \frac{1}{\pi}\int_{-\infty}^{+\infty}\frac{V(\tau)}{\tau - t}d\tau\,.$$

Визначені таким способом функції $F(t)$ і $V(t)$ являють собою на комплексній площині функцію $F(t) + jV(t) = U_F(t)e^{j\varphi(t)}$, що називається аналітичною формою сигналу, утвореного з функції $F(t)$.

Сигнал $F(t)$ є дійсною частиною аналітичного виразу $F(t) = R_e U_F(t)e^{j\varphi(t)}$.

Вхідні у виразі (2.7) функції $U_F(t)$ і $\varphi(t)$ являють собою огинаючу і фазу сигналу $F(t)$ і містять відповідно амплітудну і частотну інформації. Очевидно, що похідна миттєвої фази $\omega(t) = \frac{d\varphi(t)}{dt}$ є миттєва частота сигналу $F(t)$.

Кліпування мови зводиться до усунення амплітудної інформації і до виділення та передачі частотної інформації, що міститься у функції $\cos\varphi(t)$, тобто в передачі мови постійного рівня. Виділення частотної інформації не можна здійснювати шляхом безмежного стискання, тому що спектри $U_F(t)$ і $\cos\varphi(t)$ перекриваються, а ширина спектра $F(t)$ перевершує октаву. У такому випадку частина гармонік, що виникли в результаті сильного обмеження, потрапить у вхідний діапазон частот і буде засмічувати обмежений сигнал на виході. Один зі способів усунення зазначеного недоліку полягає в зменшенні продуктів нелінійного викривлення шляхом попередньої корекції частотної характеристики мови до обмеження.

При стисненні динамічного діапазону сигналу найбільш обмежуються низькочастотні складові спектра, що мають найбільшу частку енергії мови, в результаті чого утворюються інтенсивні гармоніки, що не виходять за межі спектра мови, і тому спотворюють її. Крім того, в обмежувачі має місце безпосереднє придушення високочастотних складових низькочастотними. Якщо перед обмежувачем підняти високочастотні складові мови, то воно буде більш рівномірним, і зазначені викривлення зменшаться. Таке піднімання частотної характеристики може бути отримано під час проходження мовного сигналу через ланку, що диференціює. Це також є причиною підвищення розбірливості попередньо диференційованої обмеженої мови. Ще більш ефективним способом зменшення продуктів нелінійних викривлень є перенесення обмеження в область високих частот. Так, якщо

$$F(t) = U_F(t)\cos[\omega t + \varphi(t)],$$

то частоту ω можна вибрати настільки великою, що спектри функцій $U_F(t)$ і $\cos[\omega t + \varphi(t)]$ не будуть перекриватися, тобто $U_F(t)$ порівняно з $\cos[\omega t + \varphi(t)]$ буде змінюватися повільно. Крім того, можна домогтися, щоб ширина спектра сигналу, зміщеного на частоту ω, була меншою порівняно зі значенням $\frac{\omega}{2\pi}$, тобто вже октави.

Таким чином, гармоніки, що виникають при обмеженнях, виявляються поза межами діапазону частот функції $F(t)$ і тому можуть бути відфільтровані на виході обмежувача.

У результаті замість сигналу прямокутної форми процес на виході фільтра буде мати вигляд частотно-модульованого коливання.

Отже, оптимальний ступінь обмеження залежить від виду модуляції, від заходів, прийнятих для боротьби з нелінійними викривленнями, а також від умов, за яких здійснюється передача мовних повідомлень. Так, під час передачі з тиші оптимальним є обмеження на 18...24 дБ щодо пікового рівня мови. Таке обмеження прийнятне доти, поки відношення шум/сигнал менше одиниці. У разі більш інтенсивних завад розбірливість обмеженого сигналу різко знижується. Розбірливість необмеженого сигналу за таких умов знижується менш різко, однак вона буде також незадовільною. У разі ступеня обмеження 40 дБ розбірливість обмеженого сигналу при будь-якому рівні завад буде нижче розбірливості необмеженого сигналу.

За умов роботи з високим рівнем шуму $(\beta_{ш} = 110 \ldots 120 \text{ дБ})$ за рахунок мимовільного збільшення рівня мови оператором на 6...8 дБ ступінь обмеження можна вибирати в межах 18...24 дБ. Слід зазначити, що передача обмеженої мови пов’язана з необхідністю великого підсилення в низькочастотному тракті передавального пристрою. Це призводить до відносного зростання шумів у паузах, що погіршує якість звучання, і є істотним недоліком систем зв’язку, що використовують граничну компресію динамічного діапазону.

Одним зі способів зменшення шумів у паузах є запирання мовного тракту за допомогою обмежувача по мінімуму. Однак у цьому випадку погіршується якість відтворення внаслідок зникання коротких вибухових звуків, особливо на початку слів. Високу розбірливість і гарну якість звучання мови можна одержати шляхом передачі по рівнобіжних каналах кліпованого сигналу і його огинаючої з наступним перемножуванням на приймальному кінці. Порівнюючи між собою перший і другий способи стиснення динамічного діапазону, бачимо, що при другому способі відбувається більше звуження динамічного діапазону, однак нелінійні викривлення при цьому більш значні. Пристрої, що реалізують цей спосіб, дуже прості, тоді як пристрої автоматичного регулювання рівня досить складні, нестійкі в роботі і вносять помітні викривлення внаслідок процесів, що відбуваються в них.

Існує третій спосіб стиснення динамічного діапазону, що називається амплітудною селекцією. Сутність його полягає в передачі тільки максимальних і мінімальних значень мовного сигналу. Амплітудна селекція, маючи всі достоїнства кліпованої мови, має перевагу перед нею, тому що потребує смугу передачі в 2,5 рази вужчу.

Розглянемо основні методи частотної компресії. Спектр мови займає смугу частот 100...9000 Гц. Найпростіший і найбільш поширений спосіб частотної компресії полягає в

обмеженні спектра мовних сигналів, переданих по лінії зв'язку. Для передачі вибирається ділянка спектра, що є найбільш важливою для забезпечення необхідної якості зв'язку. Високочастотні складові мови понад 3...5 кГц несуттєво впливають на її розбірливість, тому з метою звуження спектра телефонного каналу і зниження внаслідок цього рівня завад ці складові доцільно обрізати. Це також доцільно і для низькочастотних складових нижче 250...300 Гц, що мають досить високу інтенсивність, однак мало впливають на розбірливість мови. Результати досліджень показали, що під час телефонної передачі мови, особливо за умов флуктуаційних шумів з рівномірною щільністю по частоті, обмеження частотного діапазону зверху частотою 3500 Гц і знизу частотою 300 Гц призводить лише до підвищення розбірливості мови.

Компресія спектра телефонного сигналу може бути отримана також за рахунок збільшення часу передачі. Якщо мову спочатку записати на плівку і зменшувати частоту обертання магнітофона проти нормальної в *n* разів, то у таке ж число разів звузиться спектр мови. На приймальній стороні для відновлення нормальної мови частота обертання повинна бути збільшена в *n* разів. Хоча розглянуті вище методи безпосередньої частотної компресії мають практичне значення, стиснення спектра мови в цьому випадку невелике і дуже далеке від гранично можливого стиснення.

Теоретична межа можливого стиснення спектра телефонного сигналу може бути встановлена на основі формули Шеннона [1]:

$$C = \frac{I}{T} = \frac{FT \log\left(1 + \frac{P_{\text{с}}}{P_{\text{п}}}\right)}{T} = F \log_2\left(1 + \frac{P_{\text{с}}}{P_{\text{п}}}\right),$$

де F – ширина спектра сигналу; $\frac{P_{\text{с}}}{P_{\text{п}}}$ – відношення потужності сигналу до потужності функціональної завади.

Нормальна розмова ведеться зі швидкістю $V = 10$ фонем/с. У разі ідеального кодування кількість двійкових одиниць, необхідних для передачі кожної букви, близька до ентропії повідомлення, тобто $H = 2$ біт/фонем. Тоді швидкість передачі при розмові $C = VH = 20$ біт/с. Якщо взяти відношення сигналу до завади в каналі зв'язку рівним $\frac{U_{\max}}{\sqrt{2\sigma}} = 3$, тобто $\frac{P_{\text{с}}}{P_{\text{п}}} = 9$, що необхідно для системи зв'язку з амплітудною модуляцією (АМ), то необхідна смуга частот визначиться з умови

$$F = \frac{VH}{\log_2(1+9)} = \frac{VH}{3{,}32}.$$

Якщо $H = 2$ біт/фонем, то $F \approx 6$ Гц, а при $H = 5$ біт/фонем $F \approx 15$ Гц. Системи телефонного радіозв'язку з безпосередньою компресією, які застосовуються на практиці, займають значно більшу смугу частот.

Існує також метод тимчасової компресії телефонного сигналу, що полягає в збереженні часу передачі і заснований на надмірності мови, обумовленої її тимчасовими характеристиками. Зазначена надмірність характеризується наявністю повторюваних ділянок у тимчасовій функції. Так, при розгляді спектрограм голосних звуків помітні повторювані ділянки, що випливають одна за одною з частотою основного тону. Наявність основного тону в мові може бути визначена за її осцилограмою (див. рис.2.2). Осцилограма являє собою серію згасаючих коливань. Інтервал між сусідніми коливальними процесами дорівнює періоду основного тону. Статистика показує, що основний тон чоловічих голосів знаходиться в межах від 70...120 до 150...160 Гц із середньою частотою 120 Гц, для жіночих голосів в межах від 180...220 до 300...330 Гц із середньою частотою 240 Гц.

Враховуючи, що більшість дзвінких звуків має тривалість 50...300 мс, процес коливань можна вважати до середини звуку цілком сталим і тому говорять про частоту тимчасової огинаючої процесу коливань, вимірюваної системами з невеликою сталою часу (не більше 1/50 с). При цьому розрізняють два основних аспекти основного тону: мелодію, що представляє собою зміну миттєвої частоти тону, та інтегральний розподіл миттєвої частоти тону. Можна сформулювати три основні особливості характеристик основного тону.

Першою особливістю є те, що основний тон голосу є майже періодичним процесом і, отже, має спектр, що складається з ряду груп складових. У кожній групі є складові, які розташовані на частотних інтервалах, близьких до інтервалів між гармоніками основного тону при тривалому його звучанні. Таке представлення про особливості основного тону не завжди правомірно, тому що тільки для деяких тривалих звуків можна говорити про встановлення процесу. У більшості ж випадків тривалість звучання основного тону невелика. Вважають, що якщо різниця в інтервалах не виходить за межі 10...15 %, то основний тон незмінний. Однак слух розрізняє таку зміну основного тону як характерну рису, за якою можна впізнати голос.

Другою особливістю основного тону є зміна в значних межах тривалості інтервалів під час вимови окремих фраз, а також наявність у багатьох людей різного основного тону для вимови тих чи інших фраз. Перше явище називається мелодією основного тону. Вона характерна, наприклад, для питальних і окличних речень. За цією особливістю можна впізнати голос людини, що говорить.

Третьою особливістю основного тону є швидка зміна його інтервалів, особливо при переходах від голосного до приголосного, і навпаки. Якщо ввести поняття швидкості зміни основного тону, то виявляється, що вона доходить до 6000 Гц/с.

Розглянуті вище характеристики основного тону допомагають краще зрозуміти процес тимчасової компресії мовного сигналу. На відміну від спектрограми голосних звуків багато приголосних звуків за своїми властивостями наближаються до шумів, а, отже, не мають періодичності. Однак і в цьому випадку деякі параметри коливання на невеликому відрізку часу залишаються постійними.

Для розпізнавання звуків необов'язково передавати їх протягом всього інтервалу часу мовного повідомлення. Щоб зрозуміти звук мови, потрібно інтервал часу близько 10 мс. Отже, скорочення часу передачі можливо шляхом усунення тимчасової надмірності. Дослідження показують, що можна скоротити половину чи навіть більше половини загальної тривалості передачі при збереженні досить високої розбірливості.

В роботі запропонований метод тимчасової компресії мови, синхронної з частотою основного тону. Тут із сигналу, що надходить, виділяється частота основного тону і замикає канал передачі сигналу в момент найбільш слабких коливань на час, рівний трьом періодам основного тону, після чого канал відкривається на один період основного тону і т. ін.

На приймальному кінці є лінія затримки з паралельними послідовними ланками, керована імпульсами основного тону. Сумарний сигнал від відповідних ланок лінії затримки представляє безупинний сигнал.

2.4. Статистичні характеристики мовних повідомлень

Дослідження статистичних характеристик мовного сигналу базується на математичному представленні акустичного процесу утворення мови, який, у свою чергу, базується на фізичних процесах утворення мови. Розглянемо дискретну модель утворення мови (рис 2.12).

В цій моделі можна виділити дві системи, модель збудження і модель випромінювання. Більшість звуків мови можна віднести або до вокалізованих (голосних), або до невокалізованих (приголосних). У випадку вокалізованих звуків джерело збудження повинно формувати квазіперіодичну послідовність імпульсів. У випадку невокалізованих – випадкові шумові коливання [2].

Структурна схема пристрою, який реалізує один із способів одержання такого сигналу, показана на рис.2.12. Вона складається з генератора імпульсної послідовності (ГІП) з періодом слідування імпульсів $T_{\text{і}}$, який дорівнює періоду основного тону $T_{\text{от}}$ мовного сигналу. З виходу ГІП сигнал надходить на лінійну інерційну систему імпульсна

характеристика $\upsilon(t)$ якої відповідає формі коливань в голосовій щілині. Коефіцієнт підсилення вокалізованого звуку $K_{\text{в}}$ визначає інтенсивність голосового збудження.

Для невокалізованих звуків модель збудження реалізується у вигляді генератора шуму (ГШ) з коефіцієнтом підсилення $K_{\text{нв}}$, який регулюється. Так, у дискретному часі замість ГШ може бути використано генератор випадкових чисел, який формує послідовність із рівномірним спектром та довільною функцією розподілу.

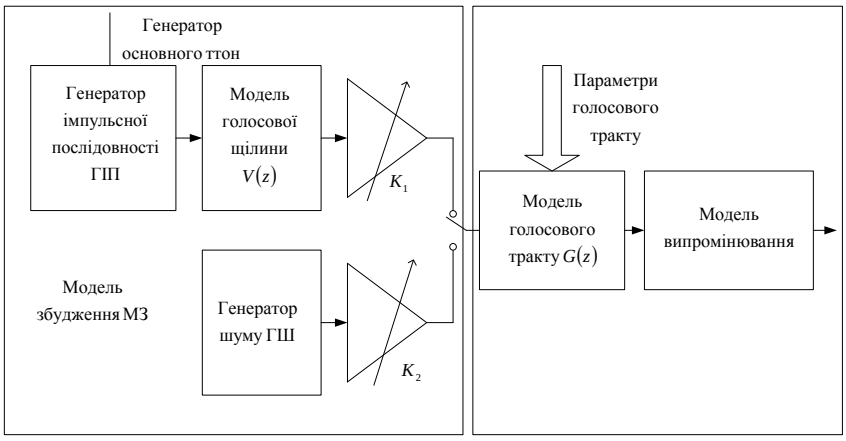


Рис.2.12. Дискретна модель утворення мови

Модель голосового тракту цілком характеризується передавальною функцією $G(z)$, полюси якої відповідають резонансам (формантам) мовного сигналу. Полюсна модель $G(z)$ дає у більшості випадків хороше зображення голосового тракту для більшості звуків мови. Для розширення можливостей описаних звуків необхідно використовувати не тільки резонанси, а й антирезонанси, тобто враховувати не тільки полюси, але й нулі функції $G(z)$, що в деяких випадках і робиться.

Передавальну функцію $G(z)$ можна реалізувати як аналоговими, так і цифровими пристроями.

Ефект випромінювання мови можна описати за допомогою передавальної функції $R(z)$. Звичайно, моделі голосового тракту об’єднують разом. При цьому результуючу передатну функцію процесу утворення мови записують у вигляді

$$H(z) = V(z)G(z)R(z).$$

Для управління такою моделлю повинна бути апріорна інформація про залежність відповідних параметрів (частоти основного тону, положення перемикача гучності та коефіцієнти передачі фільтрів) від часу.

Для вокалізованих звуків, які повільно змінюються у часі, ця модель виявляється найбільш точною. Для невокалізованих звуків, які швидко змінюються, розглянута модель утворення мови може не відповідати реальним фізичним процесам.

У будь-якому випадку припускається, що мовний процес, який є випадковим нестаціонарним процесом, повинен бути підданий короткочасному аналізу. Найчастіше вважають, що параметри моделі незмінні протягом 10...20 мс.

Під час синтезу та аналізу систем передачі мови використовують різні абстрактні моделі мовного процесу, що в якійсь мірі відповідають реальній дійсності. Найбільш поширена модель являє собою нестаціонарний гауссівський випадковий процес з дисперсією та спектральною щільністю, що повільно змінюються. У разі використання такої моделі можна синтезувати систему зв'язку з найкращими характеристиками. Але при цьому виходить досить складна система, яка сама настроюється, синтез її досить складний, тому що відсутні численні статистичні характеристики таких моделей мовного процесу.

Меншу точність має модель мовного сигналу, який являє собою нестаціонарний гауссівський процес з повільно змінюваною дисперсією та постійною усередненою спектральною щільністю, яка визначається експериментально з використанням усереднення за часом.

Разом з тим, для реальних мовних процесів на досить великих відрізках часу задовольняються умови стаціонарності, що дає можливість розглядати мовний сигнал як квазістаціонарний.

Для оцінки якості передачі мовного сигналу в цифрових системах передачі інформації широко використовуються різні апроксимації усередненої за часом щільності розподілу вірогідності розподілу мови (ЩВР) $\omega(\lambda)$.

Найбільш зручною вважається така модель апроксимації ЩВР:

$$\omega(\lambda) = \frac{0{,}5}{\sqrt{2\pi}\sigma_{\text{ПР}}}\exp[-\frac{\lambda^2}{2\sigma_{\text{С}}^2}] + \frac{0{,}5}{\sqrt{2\pi}\sigma_{\text{Г}}}\exp[-\frac{\lambda^2}{2\sigma_{\text{Г}}^2}],$$

де $\frac{\sigma_{\text{П}}}{\sigma_\lambda} = 0{,}1$; $\frac{\sigma_{\text{Г}}}{\sigma_{\text{к}}} = 1{,}4$.

Вважається, що вірогідності голосних $P_{\text{Г}}$ та приголосних $P_{\text{ПР}}$ звуків однакові та дорівнюють 0,5.

Поряд з ЩВР важливе прикладне значення для аналізу систем передачі мови мають спектральні $S_\lambda(f)$ та кореляційні $B_\lambda(\tau)$ характеристики.

Найбільш поширена модель мовного процесу, який пройшов попереднє обмеження спектра за допомогою фільтра нижніх частот з частотою зрізу $F_З$. Спектральна щільність потужності мовного процесу на виході такого фільтра визначається за співвідношенням:

$$S_\lambda(f) = \sigma_\lambda^2\alpha(1+M)[\frac{1}{\alpha^2+4\pi^2(f+f_0)^2} + \frac{1}{\alpha^2+4\pi^2(f-f_0)^2}];$$

$$M = 1 - \frac{1}{\pi}\text{arctg}(\frac{2\pi F_З - \omega_0}{\alpha}) - \frac{1}{\pi}\text{arctg}(\frac{2\pi F_{СР} + \omega_0}{\alpha}); \qquad (2.5)$$

$$\alpha = \frac{4\Delta f}{1+g^2};\ \omega_0 = \frac{4\Delta f_g}{1+g^2};\ g = \frac{2\pi f_0}{\alpha}. \qquad (2.6)$$

Для аналізу пристроїв перетворення мови, наприклад у вокодерах, використовують апроксимацію у вигляді

$$S_\lambda(f) = \sigma_\lambda^2 \sum_{i=1}^{n-1} S_i(\omega);\ S_i(\omega) = S_i(\tfrac{\omega_i - \omega_{i+1}}{2}) = S_i(\tfrac{\pi F_{\text{СР}}}{n}).$$

Взагалі мовні випадкові процеси не є суттєво гауссівськими випадковими процесами.

2.5. Параметрична компресія мовних сигналів

2.5.1. Загальні положення

Методи компресії телефонних сигналів з функціональним перетворенням мови (параметрична компресія) ґрунтуються на заміні мови її параметрами, відомості про які передаються в лінію зв'язку для відновлення повідомлення в приймальному пристрої. Найчастіше вибирають параметри, які повільно змінюються в часі, тому для передачі інформації про такі параметри треба використовувати смугу частот, вужчу ніж для передачі самої мови [8].

Пристрої для функціонального перетворення мови називають вокодерами (від англ. voice – голос та coder – кодувальник).

Робота вокодерів ґрунтується на моделюванні людської мови з урахуванням її характерних особливостей. Замість безпосереднього вимірювання амплітуди вокодер перетворює вхідний сигнал в деякий інший, схожий на первинний. При цьому характеристики мовного сигналу використовують для коригування параметрів прийнятої моделі мовного сигналу. Саме ці параметри і передаються приймачу, який за ними відновлює первинний мовний сигнал. По суті йдеться про синтез мови. У цьому випадку випромінювання спотворень відношення сигнал/шум не має сенсу для вокодерів, а тому необхідні інші суб'єктивні оцінки, такі як середня експертна оцінка, діагностичний римований текст та інші оцінки.

Вокодери можна розділити на два класи: мовноелементні та параметричні. У мовно елементних вокодерах під час передачі розпізнаються елементи мови (наприклад фонеми) і передаються тільки їх номери. На приймальному кінці ці елементи створюють за правилами мово утворення або беруть із пам'яті пристрою. Галузь застосування фонемних вокодерів – лінії командного зв'язку, мовне керування та інформаційно-довідкові служби. Практично в таких вокодерах здійснюється автоматичне розпізнавання слухових образів, а не визначення параметрів мови.

В параметричних вокодерах з мовного сигналу виділяють два типи параметрів:

- параметри, які характеризують огинаючу спектра мовного сигналу (фільтрову функцію);

- параметри, які характеризують джерело мовних коливань (генераторну функцію) – частота основного тону, її зміни в часі, моменти появи та зникнення основного тону, шумового сигналу.

За цими параметрами на приймальній стороні синтезують мову.

За принципом визначення параметрів фільтрової функції мови розрізняють вокодери:

- смугові канальні (channel);

- формантні;

- ортогональні;

- ліпредери (з лінійним передбаченням мови);

- гомоморфні.

У смугових вокодерах спектр мови ділиться на 7...20 смуг (каналів) аналоговими або цифровими смуговими фільтрами. Велике число каналів у вокодері дозволяє збільшити натуральність та розбірливість. З кожного смугового фільтра сигнал надходить на детектор та фільтр низьких частот з частотою зрізу F_3. Таким чином, сигнали на виході кожного каналу змінюються з частотою не більше F_3. Їх передача можлива в аналоговому та цифровому вигляді.

У формантних вокодерах огинаюча спектра мови зображується комбінацією формант (резонансних частот голосового тракту). Основні параметри формант – центральна частота, амплітуда та ширина смуги частот.

В ортогональних вокодерах огинаюча миттєвого спектра розкладається в ряд за вибраною системою ортогональних базисних функцій. Коефіцієнти цього розкладання передаються на приймальну сторону. Найбільше поширення отримали гармонічні вокодери, які використовують розкладання в ряд Фур'є.

Вокодери з лінійним передбаченням (LPC – Linear Prediction Coding) ґрунтуються на оригінальному математичному апараті.

Гомоформна обробка дозволяє розділити генераторну та фільтрову функції, які утворюють мовний сигнал.

Враховуючи складність одержання параметрів генераторної функції, широке застосування отримали напіввокодери (VE – Voice Excited Vocodec), в яких замість сигналів основного тону та тон-шум використовується смуга мовного сигналу. Смуга частот до 1000 Гц передається по каналу зв'язку в аналоговому або цифровому вигляді. Найбільш відомі напіввокодери VELP (Voice Excited Linear Prediction) та RELP (Residual Excited Linear Prediction).

Вокодери VELP використовують голосове збудження та коефіцієнти лінійного передбачення (КЛП). У вокодерах RELP по вихідному сигналу також обчислюють КЛП.

Якість мови вокодерів є функція від швидкості передачі, продуктивності та затримки обробки. Так, наприклад, низькошвидкісні вокодери звичайно мають більшу затримку та нижчу якість мови ніж високошвидкісні.

У зв'язку з тим, що вокодер використовує канал разом з іншими споживачами або Інтернет з іншими інформаційними потоками, максимальна швидкість повинна бути якомога меншою. Метою сучасних розробок є вокодери зі змінною швидкістю. При цьому використовують фіксовану швидкість для мови та низьку швидкість для фонових шумів. Це досягається за допомогою алгоритмів стискання пауз. У цьому випадку використовують детектор активності мови (VAD), який визначає, чи є вхідний сигнал мовою, чи фоновим шумом. Якщо сигнал вважається мовою, він кодується на номінальній фіксованій швидкості, а коли сигнал вважається шумом, він кодується на більш низькій швидкості.

На приймальній стороні відбувається генерація комфортного шуму. Спосіб генерації комфортного шуму повинен бути таким, щоб кодер та декодер залишалися синхронізованими, навіть якщо протягом деякого часу передача даних не здійснюється. Це дозволяє згладжувати переходи між сегментами активної та неактивної мов.

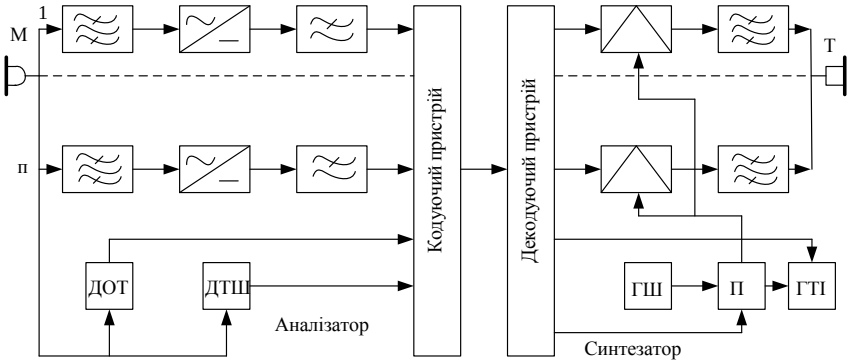
2.5.2 Смугові вокодери

Типова схема смугового вокодера показана на рис 2.13. Мовний сигнал із мікрофона надходить на гребінку смугових фільтрів (СФ) аналізатора. Кількість фільтрів, а отже і кількість смуг можуть бути різними (від 5 до 20). На виході кожного СФ підключено детектор та згладжувальний фільтр НЧ, який виділяє огинаючу мовного сигналу в даній частотній смузі. Отримана повільно змінювана напруга на виході ФНЧ характеризує амплітуду мовного сигналу в даній смузі частот $a_n(t)$. Практика показує, що при досить великій кількості смуг напруга на виході ФНЧ змінюється повільно, тому за амплітуду мовного сигналу в *i*-й смузі для інженерних розрахунків приймають значення мовного сигналу на середній частоті *i*-ї смуги. Мовний сигнал надходить також на пристрій виділення основного тону (ОТ), на виході якого формується сигнал, який характеризує частоту основного тону $\Omega(t)$.

Крім того, в аналізаторі виділяється сигнал тон-шум (Т-Ш), який характеризує склад спектра звуків мови – дискретний для вокалізованих звуків (тон) або безперервний для невокалізованих звуків (шум). Пристрій виділення сигналів Т-Ш може працювати або безпосередньо від мовних сигналів, або від сигналів, отриманих на виході пристрою виділення ОТ. Тому на рис. 2.13. схема виділення сигналів має два входи.

Сигнали, отримані на виході згладжувального фільтра та на виходах схеми виділення сигналів ОТ та Т-Ш, об'єднуються і перетворюються у форму, яка придатна для передачі каналом зв'язку.

Об'єднання та перетворення сигналів $a_i(t)$, $i=\overline{1,N}$ виконуються в пристрої (рис. 2.13), який називається об'єднуючим. На приймальній стороні каналу зв'язку здійснюється розділення сигналів (у розділювальному пристрої) та перетворення їх у форму, яка необхідна для роботи синтезатора.



2.13. Функціональна схема смугового вокодера

В аналогових вокодерах об'єднувальні та розділювальні пристрої реалізуються за принципами частотного розділення сигналів, а в аналогових та цифрових вокодерах – за часовим розділенням сигналів.

Сигнали Т-Ш керують приймачем, за допомогою якого на вхідну гребінку смугових фільтрів подається або широкосмуговий шум від генератора шуму, або імпульси від генератора ОТ. Цей генератор керується сигналом $\Omega(t)$ таким чином, що частота слідування імпульсів на виході дорівнює частоті основного тону мовного сигналу на передавальній стороні. Сукупність генераторів ОТ, шуму та схеми переключення Т-Ш називають генератором мовного сигналу (ГМС).

З виходу смугових фільтрів сигнали надходять на амплітудні модулятори (АМ). На інший вхід АМ як модулюючи надходять сигнали $a_i(t)$, $i=\overline{1,N}$, які після розділювального пристрою проходять через згладжувальні фільтри ФНЧ. З виходу АМ сигнали надходять на гребінку вихідних смугових фільтрів, які застосовуються для зменшення впливу побічних продуктів модуляції, які виникають в АМ. Сукупність схем та вузлів, у яких перетворюють мовні сигнали в межах кожної з частотних смуг (від входу смугового фільтра до виходу вихідного смугового фільтра синтезатора), називають спектральним каналом смугового вокодера. Звичайно, схеми смугових вокодерів доповнюються пристроями лінійного передбачення, що дозволяє створити смугові вокодери з лінійним передбаченням або ЛПК - вокодери. У таких вокодерах використовуються алгоритми лінійного передбачення, за

допомогою яких під час аналізу в передавальному пристрої визначаються коефіцієнти передбачення, а в приймальному пристрої на основі цих коефіцієнтів за допомогою рекурсивного цифрового фільтра синтезується еквівалент голосового тракту.

Ідея методу лінійного передбачення полягає в тому, що величина, яка прогнозується у мовному сигналі $\tilde{\lambda}(h)$ на момент випробування h, визначається як лінійно зважена сума попередніх вибірок:

$$\tilde{\lambda}(h) = \sum_{m=1}^{P} \tilde{\lambda}(h-m) a_m ,$$

де $\tilde{\lambda}(h-m)$ – мовний сигнал в попередній момент випробувань; $m = 1,2,...P$; a_m – коефіцієнти передбачення.

Інтервали часу між моментами вимірювань частотної дискретизації $t_h - t_{h-1} = 1/F_д$. В момент h, коли відомі $\tilde{\lambda}(h-m)$, але й дійсне значення мовного сигналу $\lambda(h)$, можна визначити помилку передбачення

$$e_h = \lambda_h - \tilde{\lambda}_h ,$$

а потім підібрати коефіцієнти передбачення a_m таким чином, щоб помилка передбачення була мінімальною. Звичайно, як критерій мінімізації використовують мінімум середньоквадратичної помилки. В цьому випадку треба визначити такі значення a_m, при яких $\sum_{h=0}^{M-1} e_h^2 = \min$. Задача мінімізації зводиться до рішення системи лінійних рівнянь відносно a_m.

Пристрій для обчислення помилки передбачення відповідно до виразу (2.6) представляє собою фільтр, передатна характеристика якого дорівнює передатній характеристиці фільтра, який імітує мовний тракт. Тому перетворення, що відповідає виразу (2.6), називають інверсною фільтрацією.

Усереднення помилки передбачення виконується на інтервалі $\Delta t = M t_h$ вибірок, які утворюють кадр (фрейм). Бажано, щоб довжина аналізованого звуку мови була узгоджена з довжиною кадру, але це технічно виконати складно. Тому звичайно приймають $M = 100...200$, що при $F_д = 8000$ Гц відповідає довжині кадру $\Delta t \approx 12,5...25$ мс.

Для одержання задовільної якості мовних сигналів, які синтезуються, потрібно підрахувати не менше десяти коефіцієнтів передбачення a_m, що в (2.5) відповідає $p = 10...12$. Враховуючи це, в аналізаторі ЛПК - вокодера треба вирішувати 100...200 лінійних рівнянь з 10...12 невідомими.

Коефіцієнти передбачення, значення яких передаються каналом зв’язку, використовуються як перемінні параметри у рекурсивному цифровому фільтрі, на вхід якого

подаються сигнали збудження. Як сигнали збудження в ЛПК - вокодері використовуються такі ж сигнали, які мають місце на виході генераторів мовного спектра (ГМС) у смугових вокодерах. Під час відтворення вокалізованих звуків – це послідовність імпульсів ОТ, а невокалізованих звуків – це випадкова послідовність імпульсів, сформованих генератором шуму.

Замість коефіцієнтів передбачення в більшості варіантів схем ЛПК - вокодерів передбачено отримання еквівалентного набору величин, які носять назву коефіцієнтів відбиття K_0. Ці параметри менш чутливі до квантування, ніж коефіцієнти передбачення a_m. Набори параметрів a_m та K_0 пов'язані поміж собою набором стандартних рекурентних співвідношень.

Ширина смуги фільтрів на вході та виході вибирається з урахуванням електроакустичних перетворювачів, які використовуються при цьому. Перетворювачі аналог-код та код-аналог працюють на принципах ІКМ. Аналізатор сигналів збудження здійснює виділення сигналів ОТ та Т-Ш, а також загального рівня (огинаючої мовного сигналу). Інші вузли виконують ті ж функції, що й у смуговому вокодері без лінійного передбачення.

Під час синтезу та дослідження смугових вокодерів з ЛПК використовують різні моделі мовного процесу. Найбільш точна модель мови представляє собою нестаціонарний випадковий процес з повільно змінюваною дисперсією та спектральною щільністю. У разі використання такої моделі можна одержати найбільш точний результат оцінки якості вокодера.

Питання для самоперевірки

1. Яка роль безперервних систем зв'язку в загальній системі зв'язку цивільної авіації?
2. Наведіть основні характеристики мовного сигналу.
3. Що таке основний тон мови, форманта, фонема?
4. Що таке артикуляція?
5. Які орієнтовні цифри, що характеризують норми розбірливості?
6. Яка природа надлишковості мовного сигналу?
7. Що таке кліпування мови?
8. Яка теоретична границя можливого стиснення спектра телефонного сигналу?
9. Що таке вокодер?
10. Які схемні методи підвищення завадостійкості безперервних систем зв'язку ви знаєте?

Розділ 3. Характеристика каналів витоку інформації в телекомунікаційних системах

3.1 Класифікація каналів витоку інформації

Під каналом витоку інформації будемо розуміти фізичний шлях від джерела конфіденційної інформації до зловмисника, по якому можливий витік відомостей, які охороняються. В залежності від фізичної природи утворення канали витоку інформації можна розділити на такі групи :

–візуально-оптичні ;

- акустичні ;
- електричні;
- радіотехнічні ;
- матеріально-речевинні .

Аналіз фізичних явищ багатьох перетворювачем та випромінювачем вказує ,що джерелом небезпечного сигналу є елементи ,вузли та провідники різних технічних засобів телекомунікаційних систем. Більшість природних каналів витоку можуть бути віднесені до таких видів:

1) Канали витоку за рахунок мікрофонного ефекту елементів електронних схем.

2) Канали витоку за рахунок магнітної складової поля електронних схем .

3) Канали витоку за рахунок електромагнітних випромінювань низької та високої частоти.

4) Канали витоку за рахунок виникнення паразитної генерації підсилювачів різного призначення.

5) Канали витоку за колами живлення.

6) Канали витоку за колами заземлення.

7)Канали витоку за рахунок високочастотного нав’язування .

8) Канали витоку за рахунок взаємного впливу проводів та ліній зв’язку.

9) Канали витоку волоконно-оптичних систем зв’язку.

Як було зазначено, відомчі телекомунікаційні системи будуються, як правило, на базі орендованих магістральних ліній передачі (телефонних каналів загального користування (ТФЗК)). Тому метою даного розділу є виявлення та класифікація каналів витоку інформації в типових каналах загального користування на базі яких створюються системи передачі даних (СПД). Розгляд СПД з точки зору визначення каналів витоку інформації обумовленим тим, що передачу мовної інформації можна розглянути як частину СПД.

Як правило, дискретний канал СПД містить в собі модулятор, демодулятор та аналоговий канал (ТФЗК). Аналоговий канал може бути двох типів – такий що комутується і такий що не комутується.

Найбільш складним для оцінки вразливості інформації в СПД є канал, що змінюється в часі та просторі (тобто має не детермінований характер).

Бурхливий розвиток обчислювальної техніки та мікроелектронної технології значно вплинув на побудову СПД. Сучасні СПД представляють собою програмно – технічні комплекси (ПТК), які виконують на базі персональних комп'ютерів, високошвидкісних модемів та існуючих каналів зв'язку. В значній мірі змінилася технологія обробки сигналів у СПД. Тепер формування та аналіз сигналів виконується як на апаратному так і на програмному рівнях.

Особливістю ПТК систем передачі даних є те, що в них інтегровані процеси вводу – виводу, захисту від помилок, формування та аналізу сигналів. У багатьох випадках важко або й не можливо роз'єднати ці процеси як на апаратному, так і програмному рівнях. Інша особливість цих систем полягає в тому, що вони виконують додаткові функції, які не пов'язані безпосередньо з передачею даних. До них відноситься – пошук та формування файлів даних, компресія, та декомпресія, захист від несанкціонованого доступу та інше.

Слід зазначити, що визначення "модем" відноситься до пристроїв, які виконують функції модуляції та демодуляції сигналів, тобто до пристроїв, які реалізують інтерфейс поміж аналоговим каналом та входом або виходу дискретного каналу. У Хейс – модемах, окрім зазначених функцій, виконується низка додаткових функцій, які пов'язані з обробкою даних.

У СПД широко використовуються Хейс – модеми з фіксованою швидкістю передавання даних 1300 та 3400 $\frac{БІТ}{с}$. В цих модемах, у відповідності до рекомендацій МККТТ V33, V34, використовується частотна та фазова маніпуляція.

На цей час стрімко зростає застосування Хейс – модемів – адаптивних пристроїв, які дозволяють передавати дані з швидкістю 19300 $\frac{БІТ}{с}$ за протоколами V33, V33 Біс. На швидкостях понад 3400 БІТ/с використовуються складні багато позиційні види модуляції. Високошвидкісні модеми адаптуються за швидкістю та форматом даних до стану каналу зв'язку. Адаптовано корегуються також частотно - фазові характеристики тракту передачі. Розподіл прямого та зворотного каналів у Хейс – модемах не частотний а часовий. Відзначимо, що передача даних по зворотному каналу іде з тією же швидкістю і з тим же видом маніпуляції, що й в прямому каналі.

Хейс – модеми виконуються у двох конструктивних варіантах. Перший – вбудований, який встановлюється в системну плату персонального комп'ютера (ПК). Другий – прибори у вигляді приладу з окремим джерелом живлення. Він підключається до ПК через COM – порт (COM1 – COM4). Це, як правило високошвидкісні модеми, які адаптується до середовища передачі даних.

В модемах, які використовують Хейс – модемну технологію, реалізуються MNP – протоколи різних рівнів. MNP – протоколи підтримують сценарій авто виклику, стискання даних та захисту від помилок. У Хейс – модемах авто набір використовується імпульсним або частотним способом. Режим авто набору реалізують без участі двохсотих кіл стику С3(RS333), так як у COM- портах ПК ці кола відсутні.

На цей час, серійно випускають великий набір Хейс – модемів, які розрізняються за швидкістю, ступеню адаптації до каналу зв'язку та за ступенем досконалості реалізації MNP – протоколів. Найбільш ефективними є автономні високошвидкісні Хейс – модеми, які реалізують апаратно MNP – протоколи.

Окрім Хейс – модемів, до цього часу використовується низько швидкісна апаратура передачі даних (від 600 до 3400 Біт / с).Вона добре зарекомендувала себе в СПД, де передаються невеликі обсяги інформації за один сеанс зв'язку.

Таким чином, в СПД, які функціонують по каналах ТФЗК, використовується апаратура передачі даних з різним набором компонентів та програмно – технічних засобів, з різним типом розподілу зворотного каналу (частотним, часовим) та з різним рівнем інтегрування процесів, апаратних та програмних засобів.

Вразливість інформації в СПД зменшується зі збільшенням ступеню інтеграції. Тому доцільно розглядати найбільш загальну модель дезінтегрованої СПД з повним набором функцій та режимів роботи. Такий підхід дозволить виключити втрату можливих місць виникнення каналів витоку інформації.

З метою визначення каналів витоку інформації розглянемо структурну схему СПД, яка представлена на рисунку 3.1.

Особливістю цієї моделі є те, що вона передбачає частотний та часовий розподіл прямого та зворотного каналів. У випадку частотного розподілу каналів (рекомендації МККТТ V34) апаратура передачі даних на боці відправника містить демодулятор зворотного каналу (М ЗК). Якщо в АПД реалізовано алгоритм роботи з часовим розподілом прямого та зворотного каналів, тобто підтримується протоколи V33, V33 біс (MNP3 – 10), тоді МЗК та Дем. ЗК – відсутні. Іншою особливістю моделі е те, що аналоговий канал представлений топологічною схемою проходження сигналів з урахуванням різних видів канало утворюючого обладнання.

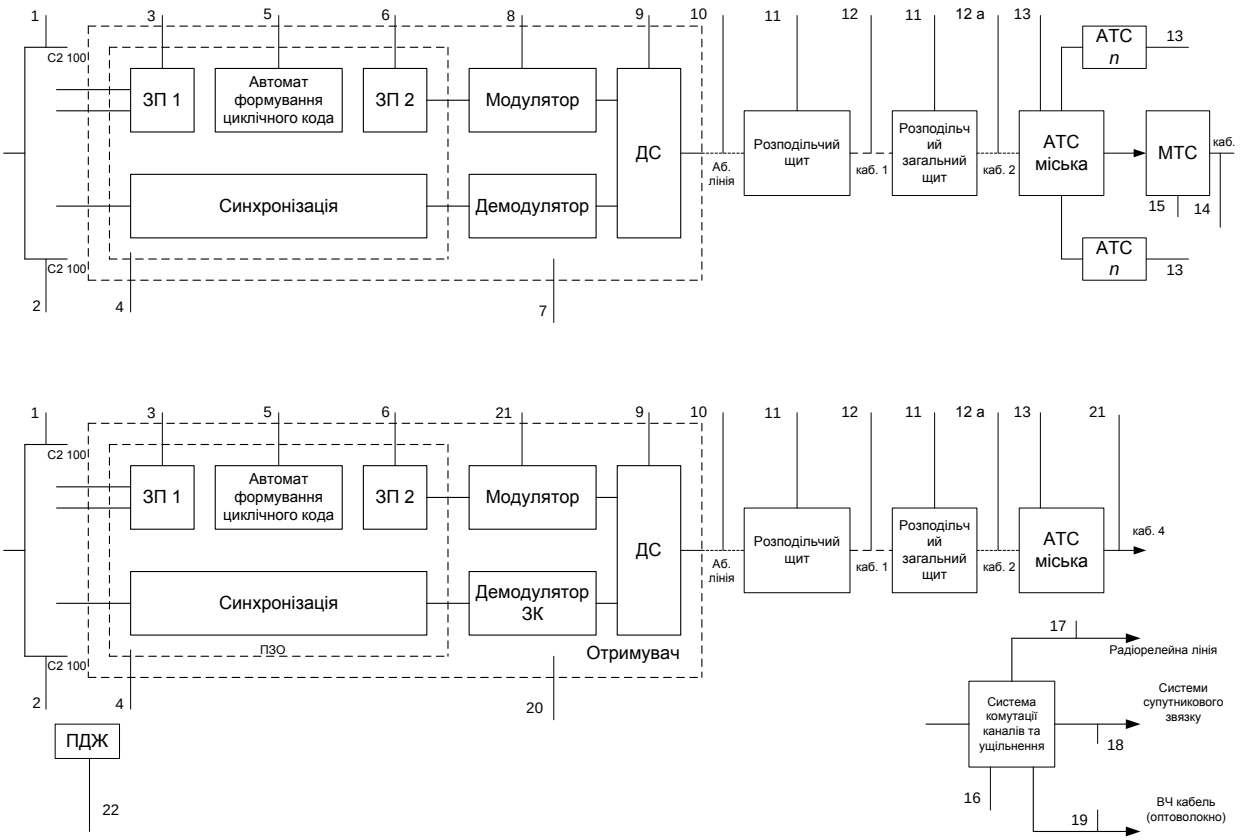


Рис. 3.1. Структурна схема системи передачі даних

Цифрами на топологічній схемі відмічені потенційно можливі місця вразливості СПД, в тому числі, місця проявлення каналів витоку та забороненого доступу до інформації. Місця вразливості визначались за допомогою досліджень фізичних процесів в елементах СПД, пов’язаних з даними, що передаються, сигналами синхронізації, авто набору, авто виклику, автовідповіді, сигналами зворотного каналу, а також перехідних процесів у колах первісних джерел живлення АДП. Місцями уразливості є, як правило самі елементи АПД, абонентські лінії зв’язку, розподільні щити, коробки, комутаційні обладнання АТС, ГТС, МТС, системи ущільнення, комутаційне обладнання, антенно – фідерні пристрої, кабелі та інше обладнання.

Цифрою 1 на топологічній схемі зазначені кола вхідних сигналів стику С3 (rs333) відправника та одержувача інформації. До них відносяться кола даних, що передаються (103, 103) відправника, кола даних, що приймаються (103 а, 104) приймача, кола детекторів якості каналу зв’язку з боку відправника та одержувача (109, 109а) кола синхронізації АДП та кінцевого обладнання даних (КОД) кола (105, 106, 107, 108), а також кола (115 – 135) зворотного каналу (якщо СПД з частотним розподілом каналів.

Цифрою 3 на топологічній схемі зазначені двохсоті кола стику С3(С3 – 300). За допомогою цих кіл здійснюється авто набір, авто виклик та автовідповідь з боку відправника та одержувача, фізично ці кола виконані у вигляді з’єднуючого кабелю довжиною не більше 3 м.

В АПД, на топологічній схемі, показані блоки, в яких відбувається перетворення сигналів або які мають фізичні з'єднання з іншими блоками.

Цифрами 3 та 6 відмічені однотипні блоки ЗП! Та ЗП3 (запам'ятовуючі пристрої) ЗП1 служить для накопичування інформації, з КОД з боку відправника або з виходу демодулятора з боку одержувача. ЗП3 є буфер між автоматом формування циклічного контролю (АФЦК) та модулятора з боку відправника та буфером між АФЦК реалізує функції завадостійкого кодування з боку відправника та декодування з боку одержувача. У відповідності до рекомендацій МККТТ, в АФЦК формується циклічний контроль за алгоритмами БЧХ - кодів та поліномами високого ступеню. АФЦК на топологічній схемі відмічений цифрою 5.

Цифрою 8 відмічений модулятор, який перетворює сигнали прямокутної форми в модульовані (за частотою / або за фазою) синусоїдальні сигнали тотальної частоти (ТЧ), які через диференціальну систему поступають в лінію зв'язку.

Цифрою 9 відмічено диференціальна система, яка здійснює перехід від двох провідної лінії до чотирьох провідної в АПД і тим самим розв'язує сигнали прямого та зворотного каналів. Крім того, по ній передаються сигнали авто набору, авто виклику та автовідповіді. Конструктивно диференціальна система виконана у вигляді екранованого трансформатора.

Цифрою 4 відмічений пристрій синхронізації, на який поступають сигнали з кіл стика С3. Він підтримує синхронну роботу КОД, модулятора зворотного каналу, демодулятора зворотного каналу, модулятора та демодулятора.

Цифрою 30 відмічено модулятор зворотного каналу на приймальній стороні. Він формує частотно модульовані сигнали, які передаються по частотному каналу зворотного зв'язку.

Цифрою 7 відмічено демодулятор зворотного каналу на передавальній стороні. Він демодулює сигнали зворотного каналу та ініціює повторну передачу блоків, які були пошкодженими.

АПД відправника та одержувача інформації об'єднані між собою трактом передачі даних. Весь тракт передачі даних можна розділити на три основних ділянки. Перші дві є однорідними ділянками. Вони об'єднують вихід АПД (відправника та одержувача) з входом місцевої АТС. Третя ділянка - між входом АТС відправника та виходом АТС одержувача.

Перші дві ділянки (абонентські лінії) сурово визначенні просторі та часі. Їх топологія не змінюється або змінюється дуже рідко.

Топологія третьої ділянки (канал, що комутується) апріорі не визначений ні в просторі, ні в часі. Перші дві ділянки містять лінії зв'язку (відмічені цифрою 10), один або більше розподільних щитів (цифра 11) з'єднувальні кабелі (цифри 13 та 13а), які ведуть до місцевої АТС.

Третя ділянка тракту передачі може містити ділянки пере приймальних ділянок з різним телекомунікаційним обладнанням, з різноманітними системами ущільнення та різними середовищами розповсюдження сигналів. Телекомунікаційне обладнання АТС, МТС, ММТС (цифри 13 та 14) можуть бути різної ємності (від 10 номерів до 100 000) та різних типів (декадно – крокова, координатна, квазіелектронна, електронна).

Цифрою 15 позначено системи ущільнення, які утворюють групові канали, та можуть бути як з частотним, так і з часовим ущільненням. Часові системи ущільнення (імпульсні) можуть бути фазоімпульсні. кодоімпульсні та інші.

В зв'язку з тим, що тракт передачі складається з окремих ділянок, то його технічні характеристики (коефіцієнт передачі, амплітудно частотна характеристика, відношення сигнал / шум та інші), можуть бути представленні в мультиплікативній формі. Звичайно, якщо технічні характеристики (ділянки 1 та 3) повністю детерміновані, то вони входять постійними коефіцієнтами мультиплікативних складових кожного з параметрів.

Для третьої ділянки значення параметрів, у загальному випадку, не визначено. Третя ділянка є канал, який комутується з лінійними і/або нелінійними перетвореннями сигналів. Характерною особливістю цього каналу є те, що він не стаціонарний у просторі та часі. Не стаціонарність каналу в просторі пояснюється тим, що при кожному новому з'єднанні (відправника та одержувача) він утворюється з тих ділянок, які на цей час розташовані ближче до елементу комутації або з тих ділянок, які на цей час є вільними. Суттєві зміни параметрів ТФЗК відбувається протягом доби. Це пов'язано з тим, що в години найбільшого навантаження ГНН навантаження може збільшуватися на декілька Ерланг. При цьому різко збільшується кількість відмов в автоматичних з'єднаннях абонентів в зв'язку з відсутністю вільних ліній. У СПД збільшується кількість перезапитів по зворотному каналу, що суттєво збільшує час передачі інформації.

Таким чином, для кожного технічного параметру тракту передачі інформації можна записати

$$R_{\sum}=R_1R_3R_3, \qquad (3.1)$$

де $R_{\sum}$ - загальний технічний показник тракту передачі; R_1, R_3, R_3 – параметри першої, другої та третьої ділянки відповідно.

Параметр R_3 є стохастичною функцією двох незалежних змінних в часі та просторі.

$$R_3 = f(S,T), \qquad (3.3)$$

де S – координата простору, T – координата часу.

У зв'язку з тим, що R_1 та R_3 величини детерміновані та апріорі відомі, то їх можна враховувати під час передачі та прийому даних. Тому загальний параметр буде визначатися тільки характеристиками третьої ділянки, що комутується.

$$R_{\sum} = f(S,T), \qquad (3.3)$$

Для невеликої кількості пере приймальних ділянок (або кількості з'єднань) можна визначити кінцеву кількість значень, що складають просторові координати параметра. Тоді $R_{\sum}$ буде належати деякій множині стохастичних функцій часу з множини R_T:

$$\{R_{\Sigma_1}(t), R_{\Sigma_2}(t), \dots, R_{\Sigma_k}(t),\} \subset R_T \qquad (3.4.)$$

Якщо кількість пере приймальних ділянок не більше двох, кількість множин функцій не перевищує 100, що робить можливим обчислення цього параметра з високою вірогідністю.

Таким чином, наявність в СПД, які функціонують по ТФЗК, елементів, що комутуються та залежність характеристик каналу від часу збільшує термін входження СПД у зв'язок та подовжує сеанс передавання даних. Це призводить до збільшення вирогідості вразливості інформації в СПД, тому що вірогідність вразливості є функцією часу, яка не зменшується.

На цій підставі можна зробити такі висновки:

- топологія СПД, які функціонують на ТФЗК, змінюється від з'єднання до з'єднання;
- характеристики таких СПД нестаціонарні у просторі та часі;
- показники, які пов'язані з вразливістю СПД, суттєво залежать від режиму роботи СПД (режим очікування зв'язку, режим входження в систему, режим передавання даних).

Враховуючи те, що зазначене вище, можна приступити до обґрунтування класифікатора каналів витоку інформації в СПД. Під каналом витоку інформації розуміють такі діючі на СПД дестабілізуючі фактори, наслідком яких може бути отримання (або безпека отримання) інформації з обмеженим доступом особами, які не мають на це законної підстави.

Класифікація каналів витоку інформації виконується з метою формування відносної множини потенційно можливих каналів витоку інформації. До формування повної множини дестабілізуючих факторів, пов'язаних з витоком інформації, висуваються абсолютні вимоги, тому що при втраті одного значущого фактору СПД, яка захищається, може виявитися абсолютно вразливою.

Взагалі то формування абсолютно повної множини витоку інформації в СПД, які функціонують по ТФЗК, в загальному вигляді не формалізована задача. Це пояснюється двома основними причинами. Перша – характеристики СПД носять стохастичний характер, що вносить невизначеність при визначенні кінцевої кількості елементів множин. Друга – завжди можна знайти маловірогідний, але потенційно можливий фактор, який приводить до вразливості інформації в СПД.

В цих умовах найбільш ефективним може бути підхід, який ґрунтується на використанні апарату нечітких множин. Нагадаємо, що нечітка множина – це така множина, кожний елемент якої визначено його значенням та вірогідністю належності до цієї множини. Нехай, наприклад, існує нечітка множина А. То наведений нижче вираз означає, що елемент a_i з вирогідністю *Pi* належить множині А:

$$\{a_i, P_i\} \in A, \tag{3.5.}$$

Нижче наведена методика формування повної множини каналів витоку інформації.

Кожний клас каналів витоку представимо як нечітку множину, елементи якої належать з вірогідністю *Pij* до *Aj*, тобто:

$$\{a_{ij}, P_{ij}\} \in A_j, \tag{3.6.}$$

для всіх n_i, де n_i – кількість елементів множини.

Тоді існує така нечітка множина, для якої справедливий такий вираз:

$$\left\{ \begin{array}{l} B = \bigcup_{j=1}^{n} A_j = A_1 \cup A_2 \cup \ldots \cup A_n; \\ \max\{P_{i1}, P_{i2}, \ldots, P_{in}\} \end{array} \right\} \tag{3.7.}$$

Вираз 10.7значає об’єднання *n* нечітких множин, де вірогідність появи однотипних елементів (елементів, які належать двом або більше множинам) враховується з максимальною вірогідністю. З метою спрощення розв’язання цього завдання скористаємося таким підходом. Введемо поняття порогового рівня вірогідності присутності елемента в нечіткій множині. Запишемо

$$P_{akj} < P_{nop}, \tag{3.8.}$$

де P_{akj} – вірогідність присутності елемента *a* підмножини *k* множини *j*; P_{nop} – нижня порогова вірогідність присутності a_{ki}.

На практиці це означає, що цей дестабілізуючий фактор у заданому класі маловірогідний та їм можна знехтувати. Цей процес назвемо просіюванням нечітких множин.

Якщо в результаті буде виконана умова

$$\sum_{k=1}^{nj} \sum_{j=1}^{n} P_{akj} < P_{nop}, \tag{3.9}$$

де *nj* – кількість елементів у цьому класі, для яких виконується (10.8) *n* – кількість класів каналів витоку.

Тоді елементам , що залишилися, можна привласнити норму $P_н = 1$ (рівну одиниці) та елементи, які залишились розглядати як елементи звичайних множин.

Вираз, наведений нижче (3.10), означає, що за зазначений термін з вірогідністю $P_н$ не може здійснитись жодна з подій із усіх (*n*) підмножин.

$$P_H = \left(1 - \sum_{k=1}^{nj} \sum_{j=1}^{n} P_{akj}\right) > \left(1 - P_{пор}\right) \tag{3.10}$$

Вірогідність появи хоча б однієї з подій із множини (n) визначається за формулою

$$Рв = 1 - Рн \tag{3.11}$$

Таким чином, в результаті просіювання одержимо нові підмножини, для яких справедливе таке співвідношення

$$\{a_i'\} \in A_j', \tag{3.13}$$

для всіх $i \neq k$

Визначимо повну множину елементів, які входять в об'єднання множин, які були просіяні з 3.7та 3.13

$$B^{/} = \bigcup_{j=1}^{n-k} A_j^{/} \tag{3.13}$$

Потім визначимо кількість елементів множини $B^{/}$, яка за визначенням відбиває повну множину каналів витоку. Позначимо кількість елементів, які належать j-й множині (3.13) $N_i = N[N_j]$, тоді кількість елементів, що входять в ділянки, які перетинаються складає:

$$N_P^l = N(n^{(l)} A_{Pl}) \tag{3.14}$$

де N_P^l - кількість елементів, які належать ділянкам множин, які перетинаються.

l - кількість множин, які перетинаються одночасно;

A_{Pl} - ділянка, яка утворена перетинанням (l) множин. Загальний вираз для визначення кількості елементів, які входять у об'єднання підмножин 3.7 та 3.13, має вигляд:

$$M = \sum_{j=1}^{n} N[A_j^{/}] - \sum_{i=1}^{C_n^2} N(n^{(2)} A_{2i}^{/}) + \sum_{i=L}^{C_n^2} N(n^{(3)} A_{3i}^{/}) + \ldots +$$

$$+ \sum_{i=L}^{C_n^{n-1}} N(n^{(n-1)} A_{(n-1)i} + N(n^{(n)} A_{ni})) \tag{3.15}$$

$$C_n^l = \frac{n(n-1)\ldots(n-l)}{l!} \tag{3.16}$$

Вираз (3.15) справедливий для визначення кількості елементів об'єднання нечітких множин, якщо $A_j^{/}$ замінити на A_j та скористатися формулами (3.6) та (3.7).

Рівняння (3.15) дозволяє дати оцінку якості класифікації каналів витоку інформації. Так, якщо всі елементи правої частини рівняння (3.15), окрім першого, дорівнюють нулю, то множини B (3.7) та $B^{/}$ (3.13) складаються з множин, які не пересікаються. Цей випадок є ідеальним з точки зору якості класифікації каналів витоку. Оцінка „відмінно". Самий невдалий випадок, коли останній член не дорівнює нулю. Це означає, що всі множники

пересікаються. Оцінка може бути „незадовільно”. Якщо не дорівнює нулю тільки перший та другий член, та значення суми елементів першого члена суттєво більше значення суми елементів другого члена, то оцінка якості – „добре”. Якщо відмінні від нуля другий та третій член та їх сума суттєво менше елементів першого члена, то оцінка – „задовільно”.

Кількісну характеристику оцінки якості класифікації за критерієм рівня уложення множин можна отримати скориставшись такими рівняннями:

$$K_B = (1 - \frac{F - D}{F}), \tag{3.17}$$

$$\text{де } F = \sum_{i=1}^{n} N(A_j^{/}), \tag{3.18}$$

$$D = \sum_{i=1}^{n} (\bigcap\nolimits^{(2)} A_{P2i}^{/}) - \sum_{i=1}^{C_n^n} N(\bigcap\nolimits^{(3)} A_{P3i}^{/}) - ... - \sum_{i=1}^{C_n^{n-1}} N(\bigcap A^{/} p(n-1)i) - N(\bigcap\nolimits^{(n)} A_{Pni}^{/}) \tag{3.19}$$

Значення коефіцієнта K_B лежить в межах від 0 до 1. Він вказує, яка частина множин (3.17)або (3.13) є загальними (вкладеними) для двох або більше підмножин $A_j, A_j^{/}$ де $j = [1, n]$. Значенню $K_B = 0$ відповідає оцінка – „відмінно”.

Кількісну оцінку з (3.17) можна значно спростити, якщо у виразі (3.19) обмежитись першими двома членами, тобто враховувати перетинання кратністю не більше трьох. Ці випадки найбільш важливі для практики, тому що перетинання кратністю більш ніж три маловірогідні:

$$D^{/} = \sum_{i=1}^{C_n^2} N(\bigcap\nolimits^{(2)} A_{p(2)i}^{/}) - \sum_{i=1}^{C_n^3} N(\bigcap\nolimits^{(3)} A_{P(3)i}^{/}) \tag{3.30}$$

Як було сказано вище, характеристики СПД, які функціонують за допомогою ТФКЗК, нестаціонарні в просторі та часі, і як наслідок цього показники захищеності залежать від режиму роботи СПД. Тому структура класифікатора в значній мірі визначається режимами роботи СПД. Режим роботи СПД встановлюється часовим трафіком, який може бути детермінованим. У відповідності до часового трафіку розрізняють чотири основних режими роботи СПД:

- передавання даних (режим 1);
- входження в зв’язок (режим 3);
- очікування зв’язку (режим 3);
- АПД виключена – це режим не пов’язаний з передаванням даних (режим 4).

Режими 3 та 4 утворюють підмножину, для яких значення коефіцієнту включення множин (3.17) K_B наближається до одиниці. Вказані підмножини відрізняються тільки апріорними вірогідностями виникнення окремих елементів. Тому дві підмножини можна замінити підмножиною $P_{очі}$, надав кожному і-му елементу норму $P_{очі} = 1$.

Таким чином, одержимо три групи підмножин відповідаючих режимам передачі, входження в зв'язок та очікування зв'язку:

$$\{П_{вих\,i}\} \subseteq \{П_{оч\,i}\}, \tag{3.31}$$

де $\{П_{вих\,i}\}$ - групи підмножин у режимі АПД – виключена;

$\{П_{оч\,i}\}$ - групи підмножин у режимі АПД – очікування зв'язку.

Другим критерієм вибору груп класів, служить показник, який визначає ступінь взаємодії зловмисника з СПД та її елементами. За цим критерієм канали витоку розбиваються на дві категорії – опосередковані канали та прямі. Опосередковані канали витоку це канали без доступу до СПД та її елементів. Прямі, в свою чергу, розбиваються на дві групи – з доступом до елементів СПД, але без зміни або модифікації її елементів та з доступом і можливістю зміни та модифікації її елементів.

Класифікатор каналів витоку інформації з обмеженим доступом в СПД, які функціонують по каналах ТФЗК, наведено в таблиці 3.1

Всю множину каналів витоку розбито на групи за режимами роботи, які утворюють три стовпці та три групи за типом доступу до інформації, які утворюють три строки. Таким чином, всю множину потенційно можливих каналів витоку інформації розбито на 9 класів.

Таблиця 3.1

Класифікатор каналів витоку інформації

Види каналів	Режим очікування зв'язку	Режим входження в зв'язок	Режим передавання або приймання даних
Без доступу до СПД (опосередковані)	1 клас	3 клас	3 клас
З доступом до СПД але без зміни її модифікації (прямі)	4 клас	5 клас	6 клас
З доступом до СПД та зміною її модифікації (прямі)	7 клас	8 клас	9 клас

Далі наведені результати досліджень, пов'язаних з формуванням відносно повної множини каналів витоку інформації в СПД.

Вказана множина каналів витоку інформації розбита на дев'ять підмножин у відповідності до класифікатора (табл. 10.1)

Результати формування підмножин каналів витоку інформації (для кожного класу) наведені у вигляді дев'яти таблиць. У кожній таблиці вказані елементи множин (канали

витоку інформації), місця їх проявлення (у відповідності до топологічної схеми СПД) та їх приналежність (Відправник, Одержувач).

Місця проявлення дестабілізуючих факторів, які не пов’язані з системою передачі даних, відмічені в таблицях латинськими літерами.

Таблиця 3.3

Клас 1. Опосередковані канали. Режим очікування зв’язку.

№	Вид дестабілізуючих факторів (вид каналу витоку інформації)	Місце прояву	Одержувач Відправник
1	3	3	4
1	Крадіжка програмно-технічних засобів та (або) документації на неї на заводах-виробниках, службах ремонту, перевірки сертифікації її у користувача з метою виявлення характеру та структури даних, що передаються	A	
3	Провокування на розмови осіб, які мають відношення до СПД та лініям зв’язку, з метою виявлення трафіків передачі, характеру та параметрів передавання даних	A	
3	Підслуховування розмов осіб, які мають відношення до СПД та лініям зв’язку, з метою виявлення трафіків передачі, характеру та параметрів передавання даних	A,D,C	
4	Використання візуальних засобів (фотоапарати, телекамери, біноклі та інші) з метою отримання інформації про апаратуру та технології обробки інформації, характеристиках даних, що передаються	D	
5	Використання зловмисниками підслуховуючої апаратури для прослуховування розмов осіб, які мають відношення до СПД	D	
6	Крадіжка виробничих відходів (носіїв інформації, документів та таке інше).	C, 9	

Таблиця 3.3

Клас 3. Опосередковані канали. Режим входження у зв’язок.

№	Вид дестабілізуючих факторів (вид каналу витоку інформації)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Перехоплення електромагнітних випромінювань (ЕВМ) з’єднувального кабелю стику С3 з метою визначення номеру абонента, що викликається	3	Відправник (Вд)
3	Перехоплення ЕМВ з’єднувального кабелю стику С3 (кола С3-100) з метою визначення характеристик сигналів синхронізації	1	Одержувач (Од)

			Відправник (Вд)
3	Перехоплення ЕМВ ОЗУ з метою визначення номеру абонента, що викликається	3,6	Вд.
4	Перехоплення ЕМВ блока СИНХР з метою визначення характеристик сигналів синхронізації	4	Вд., Од.
5	Перехоплення ЕМВ диф. системи з метою визначення номеру абонента, що викликається	9	Вд.
6	Перехоплення ЕМВ абонентських ліній, кабелів з'єднувальних та магістральних з метою визначення номера абонента, що викликається	10,13,14	Вд.
7	Перехоплення ЕМВ розподільчих щитів з метою визначення номера абонента, що викликається	11	Вд.
8	Перехоплення ЕМВ елементів комутації АТС з метою визначення номера абонента, що викликається	13,15	Вд., Од.
9	Перехоплення наводок ЕМВ в колах первісних джерел живлення з метою визначення номера абонента, що викликається	33	Вд.
10	Перехоплення ЕМВ систем ущільнення, ретрансляції, високочастотних кабелів з метою визначення номера абонента, що викликається	15	Вд.
11	Перехоплення наводок ЕМВ в інших колах з метою визначення номера абонента, що викликається	В	Вд.
13	Перехоплення наводок ЕМВ в інженерних системах будинків та споруд з метою визначення номера абонента, що викликається	С	Вд.
13	Перехоплення оптичних сигналів у оптоволоконних системах з метою отримання номерів абонентів СПД	30	Вд., Од.

Таблиця 3.4

Клас 3. Опосередковані канали. Режим передачі даних.

№	Дестабілізуючі фактори (канали витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Перехват ЕВМ на стику С3 (кола С3-100) з метою одержання даних, що передаються	1	Вд., Од.
3	Перехват ЕМВ блоків ОЗП та АФЦК з метою отримання даних, що передаються	3,5,6	Вд., Од.
3	Перехват ЕМВ ОЗУ з метою визначення номеру абонента, що викликається	7,8	Вд.

4	Перехоплення ЕМВ блоком Диф. системи з метою одержання даних, що передаються	9	Вд., Од.
5	Перехват ЕМВ абонентської лінії, з'єднувальних та магістральних кабелів з метою одержання даних, що передаються	13,10,14	Вд., Од.
6	Перехват ЕМВ розподільчих щитів з метою одержання даних, що передаються	11	Вд., Од.
7	Перехоплення ЕМВ в коаксіальних кабелях з метою одержання даних, що передаються	13	Вд., Од.
8	Перехват ЕМВ апаратури АТС, МАТС з метою одержання даних, що передаються	13,15	Вд., Од.
9	Перехват ЕМВ радіорелейних ліній, ретрансляторів, в тому числі кабелів та каналів супутникового зв′язку з метою одержання даних, що передаються	16,17,18, 19	Вд., Од.
10	Перехват ЕМВ Демодулятора та модулятора ЗК з метою одержання даних, що передаються	8,31	Од.
11	Перехоплення оптичних випромінювань оптоволоконних систем з метою одержання даних, що передаються	30	Вд., Од
13	Перехват наводок ЕМВ в колах первісних джерел живлення з метою одержання даних, що передаються	33	Вд., Од
13	Перехоплення наводок ЕМВ в колах телефонізації та інших	В	Вд., Од
14	Перехоплення наводок ЕМВ в інженерних системах будинків та споруд з метою одержання даних, що передаються	С	Вд., Од.

Таблиця 3.5

Клас 4. Прямі Канали без доступу до елементів СПД. Режим очікування зв′язку.

№	Види дестабілізуючих факторів (канали витоку)	Місце прояв-лення	Одержувач, Відправник
1	3	3	4
1	Копіювання змісту файлу ОЗП з метою одержання даних, які раніше передавалися.	3,6	Вд., Од.
3	Перегляд та копіювання експлуатаційних документів з метою одержання інформації про характер даних, що передаються, трафіку та інші.	А	Вд., Од.
3	Перегляд та копіювання журналів обліку з метою одержання інформації про характер даних, що передаються, трафік та інше.	А	Вд., Од
4	Визначення стану комутаційних елементів з метою визначення телефонів абонентів СПД після завершення сеансу зв′язку	13,15	Вд., Од.
5	Крадіжки виробничих відходів з метою одержання інформації про характер даних, що передаються, про трафік та інше.	А	Вд., Од.

Таблиця 3.6

Клас 5. Прямі канали без доступу до елементів СПД. Режим входження в зв’язок.

№	Вид дестабілізуючих факторів (вид каналу витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Копіювання сигналів на стику С3 (кола С3-300) з метою визначення номера абонента, що викликається	3	Вд.
3	Копіювання сигналів на стику С3 (кола С3-100) з метою визначення характеристик сигналів синхронізації	1	Вд., Од.
3	Копіювання сигналів виклику на вході СПД (стик С1 та абонентської лінії з метою визначення номера абонента, що викликається	10,9	Вд.
4	Копіювання сигналів виклику з розподільчих щитів з метою визначення номера абонента, що викликається	11	Вд.
5	Копіювання сигналів з’єднувальних кабелів з метою визначення номера абонента, що викликається	13,14	Вд.
6	Копіювання сигналів автовиклику та автовідповіді АТС, МАТС з метою визначення номера абонента, що викликається	13,15	Вд., Од.
7	Копіювання сигналів автовиклику радіорелейних ліній оптоволоконних ліній, супутникових каналів з метою визначення номера абонента, що викликається	17,19	Вд., Од.

Таблиця 3.7

Клас 6. Прямі канали без доступу до елементів СПД. Режим передачі даних.

№	Види дестабілізуючих факторів (канали витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Копіювання на вході стику С3 (кола С3-100) з метою одержання даних, що передаються	1	Вд., Од.
3	Копіювання даних ОЗП з метою одержання даних, що передаються	3,5,6	Вд., Од.
3	Копіювання на вході Мод. АПД та абонентської лінії з метою одержання даних, що передаються	8,9,10	Вд., Од.
4	Копіювання даних в місцях з′єднань розподільчих щитів з метою одержання даних, що передаються	11	Вд., Од.
5	Копіювання даних в місцях з′єднання кабелів з метою одержання даних, що передаються	13,14	Вд., Од.
6	Копіювання даних на входах та виходах каналоутворюючої апаратури АТС, МАТС з метою одержання даних, що передаються	13,15	Вд., Од.

7	Копіювання даних на входах та виходах каналоутворюючої апаратури систем супутникового зв’язку, оптоволоконного зв′язку, радіорелейного зв’язку та іншого, з метою одержання даних, що передаються	17,19,30	Вд., Од.
8	Копіювання даних на вході Дем. з метою одержання даних, що передаються	31	Од.

Таблиця 3.8

Клас 7. Прямі канали без доступу до елементів СПД. Режим очікування зв′язку.

№	Види дестабілізуючих факторів (канали витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Заміна програмно-апаратних засобів АПД з метою наступної переадресації даних зловмиснику	3,4,5,6	Вд.
3	Заміна документів, які регламентують трафік з метою Н	А	Вд.
3	Заміна або крадіжка носіїв інформації, які містять дані, що передаються з метою створення, знищення або модифікації даних (мета L)	А	Вд.
4	Підключення підслуховуючої апаратури , магнітофонів, відеотехніки з метою одержання інформації в наступні періоди про характер даних, трафік, технології передавання (мета М)	А	Вд.
5	Підключення нештатної апаратури до елементів СПД з метою одержання спотворення, модифікації або знищення даних, а також з метою переадресації даних зловмиснику	1,3,3,6,7, 8,9,1011, 13,13,14, 15	

Таблиця 3.9

Клас 8. Прямі канали з можливістю зміни елементів СПД. Режим входження в зв′язок.

№	Види дестабілізуючих факторів (вид каналу витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Копіювання, спотворення або заміна сигналів автовиклику та синхронізації на вході та виході АПД з метою визначення або переадресації даних, що передаються (мета N)	1,3,6,9	Вд.
3	Копіювання, спотворення або заміна сигналів автовиклику в будь-який точці абонентської лінії з метою N	10	Вд.
3	Копіювання, спотворення або заміна сигналів автовиклику в розподільчих щитах з метою N	11	Вд.
4	Копіювання, спотворення або заміна сигналів автовиклику в кабельних з′єднання з метою N	13,14	Вд.
5	Копіювання, спотворення або заміна сигналів автовиклику на виході та вході каналоутворюючої апаратури АТС, МАТС з метою N	13,15	Вд.
6	Копіювання, спотворення або заміна сигналів автовиклику в системах ущільнення та передавання даних з метою N	17,18,19	Вд.

Таблиця 3.10

Клас 9. Прямі канали з можливістю зміни елементів СПД. Режим передавання даних.

№	Види дестабілізуючих факторів (вид каналу витоку)	Місце прояву	Одержувач, Відправник
1	3	3	4
1	Копіювання, спотворення або генерація хибних сигналів на вході АПД з метою копіювання, спотворення або модифікація даних, що передаються (мета F)	1	Вд., Од.
3	Копіювання, спотворення або генерація хибних сигналів в різних блоках АПД з метою F	3,5,6,8,9	Вд., Од
3	Копіювання, спотворення або генерація хибних сигналів в різних точках абонентської лінії з метою F	10	Вд., Од
4	Копіювання, спотворення або генерація хибних сигналів у розподільчих щитах з метою F	11	Вд., Од
5	Копіювання, спотворення або генерація хибних сигналів у кабелях з метою F	13,14	Вд., Од
6	Копіювання, спотворення або генерація хибних сигналів на входах та виходах каналоутворюючої апаратури АТС, МАТС з метою F	13,15	Вд., Од
7	Спотворення сигналів зворотного каналу з метою спотворення або знищення даних	8	Вд., Од
8	Копіювання, спотворення або генерація хибних сигналів у системах ущільнення, супутниковому зв'язку, радіорелейних та оптоволоконних системах	17,18,19	Вд., Од

3.2 Моделі електромагнітних каналів витоку інформації

3.2.1 Загальна характеристика безпровідних мереж

Безпровідний радіоканал - це складне середовище, що забезпечує надійний зв'язок з високою швидкістю передачі. Він не тільки піддається впливу шумів, перешкод, затінень, багатопроменевого поширення, але й вносить додаткові проблеми через те, що ці негативні впливи при переміщенні користувача змінюються в часі непередбаченим чином. Моделювання зміни потужності прийнятого сигналу, що зумовлено процесами поширення сигналів й їхнім затіненням, потрібно як при аналізі, так і синтезі СРР.

Помітні зміни сигналу відбуваються при переміщенні від джерела на відстань 100... 1000 м, а затінення проявляються на відстанях, що дорівнюють розмірами об'єкта та створює перешкоду для розповсюдження хвилі (10..100 м на вулиці й ще менше усередині будинків).

Зміни характеристик без провідного каналу в результаті багатопроменевого поширення сигналів проявляються на невеликих відстанях, порівнянних з довжиною хвилі.

Надалі основну увагу буде приділено поширенню радіохвиль у діапазонах від 0,3...3 до 3...30 Ггц.

При побудові моделей поширення радіохвиль у наземних безпровідних системах варто враховувати відбиття й розсіювання від природних і антропогенних об'єктів.

Для побудови точних моделей при невеликому числі багатопроменевих складових використаються рівняння Максвелла. Моделі конкретної траси поширення радіохвиль у значній мірі залежать від геометричних і діелектричних властивостей області, через яку поширюється сигнал. Коли є велика кількість складових багатопроменевого сигналу або геометрія й діелектричні властивості середовища поширення невідомі, звичайно використають статистичні моделі.

Розглянемо особливості побудови моделей поширення хвиль у СРР. Електромагнітні хвилі поширюється у середовищі, де вони відбиваються, розсіюються й переломлюються земною поверхнею, будинками, рослинами й іншими об'єктами. Повні характеристики поширення радіохвиль можна одержати, вирішуючи рівняння Максвелла за певних умов, які відображають фізичні характеристики перешкод, що створюють об'єкти. Для цього потрібне обчислення ефективної площі об'єктів, що відбивають, з великою й складною структурою. Оскільки ці обчислення важко здійснити, а в багатьох випадках відсутні необхідні для цього параметри, для одержання характеристик поширення сигналів часто використаються методи апроксимації, які не потребують рішення рівнянь Максвелла.

Найбільш прості апроксимації припускають визначення траєкторії поширення радіохвиль. Цей метод описує поширення електромагнітних хвиль шляхом подання хвильового фронту у вигляді елементарних часток, при цьому модель дозволяє визначити вплив відбиття і переломлення на хвильовий фронт, але не враховує більше складне явище розсіювання, що враховується у диференціальних рівняннях Максвелла. Найпростішою моделлю визначення траєкторії поширення радіохвиль є дво параметрична модель, що точно описує поширення сигналу, коли є один прямий шлях між передавачем і приймачем й один відбитий. На рівнинній місцевості відбита хвиля звичайно виникає при відбитті радіосигналу від землі. Дво параметрична модель служить гарною апроксимацією для відображення поширення радіохвиль уздовж магістральних доріг, у сільській місцевості й над водою.

Часто складність і розмаїтість умов функціонування радіоканалів ускладнює побудова їх точної детермінованої моделі. У цих випадках широко використають статистичні моделі. Прикладом статистичних моделей можуть бути релеєвські завмирання, які дозволяють прогнозувати загасання, що виникають у наслідок переміщенням і різних

перешкодами. Коли на характеристики каналу значно впливають геометричні й діелектричні властивості середовища поширення радіохвиль, статистичні моделі найчастіше виявляються занадто грубими й не дозволяють одержати корисну інформацію. Це характерно для простору усередині приміщень, де характеристики поширення різко змінюються залежно від типу об'єкта (фабрика, офіс, цех з металообробними верстатами і т.д.). Для таких середовищ при прогнозуванні характеристик поширення радіосигналів застосовують комп'ютерне моделювання

Припустимо, що переданий сигнал має вигляд

$$s(t) = R\left\{u(t)e^{j(2\pi f_c t+\varphi_0)}\right\}, \qquad (3.32)$$

де $u(t)$ — сигнал без модуляції зі смугою B и потужністю передача P_t; f_c — частота несучої; φ_0 — довільна початкова фаза. Звичайно при проведенні аналізу виключається остання частина рівняння, що визначає фазу $e^{j(2\pi f_c t+\varphi_0)}$ прийнятого сигналу, оскільки вона є постійним множником для всіх складових прийнятого сигналу, включаючи промінь, що поширюється по лінії прямої видимості через вільний простір, і всіх відбитих і переломлених багатопроменевих складових. Крім випадкової фази прийнятий сигнал буде мати допплерівський зсув частоти в кожній зі складових прийнятого сигналу, рівний $\upsilon\cos\theta/\lambda$, де θ — кут приходу складового сигналу, υ — швидкість руху приймача, $\lambda = c/f_c$ — довжина хвилі радіосигналу. У першому випадку будемо нехтувати допплерівським зсувом, тому що для звичайних швидкостей руху в місті транспортних засобів (80 км/г) і частот (у межах 1 ГГц) він становить менш 70 Гц. Також передбачається, що сигнал без модуляції є реальною величиною, оскільки це не вплине на модель втрат на трасі й дозволяє полегшити рівняння.

3.2.2 Детерміновані моделі

Загасання радіосигналів у вільному просторі.

Розглянемо радіосигнал, що розповсюджується у вільному просторі на приймач, вилучений на відстань d від передавача. Передбачається, що такий сигнал поширюється на лінії прямої видимості, тобто між передавачем і приймачем немає перешкод, і без яких-небудь відбиттів. У цьому випадку прийнятий сигнал визначається з формули втрат при поширенні у вільному просторі:

$$r(t) = \mathrm{Re}\left\{u(t)e^{j(2\pi f_c t+\varphi_0)}\right\}\frac{\lambda\sqrt{G_l e^{j(2\pi d/\lambda)}}}{4\pi d} = u(t)\frac{\lambda\sqrt{G_l e^{j(2\pi d/\lambda)}}}{4\pi d} * \cos(2\pi f_c t+\varphi_0),$$

де $\sqrt{G_l}$ враховує діаграми спрямованості передавальної й приймальні антен у напрямку прямої видимості, при цьому середня прийнята потужність сигналу становить

$P_r = \overline{r(t)r^*(t)}$, r^* де позначає комплексну сполучену величину. Відношення потужностей прийнятого й переданого сигналів

$$\frac{P_r}{P_t} = (\frac{\sqrt{G_l \lambda}}{4\pi d})^2.$$

Таким чином, потужність прийнятого сигналу зменшується пропорційно квадрату відстані *d* між передавальною й приймальнею антенами.

3.2.3 Багатопроменеве поширення радіохвиль

У звичайному міському середовищі радіосигнал, переданий від нерухомого джерела до мобільного приймача, набуває змін як по амплітуді, так і по фазі. Ці зміни обумовлені багатопроменевим поширенням, що виникає при його відбитті, переломленні або розсіюванні об'єктом. Копії переданого сигналу можуть загасати по потужності, затримуватися за часом, зрушуватися по фазі й/або частоті в порівнянні із прямою хвилею. В каналах з вузькою смугою вплив багатьох променів приводить до того, що прийнятий сигнал змінюватися по амплітуді.

При побудові моделей, відстані обираються таким чином, щоб на поширення не впливала кривизна Землі. Якщо передавач, приймач і відбивачі нерухомі, то позитивні й негативні ефекти внаслідок багатопроменевого поширення, а також затримки променя, що поширюється по лінії прямої видимості, є постійними. Однак, якщо джерело сигналів або приймач переміщаються, то характеристики багатопроменевого поширення змінюються в часі, ці тимчасові зміни можуть бути враховані у випадку, коли число, місце розташування й характеристики відбивачів відомі, у протилежному випадку необхідно використовувати статистичні моделі.

Помилка апроксимації при врахуванні траєкторій поширення радіохвиль є найменшої, коли приймач вилучений від найближчого об'єкта, що створює розсіювання, на відстань багатьох довжин хвиль і всіх об'єктів, що розсіюють і є досить великим у порівнянні з довжиною хвилі, і досить гладкими (як це має місце, наприклад, при відбитті від вікон). Порівнюючи результати рішень, отриманих методом аналізу траєкторій поширення радіохвиль, з емпіричними даними показує, що модель цілком адекватна для сільських районів і міських вулиць, де передавач і приймач підняті невисоко над землею.

Найбільш точна модель, що враховує траєкторії поширення променів, включає всі складові багатопроменевого сигналу з урахуванням загасання, переломлення й розсіювання. У цій моделі враховуються всі геометричні і діелектричні властивості будинків, що оточують передавач і приймач, тому ці моделі вимагають проведення додаткових вимірів на цій ділянці місцевості. Комп'ютерні програми, засновані на цій

моделі , використають для обчислень базу знань про будинки, що перебувають на обраній ділянці місцевості, що сьогодні досить широко використовується для планування СРР як на вулиці, так й усередині будинків.

Спочатку буде розглянута двопроменева модель, що дозволяє визначати зміни сигналу в результаті додавання променів, відбитого від землі, і прямого променя. Ця модель адекватно описує процес поширення сигналу в районах з невеликим числом відбивачів, наприклад сільських або шосейних доріг. Потім розглядається десятипроменева модель, що дозволяє визначати зміни сигналу, що поширюється уздовж прямої вулиці великою кількістю будинків за умови, що передавальна й приймальня антени розташовані нижче рівня будинків. І, нарешті, буде розглянута узагальнена модель, що дозволяє прогнозувати поширення сигналів при будь-якому розміщенні будинків, приймачів і передавачів.

Двопроменева модель передбачає наявність даних тільки про висоту антен, для побудови десятипроменевої моделі необхідні вихідні дані про висоту антен і ширину вулиці, а для побудови узагальненої моделі потрібно не тільки наявність цих параметрів, але й докладна інформації про геометрію й діелектричні властивості навколишніх будинків.

3.2.3.1 Двопроменева модель поширення радіохвиль

Двопроменева модель (рис. 3.2) застосовується у випадках, коли прийнятий сигнал складається з двох складових: прямої хвилі й відбитої від поверхні Землі.

Перша складова визначається з формули втрат при поширенні у вільному просторі (3.33). Відбитий промінь представлений на рис. 3.2 сегментами r й r'. Використовуючи метод накладення, одержимо, що прийнятий сигнал у двопроменевій моделі

$$r2_{nymu}(t) = \frac{\lambda}{4\pi}\left[\frac{\sqrt{G_l}u(t)e^{j(2\pi l/\lambda)}}{l} + \frac{R\sqrt{G_r}u(t-r)e^{j2\pi(r+r')/\lambda}}{r+r'}\right] * \cos(2\pi f_c t + \varphi_0),$$

де $r = (r + r' - l)/c$ — часова затримка відбитого від землі сигналу щодо складової прямого сигналу; R — коефіцієнт відбиття від землі; G_r — результат взаємодії полів з обліком діаграмам спрямованості передавальної й приймальні антен для r й r'. Якщо переданий сигнал є з вузькою смугою щодо тимчасової затримки $\tau \le B_u^{-1}$, то $u(t) \approx u(t-\tau)$.

Таким чином, потужність прийнятого сигналу для розглянутої моделі

$$P_r = P_t\left(\frac{\lambda}{4\pi}\right)^2\left|\frac{\sqrt{G_l}}{l} + \frac{R\sqrt{G_r}e^{j\Delta\varphi}}{r+r'}\right|^2, \qquad (3.33)$$

де $\Delta\varphi$ — різниця фаз між двома складовими прийнятого сигналу. Якщо d — відстань між антенами; h_t — висота передавальної антени; h_r - висота прийомної антени, то різниця фаз визначається як:

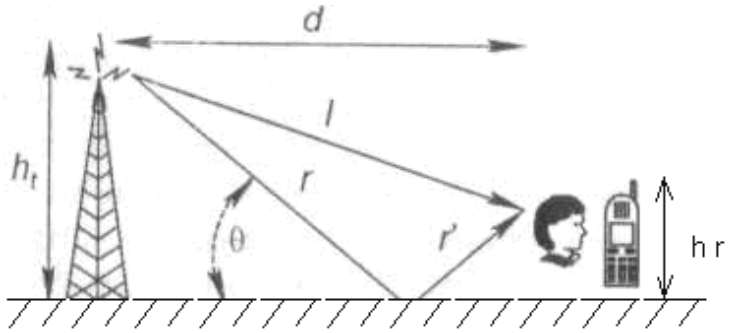


Рис. 3.2 Двопроменева модель поширення радіохвиль

$$\Delta\varphi = \frac{2\pi(r + r' - l)}{\lambda} = \frac{2\pi d}{\lambda}\left[\sqrt{\frac{(h_t + h_r)^2}{(d)^2} + 1} - \sqrt{\frac{(h_t - h_r)^2}{(d)^2} + 1}\right]. \qquad (3.34)$$

Як було відзначено раніше, рівняння (3.33) добре використовується з емпіричними даними. Розкид по затримці для двопроменевої моделі — це додаткова затримка при відбитті від землі $\tau = (r + r' - l)/c$. Коефіцієнт земного відбиття визначається

як:

$$R = \frac{\sin\theta - Z}{\sin\theta + Z},$$

де $Z = \sqrt{\varepsilon_r - \cos^2\theta/\varepsilon_r}$ $Z = \sqrt{\varepsilon_r - \cos^2\theta}$ - для вертикальної й горизонтальної поляризації відповідно.

r - діелектрична постійна поверхні, що для землі або дорожнього покриття приблизно дорівнює діелектричної постійної діелектрика (ε_r = 15).

Якщо d досить велике, те $r + r' - l \approx 2h_t h_r / d$, тоді

$\Delta\varphi \approx 4\pi h_t h_r / \lambda d$

Для великого значення d маємо $r + r' \approx l \approx d, 0 \approx 0, G_t \approx G_r$ й $R \approx -1$. Підстановка цих апроксимованих значень у вираження (3.33) показує, що потужність прийнятого сигналу приблизно становить:

$$P_r \approx \left(\frac{\lambda\sqrt{G_l}}{4\pi d}\right)^2 \left(\frac{4\pi h_t h_r}{d\lambda}\right)^2 P_t = \left(\frac{\sqrt{G_l} h_t h_r}{d^2}\right) P_t. \qquad (3.35)$$

Таким чином, при більших значеннях d потужність прийнятого сигналу зменшується обернено пропорційна четвертому ступеню d.

Апроксимація для критичної відстані d_c може бути отримана шляхом підстановки $\Delta\varphi$ замість π в (3.35), що дає $d_c = 4\pi h_t h_r / \lambda$. Отриманий параметр використається при побудові стільникових систем зв'язку для визначення оптимального розміру стільника.

Якщо взяти середнє від максимального й мінімального значень у вираженні (3.33), то отримані втрати потужності можуть бути апроксимовані шляхом розподілу кривих втрат потужності на дві області. Для $d < d_c$ середнє зменшення потужності за відстанню відповідає втратам у вільному просторі. Для $d \geq d_c$ зменшення потужності залежить від відстані, що описується законом зменшення обернено пропорційне четвертому ступеню від відстані (3.36).

Ці апроксимації лежать в основі спрощеної моделі для середнього значення прийнятої потужності (при цьому передбачається, що $G_l \approx G_r$ *):*

$$P_r = P_t G_t / L(d), \qquad (3.36)$$

Де $L(d) = (\frac{d}{d_0})^q \sqrt{1 + (\frac{d}{d_c})^{(m-2)q}}$ - являє собою лінійну апроксимацію зменшення потужності сигналу. Для цієї апроксимації m = 4, тобто має місце експонентне зниження потужності при більших d; d_0 — емпірична постійна; q — параметр, що визначає плавність зміни величини втрат на трасі в області переходу поблизу d_c.

3.2.3.2 Десятипроменева модель поширення радіохвиль

Десятипроменева модель застосовна для випадків поширення радіохвиль уздовж прямолінійних вулиць, на яких будинки розташовані по обидві сторони, і висотах передавальної і приймальні антен значно менші висоти будинків. Теоретично від будинків може відбиватися нескінченно велика кількість променів, які надходять на приймальну антену. Однак, оскільки частина енергії сигналу розсіюється при кожному відбитті, то шляхами поширення сигналів при трьох і більше числі відбиттів можна зневажити, якщо вулиця відносно пряма, при цьому відбиття у зворотну сторону звичайно малі й ними також можна зневажити.

Експериментальні дані показують, що модель із десятьма відбитими променями досить добре описує поширення сигналу через діелектричний ряд. Десять променів включають всі промені з одним, із двома або трьома відбиттями; зокрема, ураховується прямий промінь (ПП), промінь, відбитий від землі (ПВЗ), відбитий від однієї стіни (ОС), відбитий від двох стін (ДС), відбитий від трьох стін (ТС), відбитий від стіни й землі (СЗ), відбитий від землі й стіни (ЗС). Є два промені кожного типу з відбиттями від стін (по

одному для кожної сторони вулиці). Графічно (вид зверху) десятипроменевої моделі представлений на рис. 3.3.

У десятипроменевій моделі прийнятий сигнал визначається:

$$r_{10\,путей}(t) = \frac{\lambda}{4\pi}\left[\frac{\sqrt{G_l}\,u(t)e^{j(2\pi)/\lambda}}{l} + \sum_{i1}^{9}\frac{R_i\sqrt{G_{ri}u(l-\tau)e^{j(2\pi i)/\lambda}}}{r_i}\right], \qquad (3.37)$$

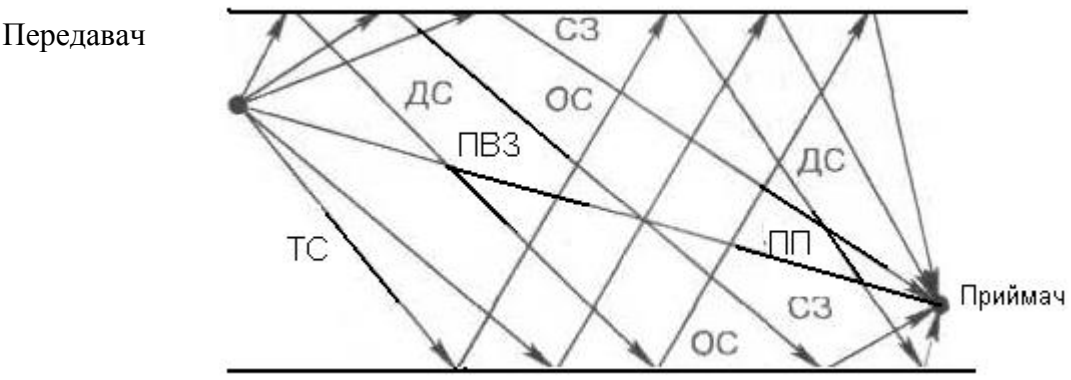


Рис. 3.3 Графічне зображення десятипроменевої моделі.

де r_i — довжина шляху і-го відбитого променя; $\tau_i = (r_i - l)/c$; G_{ri} — посилення приймальної антени, що відповідає і-му променю. Для кожного відбитого променя коефіцієнт буде являти собою коефіцієнт із одним відбиттям, що задає рівняння (3.35), або, якщо промінь відповідає декільком відбиттям, добутку коефіцієнтів, що відповідають кожному відбиттю. Діелектричні постійні, що використовувались у (3.35), приблизно такі ж, як і для землі, тому для обчислень R_i - беремо значення ε_r = 15. Якщо припустити, що $u(t) \approx u(t - \tau_i)$ для всіх *i,* тоді прийнята потужність:

$$P_r = P_t\left(\frac{\lambda}{4\pi}\right)^2\left|\frac{\sqrt{G_l}}{l} + \sum_{i1}^{9}\frac{\sqrt{G_{ri}e^{j\Delta\varphi_i}}}{r_i}\right|^2, \qquad (3.38)$$

де $\Delta\varphi_i = 2\pi(r_i - l)/\lambda$. Розкид по затримці для кожної моделі визначається рівним $\max_i\left[(r_i - l)/c\right]$.

Зменшення потужності з відстанню як для десятипроменевої моделі (3.36), так і для емпіричних моделей для міста за умови, що передавальні антени розташовані вище й нижче навколишніх будинків, звичайно пропорційно d^{-2} навіть на відносно великих відстанях. Зниження потужності обернено пропорційна квадрату відстані, що обумовлено перевагою променів, що загасають пропорційно d , у комбінації із променями, відбитими від землі (двопроменева модель), у яких загасання відбувається пропорційно d^{-4}. В інших

емпіричних дослідженнях дані про зниження потужності з відстанню пропорційно $d^{-\gamma}$, де γ перебуває в межах від 2 до 6.

3.2.3.3 Узагальнена модель поширення радіосигналів

Узагальнена модель поширення радіосигналів може використатися для прогнозування поля й затримки поширення для будь-яких конфігурацій будинків і при будь-якому розміщенні антен. Для цієї моделі необхідні точні дані про будинки (висота, місце розташування й діелектричних властивостей) і місцях розташування передавача й приймача щодо будинків. Узагальнена модель поширення радіосигналів може застосовуватися для розрахунків затримки й потужності сигналу при конкретній конфігурації передавач-приймач.

В узагальненій моделі поширення радіосигналів використовують методи геометричної оптики при визначенні напрямку поширення прямого сигналу й складових відбитого сигналу, а також складових сигналу, одержуваних у результаті переломлення й дифузійного розселення будинками.

Не існує межі для числа складових багатопроменевого сигналу в заданому місці розташування приймача; інтенсивність кожної складової обчислюють, виходячи з місця розташування будинків й їх діелектричних властивостей. Звичайно прямий і відбитий промені вносять певні складові в прийнятий сигнал. Однак у місцях, близько розташованих до поверхонь розсіювання або переломлення, які звичайно відділені від прямого й відбитого променів, ці складові можуть виявитися домінуючими.

Модель поширення для прямого й відбитого променів була розглянута раніше. Врахування дифракції на кутах дозволяє одержати досить точну модель, що описує механізм переломлення сигналів на кутах вулиць; разом з тим модель клиноподібної крайової дифракції краща завдяки своїй простоті. Геометричне подання крайової дифракції показане на рис. 3.4 Геометрична теорія дифракції дозволяє одержати наступний вираз для значень прийнятого сигналу:

$$r(t) = \frac{\lambda}{4\pi} u(t) D \frac{\sqrt{G_d e^{[2\pi(d+d')]/\lambda}}}{d'} \sqrt{\frac{d'}{d(d'+d)}} \cos(2\pi f_c t + \varphi_0).$$

де $\sqrt{G_d}$ — коефіцієнт підсилення антени; D — коефіцієнт переломлення, що залежить від поляризації сигналу, кута краю й кутів падіння й переломлення φ й φ'. Обчислення коефіцієнта переломлення звичайно здійснюється з використанням комп'ютера, разом з тим є й досить прості апроксимації.

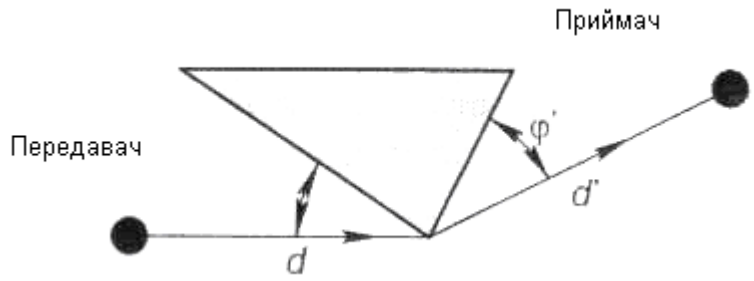


Рис. 3.4 Дифракція на клині.

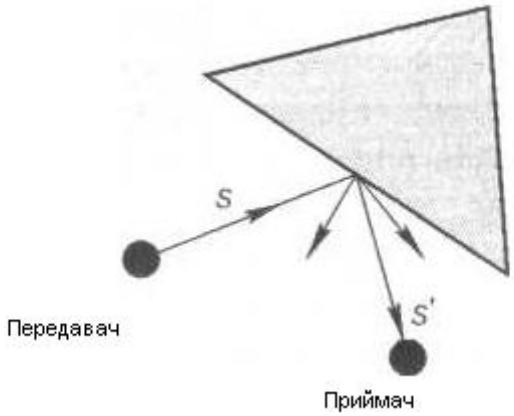


Рис. 3.5 Розсіювання

Розсіяний промінь, показаний на рис. 3.5 у вигляді сегментів s' й s, набуває втрат на трасі пропорційно відношенню s й s' . Така залежність обумовлена додатковими втратами на розходження пучка, які набуває промінь у результаті розсіювання. Прийнятий сигнал, що пройшов розсіювання, визначається з рівняння радіолокації:

$$r(t) = u(t)\frac{\lambda\sqrt{G_s}\sigma e^{j(2\pi(s+s'))/\lambda}}{4\pi s s'}\cos(2\pi f_c t + \varphi_0), \qquad (3.39)$$

де σ — ефективна площа об'єкта, що розсіює; G_s - коефіцієнт підсилення антени. Значення залежить від шорсткості, розміру й форми об'єкта, що розсіює. Є емпіричні значення для різних будинків.

Загальна величина електромагнітного поля в точці прийому визначається на основі врахування усіх складових, обумовлених багатопроменевим поширенням. Таким чином, якщо є прямий промінь, N_r відбитих, N_d переломлених й N_s дифузно розсіяних променів, то в цілому прийнятий сигнал з урахуванням (3.39):

$$r_{ообощ}(t) = \frac{\lambda}{4\pi}\left[\frac{\sqrt{G_l}u(t)e^{j(2\pi l)/\lambda}}{l} + \sum_{i=1}^{N_r}\frac{R_i\sqrt{G_{ri}}u(t-\tau_i)e^{(2\pi r_i/\lambda)}}{r_i} + \sum_{i=1}^{N_r}\frac{\sigma_i\sqrt{G_{si}}u(t-\tau_i)e^{j(2\pi(s_i+s_i^{'}))/\lambda}}{s_i s_i^{'}}\right]\times$$

$$\cos(2\pi f_c t + \varphi_0)$$

де τ_i — часова затримка конкретної складової багатопроменевого сигналу, а прийнята потужність $P_{ообощ}(t) = E\left|r_{ообощ}(t)\right|^2$.

Кожна зі складових багатопроменевого сигналу може мати додатковий коефіцієнт загасання, якщо шлях розповсюдження блокується будинками або іншими об'єктами. У цьому випадку коефіцієнт загасання перешкоди, що створює об'єкт, множиться на коефіцієнт, що відображає втрати на трасі поширення складової і сигналу. Ці втрати внаслідок загасання можуть змінюватися в широких межах залежно від матеріалу й розмірів об'єкта. У якості середньої емпіричної величини змін звичайно використовуються значення втрат через загасання рівне 12 Дб.

3.2.4 Емпіричні моделі

Більшість безпровідних систем зв'язку функціонують у складному середовищі поширення хвиль, що неможливо моделювати точно визначаючи траєкторію поширення променів і втрати на трасі поширення. Є ряд моделей визначення втрат на трасі для прогнозування загасання в типовому робітничому середовищі, наприклад для міських і приміських районів. Ці моделі головним чином засновані на даних емпіричних змін з урахуванням частотного діапазону й географічного району. Незважаючи на невисоку точність таких моделей, вони знаходять досить широке застосування.

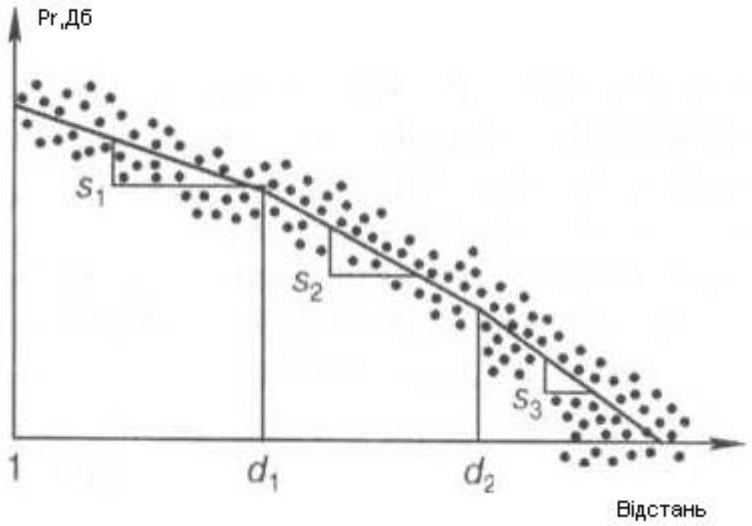


Рис. 3.6 Кусочно - лінійна модель для визначення втрат на трасі

3.2.4.1 Кусочно-лінійна апроксимація втрат на трасі поширення радіохвиль

Одним з відомих методів моделювання втрат на трасі є метод кусочно-лінійної апроксимації загасання, співвіднесеного з логарифмом відстані. Цей метод апроксимація пояснюється на рис. 3.6, де точки відображають гіпотетичні емпіричні дані вимірювань, а кусочно-лінійна модель відображає апроксимацію цих вимірів. Звичайно таку модель одержують на основі емпіричних вимірів, а потім застосовують до інших подібних умов навколишнього середовища. Кусочно-лінійна модель із N сегментами повинна відображати N — 1 точку переходу $d_1,...,d_{N-1}$ й нахили $s_1,...,s_{N-1}$ відповідному кожному сегменту. Двоінтервальна модель є частим випадком кусочно-лінійної моделі з однією крапкою переходу на критичній відстані $\log(4p_t h/\lambda)$ з нахилами s_1 = 20 й s_2 = 40. Для визначення кількості й місце розташування точок переходу, що підлягають використанню в моделі, можуть застосовуватися різні методи. Будучи зафіксованими, нахили, що відповідають кожному сегменту, можуть бути отримані за допомогою лінійної регресії. Кусочно-лінійна модель успішно застосовується для моделювання втрат всередині будинків.

3.2.4.2 Модель Окамури

Однієї з найпоширеніших моделей для прогнозування сигналу в міських умовах є модель Окамури. Ця модель часто застосовується для відстаней 1...100 км і частотного діапазону 150..1920 МГц (разом з тим вона добре екстраполюється для діапазону до 3 ГГц). Окамура використав виміри загасання сигналу при передачі від базової станції до мобільного для одержання ряду кривих, що дають середнє загасання відносно даних про поширення сигналу у вільному просторі на території з нерівною поверхнею Землі. Висоти базових станцій при цих вимірах були від 30 до 100 м, що перевищує звичайну висоту базових станцій, які використовуються у цей час. Формула Окамури для розрахунку середнього значення втрат поширення, Дб, на трасі має вигляд

$$L_{ср} = L_f + A_{ср}(f,d) - G(h_{БС}) - G(h_{АС}) - G_{НС}$$

де d — відстань між передавачем і приймачем; L_f — втрати у вільному просторі; $A_{ср}$ — середнє загасання відносно загасання у вільному просторі; $G(h_{БС})$ — висотний множник, що враховує висоту антени базової станції; $G(h_{АС})$ — висотний множник антени мобільної станції; $G_{НС}$ — коефіцієнт, що враховує тип навколишнього середовища. Значення $A_{ср}$ й $G_{НС}$ одержують із емпіричних графіків Окамури. Крім того, є формули для $G(h_{БС})$ й $G(h_{АС})$:

$G(h_{БС}) = 20\log(h_{БС}/200)$, $10\text{м} \prec (h_{БС}) \prec 1000$ м

$G(h_{AC}) = \begin{cases} 10\log(h_{AC}/3), \\ 20\log(h_{AC}/3), \end{cases}$ $h_{AC} \prec 3$ для першого випадку й $3\text{м} \prec h_{AC} \prec 10$ м для другого.

Є також поправочні коефіцієнти, що враховують характер місцевості і забезпечують підвищення точності моделі.

Модель Окамури звичайно має відхилення на 10...14 Дб між втратами на трасі, прогнозованими відповідно до моделі, і фактичними даними вимірів у міській і приміській стільникових мережах.

3.2.4.3 Модель Хата

Модель Хата є емпіричним зображенням графічних даних про втрати на трасі, що приводить Окамура, і справедлива приблизно для того ж діапазону частот. Ця емпірична модель спрощує розрахунок втрат на трасі, тому що являє собою завершену формулу, не основану на емпіричних кривих для різних параметрів. Стандартна формула для розрахунку середніх втрат на трасі у міському середовищі відповідно до моделі Хата має вигляд:

$$L_{город} = 69{,}55 + 16\log(f_c) - 13{,}83\log(h_{БС}) - a(h_{AC}) - [44{,}9 - 6{,}55\log(h_{БС})]\log(d).$$

Параметри в цій моделі такі ж, що в моделі Окамури, $a(h_{AC})$ поправочний коефіцієнт для висоти антени мобільної станції. Внесено певні зміни в модель для міста, а також у моделі поширення сигналів у приміських і сільських районах:

$$L_{пригород} = L_{город} - 2[\log(f_c/28)]^2 - 5{,}4$$

$$L_{село} = L_{город} - 4{,}78[\log(f_c)]^2 - 18{,}33[\log(f_c)] - 40{,}98$$

У моделі Хата не потрібно використання поправочних коефіцієнтів залежно від конкретної траси, як це має місце в моделі Окамури. Модель Хата добре апроксимує модель Окамури для відстаней d > 1 км. Таким чином, вона гарна для першого покоління стільникових систем, але не дозволяє моделювати з достатньою якістю сучасні стільникові системи з меншим розміром стільників.

Модифікована модель Хата

Модель Хата була розширена до 2 Ггц Європейською кооперацією на основі проведених науково-технічних досліджень (EURO-COST) у такий спосіб:

$$L_{город} = 46{,}3 + 3{,}9\log(f_c) - 13{,}82\log(h_{БС}) - a(h_{AC}) - [44{,}9 - 6{,}55\log(h_{БС})]\log(d) - C_{M.}$$

де $a(h_{AC})$—поправочний коефіцієнт, $C_{M.}$ = 0 дБ для міст середнього розміру, пригородів і 3 дБ для великих міст. Ця модель називається модифікованою моделлю Хата й

обмежується наступними граничними параметрами: 1,5 ГГц < f_c < 2 ГГц; 30 м < $h_{БС}$ < 200 м; 1 м < h_{AC} < Ю м; 1 км < d < 20 км.

3.2.4.4 Модель Уолфиша-Икегами

Модель Уолфиша-Икегами визначає медіанне значення втрат передач за формулі:

$$L_0 = L_1 + L_2 + L_3,$$

де $L_1 = 32.4 + 20\lg(Rf)$ — втрати при поширенні у вільному просторі; $L_2 = -16.9 - 10\lg(\omega)10\lg f(h_{d1} - h_{d2}) + L_p$ — втрати за рахунок відбиття від будинків; ω = *10... 15 м* — ширина вулиці; L_p — втрати, обумовлені орієнтацією вулиць щодо напрямку приходу сигналу.

$$L_p = \begin{cases} -10 + 0.35\varphi 0, якщо 0 \le \varphi \prec 35^\circ \\ 2.5 + 0.075(\varphi - 35^\circ), якщо 35^\circ \le \varphi \prec 55^\circ \\ 4.0 + 0.114(\varphi - 55^\circ), якщо 55^\circ \le \varphi \prec 90^\circ \end{cases}$$

де φ — орієнтація вулиці щодо напрямку приходу хвилі. $L_з = L_c + K_a + K_d \lg R + K_f \lg f - 9\lg d$,

де $L_c = \begin{cases} 18\lg(1 + (h_1 - h_{d1})), якщо h_1 \succ h_{d1} \\ 0, якщо h_1 \le h_{d1} \end{cases}$

h_{d1} — середня висота прилеглих до БС будинків; d — відстань між будинками

$$K_a = \begin{cases} 54, якщо h_1 \ge h_{d1}; \\ 54 - 0.8(h_1 - h_{d1}), якщо R \ge 0.5км (h_1 \le h_{d1}) \\ 54 - 0.4(h_1 - h_{d1}), якщо R \prec 0.5км (h_1 \le h_{d1}) \end{cases}$$

$$K_d = \begin{cases} 18, \_ якщо h_1 \succ h_{d1} \\ 18 - 15(h_1 - h_{d1}) / h_{d1}, якщо \_ h_1 \le h_{d1} \end{cases}$$

$K_f = \begin{cases} -4 + 0.7(f/925 - 1) \\ -4 + 1{,}5(f/925 - 1) \end{cases}$ для міста середніх розмірів або передмістя та для великого міста відповідно.

3.2.4.5 Модель Альсбрука і Парсона

Модель Альсбрука і Парсона дозволяє визначити основні втрати передачі в діапазоні (75...450) МГц у такий спосіб:

$$L = L_F + ((L_p - L_F)^2 + L_D^2)^{\frac{1}{2}} + L_B + \gamma,$$

де $L_F = 32.45 + 20\lg f + 20\lg R$ — втрати передачі у вільному просторі, дБ (f — робоча частота, МГц, R — відстань між антенами базової й мобільної станцій, км); L_D — дифракційні втрати, Дб, обумовлені характером місцевості під міською забудовою (сферичністю землі, наявністю пагорбів й т.п); L_p — втрати поширення над землею (при необхідності з урахуванням атмосферної рефракції), Дб. У більшості випадків L_p можуть бути обчислені за формулою:

$$L_p = 120 - 20\lg h_M - 20\lg h_B + 40\lg R$$

де h_M , h_B — висоти мобільної й базової антен, м. Втрати, викликані наявністю міської забудови, дб:

$$L_B = 20\lg(\frac{h_0 - h_M}{\sqrt{\lambda d}}) + 16,$$

де λ — довжина хвилі, м; d — ефективна ширина вулиці, на якій розташована мобільна антена, h_0 — середня висота будинків поблизу мобільної антени, м; γ — поправочний коефіцієнт, що залежить від частоти.

3.2.4.6 Модель Уолфица-Бертони

Модифікована модель Хата не враховує вплив дифракції від поверхонь дахів і будинків. Для врахування цих впливів була розроблена модель Уолфица-Бертони. У цій моделі при прогнозуванні середньої інтенсивності сигналу на рівні вулиці, враховується дифракція. Втрати на трасі розраховуються наступним чином:

$$L = P_0 Q^2 P_1$$

де P_0 —потужність сигналу на вході приймача при поширенні радіохвиль у вільному просторі для ненаправлених антен; Q - ураховує зниження потужності сигналу, обумовлене перешкодами у вигляді будинків, які затінюють приймач на рівні вулиці; P_1 - ураховує втрати сигналу через дифракцію. Модель прийнята для стандарту IMT-2000.

Є й інші емпіричні моделі для визначення втрат на трасі.

3.2.4.7 Модель Лі

Модель Ли була запропонована в 1982 р. У досить короткий час вона стала популярна серед дослідників і системних інженерів, оскільки параметри моделі можуть бути просто скореговані за допомогою додаткових вимірів до конкретних умов поширення. Після проведення цієї процедури прогнозування рівня сигналу стає досить точним. Більше того, алгоритм прогнозування простий для застосування. Багато систем мобільного зв'язку спроектовані із застосуванням цієї моделі (AMPS, DAMPS, GSM, IS-95).

Модель складається із двох частин. Перша частина (регіон-регіон) використана для прогнозування втрат при поширенні над відносно плоскою поверхнею без прийняття в увагу територіальних властивостей. Використання тільки цієї частини приводить до недостатньо точних результатів для горбкуватих регіонів. Друга частина (точка-точка) моделі Лі використовує результат, отриманий у першій частин, за основу й отримує більш точне значення. Заснована на даних профілю, поверхня другої частини моделі враховує умови прямої видимості. Якщо пряма видимість між приймачем і передавачем існує, те враховуємо вплив відбитих радіохвиль. Якщо умова прямої видимості не виконується, те моделюються дифракції радіохвиль як перешкоди на шляху розповсюдження сигналу.

Основна частина втрат при розповсюдженні на шляху сигналу може бути визначена наступною формулою:

$$P_r = P_{r0}(r / r_0)^{-\gamma}(f / f_0)^{-n}\alpha_0,$$

де P_r - потужність сигналу на відстані r від передавача, f - частота сигналу, P_{r0} - потужність сигналу у точці перетину лінії розповсюдження з перешкодою на відстані r_0 від передавача, γ - враховує ступінь кривизни поверхні, n – показує ступінь частотної залежності, α_0 - поправочний коефіцієнт, залежить від висоти розташування антен, потужності передавача, коефіцієнту посилення передавальної і приймальної антен.

Ця модель може використовуватися для загального випадку, коли радіохвилі розповсюджуються в різних умовах. В цьому випадку повинні буди відомі коефіцієнти кривизни поверхні γ_i і границі області з такими коефіцієнтами кривизни.

Дана модель дозволяє визначити потужність сигналу, що приймається:

$$P_{пр} = A - B\log R - n\log(\frac{f}{900}) + 10\log\alpha,$$

де A і B залежать від характеристик оточуючого середовища і були розраховані статистично по розрахункам в декількох містах. Для великих міст A=55…80, B==30…43. Для пригородів A=54, B=39. Множник n приймає наступне значення: n=2 для пригородів і для діапазону $f \prec 450 МГц$, n=3 для міст при $f \succ 450 МГц$. Параметр α розраховується наступним чином:

$$\alpha = \frac{h_b{}^2 h_M{}^m P_{перед} G_{перед} G_{прийм}}{3660},$$

де $P_{перед}$ - потужність передавача, Вт; $G_{перед}G_{прийм}$ - коефіцієнти підсилення антен,; h_b, h_M – висота антен мобільної і базової станцій; m=1 при $h_M \prec 3$ м і m=2 при $h_M \succ 10$ м.

3.2.4.8 Модель Кся-Бертолі

Ця модель дозволяє врахувати ряд додаткових параметрів, пов'язаних з кількістю поверхів, шириною вулиці і т.д. Це аналітична модель, розроблена для розрахунків загасань на трасах систем рухомого радіозв'язку у міських і приміських зонах. На відміну від статистичної моделі Хати, дозволяє вести розрахунки у більш широкому діапазоні частот (до 2200 МГц). Модель побудована на рівняннях хвильової оптики та розглядає різноманітні механізми розповсюдження радіохвиль в умовах міської забудови: розповсюдження радіохвиль у вільному просторі, дифракцію на краях дахів будинків, відбиття від стін будівель і т.д.

Коли антена БС розміщена вище середнього рівня дахів будинків, то з БС на МС припадає два проміні: один – у результаті дифракції на краях дахів будинків, другий – після відбиття від стін. Величина середніх втрат у цьому випадку:

$$L = -10\lg[(\frac{\lambda}{4\pi R})^2] - 10\lg[\frac{\lambda}{2\pi r}(\frac{1}{\theta} - \frac{1}{2\pi + \theta})^2] - 10\lg[2.35^2(\frac{\Delta h_b}{R}\sqrt{\frac{d}{\lambda}})^{1.8}],$$

де λ — довжина хвилі; R — відстань між БС и МС; $\Delta h_B = h_{BS} - h_0$ — різниця висот антени БС и середнього рівня дахів; $\theta = \tan^{-1}(\Delta h_M / x), \Delta h_M = h_0 - h_{MC}$ — різниця висот середнього рівня дахів і антени МС; x — відстань по горизонталі між МС та краєм даху, на якому хвиля піддається дифракції; звичайно $x = \omega/2$, де ω — середня ширина вулиць;

$r = \sqrt{\Delta h_M^2 + x^2}$, d — середній інтервал між кварталами.

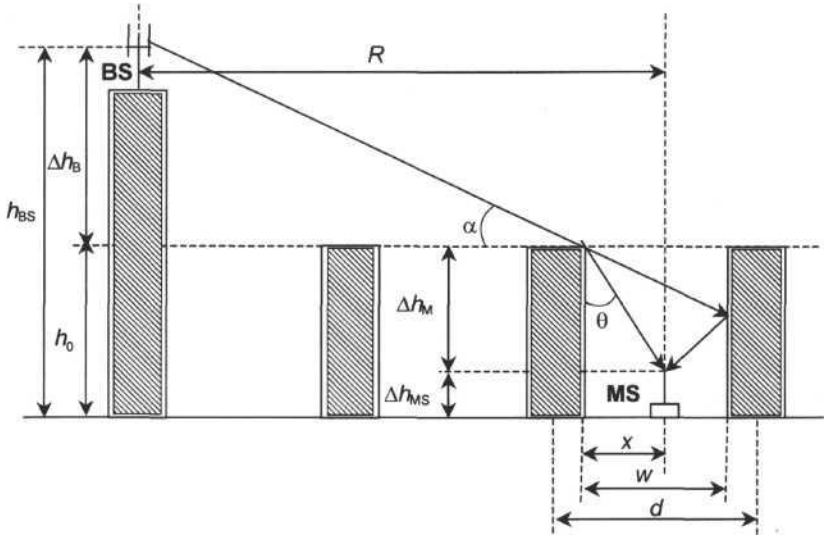


Рис. 3.7. Інтерференція променів у точці прийому

Модель Кся-Бертони дозволяє оцінити середній рівень втрат й у тих випадках, коли антена БС розташована на рівні дахів або нижче рівня дахів (такі прийоми використають, коли необхідно "засвітити" обмежену локальну область: площа, сквер і т.д.). У цих випадках вираження для величини загасання будуть наступні.

1. Антена BS на рівні дахів:

$$L = -10\lg\left[(\frac{\lambda}{2\sqrt{2}\pi R})^2 \right] - 10\lg\left[\frac{\lambda}{2\pi^2 r} (\frac{1}{\theta} - \frac{1}{2\pi + \theta})^2 \right] - 10\lg\left[(\frac{d}{R})^2 \right]$$

2. Антена BS нижче рівня дахів:

$$L = -10\lg\left[(\frac{\lambda}{2\sqrt{2}\pi R})^2 \right] - 10\lg\left[\frac{\lambda}{2\pi^2 r} (\frac{1}{\theta} - \frac{1}{2\pi + \theta})^2 \right] - 10\lg\left[(\frac{d}{2\pi(R-d)})^2 \frac{\lambda}{\sqrt{\Delta h_B^2 + d^2}} \left(\frac{1}{\varphi} - \frac{1}{2\pi + \varphi} \right) \right]$$

де $\varphi = \tan^{-1}(\Delta h_B / d)$

Незважаючи на те, що модель Кся-Бертони не враховує ряд важливих параметрів (вид будівельних матеріалів, різна орієнтація вулиць і т.п.), вона дає простий і зручний спосіб одержання попередніх оцінок рівня середніх втрат у каналі зв'язку.

3.2.4.9 Модель Егли

Іноді буває необхідно оперативно зробити розрахунок радіуса зони обслуговування системи для конкретного випадку положення БС на місцевості, робочої частоти й характеристик РЕС. Часто при цьому використається так називане модифіковане рівняння Egly**:**

$R_{90} = 10^{Eg}$,

де R_{90} - оцінка дальності прийому на рівні 90% надійності; $P_{перед}$ — потужність передавача БС; $G_{перед}$ — коефіцієнт підсилення антени БС; $G_{пр}$ — коефіцієнт підсилення антени МС; $L_ф$ — втрати у фідерних трактах приймального встаткування; $L_з$ — втрати компенсації завмирань; $L_ш$ - шумові втрати; $U_{пр}(P_{\min})$ — реальна чутливість приймача МС, Дб/Вт; f — робоча частота. Втрати на завмирання $L_З$ прийняті наступними, дБ:

- низькочастотна частина УКХ - діапазону 11
- високочастотна частина УКХ - діапазону 14
- діапазон 450 МГц 17
- діапазон 850 МГц 19.

3.2.5 Найпростіша модель визначення втрат на трасі

У зв'язку з тим, що потужність сигналу зменшується з відстанню, дуже важко одержати загальну модель, що охоплює всі особливості поширення сигналів у місті і приміській зоні. Використання моделей, що враховують траєкторії поширення радіохвиль, необхідні для одержання детальних апроксимацій значень потужності сигналу в точці прийому і важливі для визначення загальних характеристик системи, а також визначення найкращих місць розташування базових станцій. Однак при проведенні компромісного

експрес-аналізу різних варіантів побудови систем іноді зручніше використовувати просту модель, що враховує загальні особливості поширення сигналу, аніж використовувати складні моделі визначення втрат на трасі, що так чи інакше самі є апроксимацією реального каналу. Тому часто використається наступна спрощена модель для визначення втрат на трасі як функції відстані, у якій коефіцієнт втрат на трасі *y* звичайно перебуває в межах від 2 до 6 й є єдиним параметром:

$$P_r = P_t K (d_0 / d)^{\gamma}$$

де K -постійна, яка залежить від характеристики антен і середнього загасання, внесеного перешкодою; d_0 — еталонна відстань. Модель є справедлива тільки для відстаней $d_0 \prec d$.

Таким чином, оцінка зони радіо доступу з урахуванням різних факторів електродинаміки може виконуватися на основі:

- строгої теорії поля;
- наближених математичних виражень;
- великої кількості феноменологічних моделей і емпіричних формул, заснованих на статистичному підході. При проектуванні стільників мобільної мережі рівень сигналу в точці розташування мобільного термінала розраховується як різниця потужності, що випромінюється у напрямку МС, і втрат при поширенні радіосигналу.

У поточній главі було розглянуто велику кількість математичних моделей і методів, як правило емпіричних, що дозволяють робити розрахунок основних втрат при поширенні сигналу для різних умов поширення як для макростільника, так і для мікростільника. Серед цих моделей, що знайшли широке застосування на практиці, варто виділити моделі на основі Рекомендації № 370-5 МККР (CCI), моделі прогнозування втрат Альсбрука-Парсона, Окамури, Хата, Кся-Бертолі і ряд інших.

Отже, на розмір зони обслуговування впливають флуктуаційні шуми і взаємні перешкоди між станціями. Ці перешкоди нормують і враховують за допомогою наступних параметрів.

1. Мінімальна напруженість поля - рівень напруженості електромагнітного поля, необхідний для прийому із задовільною якістю в присутності шумів, але у відсутності взаємних перешкод

2. Необхідна напруженість поля - рівень напруженості електричного поля, який потрібний для прийому із заданою якістю в присутності шумів і взаємних перешкод на відстані R від БС. Поточне значення напруженості змінюється за випадковим законом, тому приблизно приймають, що на границі зони обслуговування поле, створюване передавачем, у часі змінюється мало, а зони обслуговування БС - перекриваються.

3.3 Застосування моделі Хата для моделювання технічних каналів витоку інформації в службових приміщеннях.

Зупинимось на більш детальному розгляді моделі, яка найбільше використовується на цей час, а саме Модель Хата. Існує декілька варіантів використання даної моделі з урахуванням розташування приймача і передавача, відстані між ними, а також в залежності від місцевості , в якій проводиться дослідження.

3.3.1 Модель Хата, зовнішньо-зовнішній зв'язок

$f_{розповс}(f, h_1, h_2, d, enn) = L + T(G(\delta))$, де:

L - втрати медіанного розповсюдження (дБ)

δ - стандартна девіація (дБ)

f - частота (МГц)

$H_m = \min\{h_1, h_2\}$

$H_b = \min\{h_1, h_2\}$

d - відстань, що повинна становити не більше 100 км

enn - сільська місцевість, населенні і густо населенні райони, розповсюдження вище або нижче рівня дахів.

Якщо H_m і/або H_b нижче 1м, то ми використовуємо значення, що дорівнює 1 м. Антена висотою вище ніж 200 м може привести до появи значних похибок. Розповсюдження нижче рівня дахів значить, що H_m і H_b вище рівня дахів. Розповсюдження вище рівня дахів у випадку, коли H_b також вище рівня дахів.

Розрахунок втрат медіанного розповсюдження L:

Перший випадок: $d \le 0.04$ км

$L = 34.2 + 20\log(f) \setminus +10\log(d^2 + (H_b - H_m)^2 / 10^6)$

Другий випадок: $d \ge 0.1$ км

$a(H_m) = (1.1 * \log(f) - 0.7)\min\{10, H_m\} - (1.56\log(f) - 0.8) | + \max\{0, 20\log(H_m / 10)\}$

$b(H_b) = \min\{0, 20\log(H_b / 30)\}$

$$a = \begin{cases} a = 1, d \le 20км \\ a = 1 + (0.14 + 0.000187f + 0.00107H_b) * (\log d / 20)^{0.8}, 20км \prec d \le 100км \end{cases}$$

Підпункт 1: населена місцевість

$30МГц \prec f \le 150МГц$

$$L = 69.6 + 26.2\log(150) - 20\log(150/f) - 13.82\log(\max\{30, H_b\}) + a[44.9 - 6.55\log(\max\{30, H_b\})]$$
$$\log(d) - a(H_m) - b(H_b)$$

$150МГц \prec f \leq 1500МГц$

$$L = 69.6 + 26.2\log(f) - 13.82\log(\max\{30, H_b\}) + a[44.9 - 6.55\log(\max\{30, H_b\})]$$
$$\log(d) - a(H_m) - b(H_b)$$

$1500МГц \prec f \leq 2000МГц$

$$L = 46.3 + 33.9\log(f) - 13.82\log(\max\{30, H_b\}) + a[44.9 - 6.55\log(\max\{30, H_b\})]$$
$$\log(d) - a(H_m) - b(H_b)$$

$2000МГц \prec f \leq 3000МГц$

$$L = 46.3 + 33.9\log(2000) + 10\log(f/2000) - 13.82\log(\max\{30, H_b\}) + a[44.9 - 6.55\log(\max\{30, H_b\})$$
$$\log(d) - a(H_m) - b(H_b)$$

Підпункт 2: слабо населена місцевість

$$L = L(населеної\_місцевості) - 2\{\log[\min\{\max 150, f\}, 2000\}/28]^2 - 5.4$$

Підпункт 3: відкритий простір

$$L = L(населеної\_місцевості) - 4.78\{\log[\min\{\max 50, f\}, 2000\}/28]^2 + 18.33*$$
$$\{\log[\min\{\max 50, f\}, 2000\}] - 40.94$$

Третій випадок: $0.04км \prec d \prec 0.1км$

$$L = L(0.04) + \frac{[\log(d) - \log(0.04)]}{[\log(0.1) - \log(0.04)]} * [L(0.1) - L(0.04)]$$

Коли L нижче рівня розсіювання у свободному просторі, то використовується значення, що дорівнює значенню розсіювання у свободному просторі.

Оцінка стандартного відхилення при нормальних умовах розповсюдження:

Перший випадок: $d \leq 0.04км$ $\delta = 3.5$ дБ

Другий випадок: $0.04км \prec d \prec 0.1км$

$\delta = 3.5 + \frac{(12 - 3.5)}{(0.1 - 0.04)}(d - 0.04)$ дБ розповсюдження понад дахами;

$\delta = 3.5 + \frac{(17 - 3.5)}{(0.1 - 0.04)}(d - 0.04)$ дБ розповсюдження нижче рівня дахів.

Третій випадок: $0.1км \prec d \prec 0.2км$

$\delta = 12$ дБ розповсюдження над дахами;

$\delta = 17$ дБ розповсюдження нижче рівня дахів.

Четвертий випадок: $0.2км \prec d \prec 0.6км$

$\delta = 12 + \frac{(9 - 12)}{(0.6 - 0.2)}(d - 0.2)$ дБ розповсюдження понад дахами;

$\delta = 17 + \frac{(4-17)}{(0.6-0.2)}(d-0.2)$ дБ розповсюдження нижче рівня дахів.

П’ятий випадок: $d \le 0.6км$

$\delta = 9$ дБ.

3.3.2 Сферична модель, зовнішньо - зовнішня

Сферична модель розповсюдження заснована на різновиді рекомендації ITU, у пунктах 452, 676 й 526 і використовується SEAMCAT для великих відстаней і значних частот.

Внаслідок сферичної дифракції (модель) застосовується здебільшого для Європи з використанням додаткових граничних станів.

Модель сферичної дифракції

У відповідності з рекомендаціями ITU (пункт 452) медіанні втрати між передавачем і приймачем розраховуються наступним чином:

$L_{bd}(p) = 92.5 + 20\log f + 20\log d + L_d(p) + A_o,$

$L_{bd}(p)$ - основні втрати в дБ, як функція процентного співвідношення

f - частота у ГГц

d - відстань у км

$L_d(p)$ - втрати дифракції в дб, як функція процентного співвідношення

A_o - розсіювання у атмосферних газах і рідинах. (дБ).

Розсіювання у атмосфері

$A_o = [\gamma_0(f) + \gamma_\omega(\rho, f)]d,$

де

$\gamma_0(f)$ - лінійне розсіювання у сухому повітрі (кисні) (дБ/км);

$\gamma_\omega(\rho, f)$ - лінійне розсіювання у воді, як функція концентрації.

Обидва значення можуть бути апроксимовані у відповідності до рекомендації ITU (пункт 676):

- розсіювання у воді:

$$\gamma_\omega(\rho, f) = [0.05 + 0.0021\rho | + \frac{3.6}{(f-22.2)^2 + 8.5} + \frac{10.6}{(f-183.3)^2 + 9} + \frac{8.9}{(f325.4)^2 + 26.3}]f^2 * \rho * 10$$

для $f \prec 350$ ГГц;

- розсіювання у повітрі:

$$\gamma_0(f) = [7.19 * 10^{-3} + \frac{6.09}{(f^2 + 0.277)} + \frac{4.81}{(f-57)^2 + 1.5}]f^2 * 10^{-3} \qquad f \le 57 \text{ ГГц;}$$

$$\gamma_0(f) = 10.5 + 1.5(f-57) \qquad 57 \prec f \le 60 \text{ ГГц;}$$

$\gamma_0(f) = 15 - 12(f - 60)$ $\qquad 60 \prec f \le 63$ ГГц;

$$\gamma_0(f) = [3.79 * 10^{-7} + \frac{0.265}{(f-63)^2 + 1.59} + \frac{4.81}{(f-118)^2 + 1.47}](f + 1.98)^2 * 10^{-3} \qquad f \succ 63$$

ГГц.

Примітка: для полегшення використання даних формул беремо лінійну інтерполяцію між 57 і 63 ГГц. Максимальні значення 15дБ/км для 60 ГГц.

Розсіювання внаслідок дифракції

У відповідності до рекомендацій ITU (пункт 526), дифракційні втрати $L_d(p)$ можуть відбуватися від використання E_0 (відкритий простір замість отриманого значення напруженості поля E):

$$-L_d(p) = 20\log\frac{E}{E_0} = F(x) + G(Y_1) + G(Y_2),$$

де

x - нормалізований радіоканал передавач-приймач;

Y_1 - нормалізована висота антени передавача;

Y_2 - нормалізована висота антени приймача.

$$x = 2.2\beta * f^{\frac{1}{3}} a_e^{-\frac{2}{3}} d;$$

$$Y = 9.6 * 10^{-3} \beta * f^{\frac{2}{3}} a_e^{-\frac{1}{3}} h_i,$$

де β - параметр, що походить від пропускної здатності Землі:

$\beta = 1$ для $f \succ 20$ МГц

f - частота;

a_e - еквівалент радіуса Землі у км;

d - розсіювання в км;

h_i - висота антени над в метрах с i=1 або 2 для передавача або приймача, відповідно.

Визначення $F(x)$, залежить від відстані , що розраховується за допомогою двояко-емпіричної формули: $F(x) = 11 + 10\log(x) - 17.6x$

$G(Y) = 17.6(Y - 1.1)^{1/2} - 5\log(Y - 1.1) - 8$ для $Y \succ 2$

$G(Y) = 20(Y + 0.14^3)$ для $10k \prec Y \prec 2$

$G(Y) = 2 + 20\log k + 9\log(4/k)[\log(Y/k) + 1]$ для $k/10 \prec Y \prec 10k$

$G(Y) = 2 + 20\log k$ для $Y \prec k/10,$

де k - нормалізована пропускна здатність поверхні Землі, початкове значення: 10^{-5}

Часова залежність втрат

Ця різноманітність втрат забезпечується варіаціями еквівалента радіусу Землі a_e (км), котрий вважається залежним від часового відсоткового співвідношення:

$a_e(p) = 6375k(p)$

$k(p)$ можна розрахувати наступним чином:

$$k(p) = k_{50} + (5 - k_{50}) * \frac{(1.7 - \log p)}{(1.7 - \log \beta_0)} \qquad \text{для} \qquad p \prec 50\%$$

$k(p) = k_{50}$ для $p \succ 50\%$

й $k_{50} = \frac{157}{157 - \Delta N}$, де

ΔN - значення градієнта заломлення на висоті 1 км, воно завжди позитивне

β_0 - вірогідність співіснування значно заломлюючого шару ($\Delta N \succ 100\_од/км$) в низах атмосфери (%).

Сфери використання

- Діапазон частот має бути більше 3 ГГц, починаючи з низьких частот, але не нижче 300 МГц у відповідності з пропускною здатністю поверхні і ефекту поляризації.

- Модель була розроблена для відкритої місцевості. Проте додаткові фактори розсіювання не включені для міських просторів.

- Втрати із-за дощу не враховуються.

- Ця модель може використовуватися тільки для територіального зв'язку.

Більшість моделей розповсюдження, опублікованих у загальнодоступній літературі, передбачені для сугубо внутрішнього і зовнішнього застосування. Але у реальних умовах нам потрібно комбінувати обидва різновиди.

В SEAMCAT класичні моделі (Хата і сферична) комбінуються з моделлю внутрішнього розповсюдження (COST 231).

3.3.3 Комбінація різних сценаріїв розповсюдження

Втрати при передачі P_L складаються з: втрат медіанного розповсюдження L і розподілення Гаусса $T(G(\delta))$, де δ - стандартна девіація.

$P_L(f, h_1, h_2, d, enn) = L + T(G(\delta))$,

де:

f - частота в мегагерцах;

h_1 - висота антени передавача (м);

h_2 - висота антени приймача (м);

d - відстань (м);

enn - параметр оточуючого середовища передавача і приймача.

Зовнішньо-зовнішній сценарій

- Приймач і передавач знаходяться поза будівлею.
- Змінена модель Хата.

Медіан: $L(зовнішньо-зовнішнє)=L_{хата}(зовнішньо-зовнішнє)$

Розподілення дійсне, $\delta(зовнішньо-зовнішнє)=\delta_{хата}$

- Сферична модель дифракції:

Медіан: $L(зовнішньо-зовнішнє)=L_{сферичне}$

Розподілення недійсне, $\delta(зовнішньо-зовнішнє)=0$

Внутрішньо - зовнішнє, зовнішньо - зовнішнє

- приймач знаходиться у приміщенні, а передавач зовні або навпаки
- змінена модель Хата

Медіан: $L(внутрішньо-зовнішнє)=L_{хата}(зовнішньо-зовнішнє)+L_{ωe}$, де

$L_{ωe}$ - розсіювання стін

Розподілення: $\delta(внутрішньо-внутрішнє)=\sqrt{\delta_{хата}^2+\delta_{add}^2}$, де

δ_{add} - додаткова стандартна девіація сигналу

Сферична модель дифракції

Медіан: $L(внутрішньо-внутрішнє)=L_{сферичне}+L_{ωe}$

Розподілення: $\delta(внутрішньо-внутрішнє)=\delta_{add}$

Нормальне розподілення може визначатись додатковими параметрами із-за неоднорідності будівельних матеріалів, і тільки для сферичної дифракції це не має значення.

Внутрішньо-внутрішнє

Існує дві можливості розвитку подій: приймач і передавач знаходяться в одному або різних приміщення, тому вибір подіє залежить від наступних умов.

Вибір події

По-перше визначається де знаходиться приймач, а де передавач. Це відбувається за допомогою розрахунків випадкового параметра SB (Same Building)

Визначення SB:

$*\ d \prec 0.020$ км; $SB=Yes \Rightarrow P(Yes)=1$

$*\ 0.020 \prec d \prec 0.05$км; $\begin{array}{l} SB=Yes \Rightarrow P(Yes)=(0.05-d)/0.03 \\ SB=No \Rightarrow P(No)=1-p(Yes)=(d-0.0)/0.03 \end{array}$

$*\ d \succ 0.05$км; $SB=Yes \Rightarrow P(Yes)=0$

Внутрішньо-внутрішнє, різні будівлі

- передавач й приймач знаходиться в різних будівлях

$P(Yes) = 0$ або $P(No) = 1$

- змінена модель Хата:

Медіан: $L(внутрішньо - внутрішнє) = L_{хата}(зовнішньо - зовнішнє) + 2L_{ωe}$

Останній параметр значить, що ми враховуємо втрати із-за двох внутрішніх стін.

Розподілення: $\delta(внутрішньо - внутрішнє) = \sqrt{\delta_{хата}^2 + \delta_{add}^2}$

Сферична модель дифракції

Медіан $L(внутрішньо - внутрішнє) = L_{сферичне} + 2L_{ωe}$

Розподілення: $\delta(внутрішньо - внутрішнє) = \sqrt{2\delta_{add}}$

Нормальне розподілення може визначатися додатковими параметрами із-за неоднорідності будівельних матеріалів і тільки для сферичної дифракції це не має значення. Розподілення звужується із-за наявності в розрахунках ще однієї зовнішньої стіни.

$P(Yes) = 1$ $P(No) = 0$

Модель розподілення усередині:

Медіан:

$$L(внутрішньо - внутрішнє) = -27.6 + 20\log(1000d) + 20\log(f) + fix(\frac{1000d}{d_{кімнати}}) * L_{ωi} +$$

$$+ k_f^{(\frac{k_f+2}{k_f+1} - b)} * L_f$$

$$k_f = fix(\frac{|n_2 - n_1|}{h_{підлоги}})$$

$L_{ωi}$ - втрати за рахунок внутрішніх стін (середнє значення 5 Дб)

L_f - втрати проникнення скрізь підлогу (середнє значення 18,3 Дб)

b - емпіричний параметр (середнє значення 0,46)

$d_{кімнати}$ - розмір кімнати (середнє значення 4м)

$h_{підлоги}$ - висота стелі (середнє значення 3м)

Розподілення:

$\delta(внутрішньо - внутрішнє) = \delta_{in}$ (середнє значення δ_{in} =10Дб)

Нормальне розподілення залежить від усіх параметрів приміщень (архітектура, розташування меблів і т.д.)

Таким чином, враховуючи вищенаведений матеріал, можемо побудувати модель втрат розповсюдження для адміністративного приміщення з урахуванням моделей COST 231 і модифікованої моделі Хата.

Відомо, що досліджувана модель розподілення знаходиться усередині приміщення, тобто приймач і передавач знаходяться в одному приміщенні. Отже, маємо:

$$L(внутрішньо-внутрішнє) = L_{fc} + L_c + fix(\frac{1000d}{h_{кімнати}})L_{\omega i} + k_f{}^{(\frac{k_f+2}{k_f+1}-b)} * L_f,$$

где L_{fc} - втрати у свобідному просторі; L_c - постійні втрати; $k_f = fix(\frac{|h_2 - h_1|}{d_{кімнати}})$ - і; h - кількість подоланих стін на шляху розповсюдження; $L_{\omega i}$ - втрати у стіні типу і; L_f - втрати між суміжними поверхами; $h_{кімнати}$ - висота кімнати, $d_{кімнати}$ - розмір кімнати, *b*- емпіричний параметр.

Відомо, що у вільному просторі потужність електромагнітних хвиль зменшується як відстань у квадраті між передавачем і приймачем або $1/d^2$. У лінійній формі, загасання у вільному просторі описується формулою:

$$L_{fc} = \frac{\lambda^2}{4\pi d^2}$$

Рівняння може бути також записано у логарифмічній формі:

$$L_{fc} = -32{,}4 - 20\log(d) - 20\lg(f),$$

де L_{fc} - втрати у свобідному просторі; d - відстань між передавачем і приймачем, у км; f - частота сигналу, в МГц,

Для більшості випадків з урахуванням усіх параметрів $L(d, L_{fc}, L_c, L_{\omega i}, h)$ можемо усереднити, що значення $L_c = 35-37$ дБ. $L_f = 18.3$ дБ при звичній структурі поверхів (підходить для більшості офісних приміщень), $L_{\omega i} = 3.4$ дБ для легких внутрішніх стін (вікна, дошка, гіпсокартон) і $L_{\omega i} = 6.9$ дБ (для бетону, цегли).

З урахуванням усіх факторів можемо зазначити, що:

$$L(d) = 37 + 20\lg d + 10\lg f + 18.3 * h^{(\frac{h+2}{h+1}-0.46)}$$

Таким чином, визначимо декілька значень $L(d)$ для частот та найбільш вживані для приміщення , що має спеціальне призначення.

1. Для частоти $f = 50\_МГц$, для кількості подоланих стін на шляху розповсюдження радіохвилі $h = 3$ і для відстані від передавача до радіо закладного пристрою в $d = 25\_м$ маємо: $L = 33.923$ Дб.

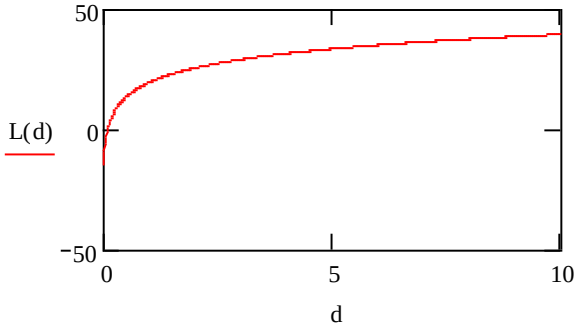


Рис. 3.8 Залежність затухання розповсюдження радіосигналу від відстані.

2. Для частоти $f = 400\_МГц$, для кількості подоланих стін на шляху розповсюдження радіохвилі $h = 3$ і для відстані від передавача до радіо закладного пристрою в $d = 25\_м$ маємо: $L = 42.953$ Дб.

Отже, маємо можливість розраховувати у заданому приміщенні на будь-яку відстань, для любої частоти і кількості стін затухання сигналу; це дозволяє з допустимою похибкою розраховувати можливі втрати корисного сигналу, а також визначати відсоток можливого перехоплення корисної інформації при наявності будь-яких радіо закладних пристроїв у приміщенні спеціального призначення.

Розділ 4. Пристрої і системи технічної розвідки

4.1. Загальна інформація

Бурхливий розвиток техніки, технології, інформатики в останні десятиліття викликав ще більш бурхливий розвиток технічних пристроїв і систем розвідки. Справді, занадто часто виявлялося вигідніше витратити N-у суму на добування, наприклад, технології, що вже існує, ніж у декілька разів більшу на створення власної. А в політиці чи у військовій справі виграш іноді виявляється просто безцінним. У створення пристроїв і систем ведення розвідки вкладалися і вкладаються величезні кошти у всіх розвинутих країнах. Сотні фірм багатьох країн активно працюють у цій галузі. Серійно виробляються десятки тисяч моделей "шпигунської" техніки. Ця галузь бізнесу давно і стійко зайняла своє місце в загальній системі економіки Заходу і має міцну законодавчу базу. У західній пресі можна знайти дуже захоплюючі документи про існування і роботу міжнародної організації промислового шпигунства "Спейс Інкорпорейтед", а також познайомитися зі спектром послуг, пропонованих цією компанією. Так, англійська газета "Піпл" повідомляє, що серед клієнтів компанії є не тільки промисловці, але й організовані злочинні угруповання. Як і будь-який бізнес, коли він вигідний, торгівля секретами розширює область діяльності, знаходячи для свого процвітання вигідний ґрунт. Так, в Ізраїлі, за прикладом США, починають відноситься до ведення розвідки в економічній області як до вигідного бізнесу. Як підтвердження можна привести факт створення колишнім прес-секретарем ізраїльської армії Ефраїмом Лапідом спеціалізованої фірми "Іфат", що займається збором й аналізом інформації, яка могла б зацікавити різних замовників (у тому числі й міністерство оборони). На думку Е. Лапіда, Ізраїль, який відрізняється великим спектром міжнародних зв'язків, вибором іноземної преси і вдалим геополітичним положенням, є "зручною" державою для організації і ведення "бізнесу-розвідки". Французький журнал ділових кіл "Антреприз" так характеризує національні риси промислового шпигунства: "... найбільш агресивними є японці. Шпигунство на Сході носить систематичний і централізований характер. Що стосується американців, то вони приділяють значну частину свого часу взаємному шпигунству..." Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно орієнтуючись на найбільше фінансово вигідні. У Росії після 1917 року ведення комерційної розвідки знаходилося під суворим контролем держави. У Радянському Союзі в цій області були зосереджені чудові, якщо не сказати кращі, фахівці. Видатним досягненням було і залишиться на багато років диво технічної розвідки - будинок посольства США в Москві, перетворене у величезне "вухо", у якому кожен подих, кожен шерех був доступний для запису й аналізу. Датчики знаходили навіть у зварених сталевих конструкціях будинку, причому по щільності матеріалу вони відповідали навколишньому

металу і були недоступні для рентгенівського аналізу. Ці системи були здатні функціонувати автономно десятки років. Американці змушені були відмовитися від використання цього будинку, навіть незважаючи на те що колишній глава КДБ Вадим Бакатін передав їм схему побудови цієї системи [1].

Катастрофа СРСР і розвиток вільної ринкової економіки відродили попит на техніку подібного роду. Фахівці військово-промислового комплексу, що залишились без роботи, не перестали запропонувати свої послуги у цій області. Спектр послуг широкий: від примітивних радіопередавачів до сучасних апаратно-програмних комплексів ведення розвідки. Звичайно, в Росії та Україні немає ще великих фірм, що роблять техніку подібного роду, немає і такого достатку моделей, як на Заході, але техніка наших виробників цілком порівнянна за своїми характеристиками з аналогічною західною, а іноді краще й дешевше. Зрозуміло, мова йде про порівняння техніки, що є у відкритому продажу. Природно, апаратура, використовувана спецслужбами (її кращі зразки), набагато перевершує за своїми можливостями техніку, використовувану комерційними організаціями. Як приклад можна привести найменший і найдорожчий у світі радіомікрофон, габарити якого не перевищують чверті олівцевої гумки. Цей мініатюрний передавач живиться від ізотопного елемента і здатний протягом року сприймати і передавати на приймальний пристрій, розташований у півтора кілометрах, розмову, що ведеться в приміщенні пошепки. Крім того, вже зараз виробляються "клопи", що можуть записувати перехоплену інформацію, зберігати її протягом доби чи тижня, передати в режимі швидкодії за мілісекунду, стерти запис і почати процес знову.

У вже згадуваному новому будинку американського посольства елементи радіозакладок були розосереджені по бетонних блоках, представляючи собою кремнієві вкраплення. Арматура використовувалася як провідники, а порожнечі – як резонатори й антени. Аналізуючи досвід розвитку подібної техніки, можна зробити висновок, що можливість її використання комерційними організаціями є тільки справою часу. Виділимо основні групи технічних засобів ведення розвідки [2].

Радіопередавачі з мікрофоном (радіомікрофони):

- з автономним живленням;
- з живленням від телефонної лінії;
- з живленням від електромережі;
- керовані дистанційно;
- які використовують функцію включення за наявністю голосу;
- напівактивні;
- з накопиченням інформації і передачею в режимі швидкодії .

Електронні "вуха":

– мікрофони з проводами;
– електронні стетоскопи (що прослухують через стіни);
– мікрофони з гострою діаграмою спрямованості;
– лазерні мікрофони;
– мікрофони з передачею через мережу 220 В;
– прослуховування через мікрофон слухавки;
– гідроакустичні мікрофони.

Пристрої перехоплення телефонних повідомлень:

– безпосереднього підключення до телефонної лінії;
– підключення з використанням індукційних датчиків (датчики Хола й ін.);
– з використанням датчиків, розташованих всередині телефонного апарата;
– телефонний радіоретранслятор;
– перехоплення повідомлень стільникового телефонного зв'язку;
– перехоплення пейджерних повідомлень;
– перехоплення факсів-повідомлень;
– спеціальні багатоканальні пристрої перехоплення телефонних повідомлень.

Пристрої прийому, запису, керування:

– приймач для радіомікрофонів;
– пристрої запису;
– ретранслятори;
– пристрої запису і передачі в прискореному режимі;
– пристрої дистанційного керування.

Відео системи запису і спостереження.

Системи визначення місце розташування контрольованого об’єкта.

Системи контролю комп’ютерів і комп’ютерних мереж.

Далі розглянемо основні характеристики технічних засобів ведення розвідки.

4.2. Радіомікрофони

Радіомікрофон, як випливає з назви, це мікрофон, об'єднаний з радіо, тобто з радіоканалом передачі звукової інформації. В даний момент немає сталої назви цих пристроїв. Їх називають радіозакладками, радіобагами, радіокапсулами, іноді - "жучками", але все-таки самою точною назвою варто визнати назву, винесену як заголовок даного розділу. Радіомікрофони є найпоширенішими технічними засобами ведення комерційної розвідки. Їхня популярність пояснюється насамперед зручністю їх оперативного використання, простотою застосування (не потрібно тривалого навчання персоналу), дешевиною, дуже невеликими розмірами. У найпростішому випадку радіомікрофон

складається з власне мікрофона, тобто пристрою для перетворення звукових коливань в електричні, та радіопередавача – пристрою, що випромінює в простір електромагнітні коливання радіодіапазону (несучу частоту), модульовані електричними сигналами з мікрофона. Мікрофон визначає зону акустичної чутливості (звичайно вона коливається від декількох до 20-30 метрів), радіопередавач – дальність дії радіолінії. Визначальними параметрами з погляду дальності дії для передавача є потужність, стабільність несущої частоти, діапазон частот, вид модуляції. Істотний вплив на довжину радіоканалу робить, звичайно, і тип радіоприймального пристрою.

На приймальних пристроях ми зупинимося, хоча і коротко, пізніше. Пристрій керування не є обов'язковим елементом радіомікрофона. Він призначений для розширення його можливостей: дистанційного вмикання-вимикання передавача, мікрофона, пристрою запису, перемикання режимів. Можуть бути передбачені режими: включення за наявністю голосу, режим запису в реальному часі, режим прискореного відтворення і т.д. Пристрій запису, як випливає зі сказаного вище, також не є обов'язковим елементом. Розроблено і випускаються серійно сотні моделей радіомікрофонів, у тому числі не менш ста типів – у Росії, Україні й Білорусії. Технічні дані радіомікрофонів знаходяться в наступних межах[2]:

- маса від 5 до 350 г
- габарити від 1 см3 до 8 дм3
- частотний діапазон від 27 до 2000 МГц
- потужність від 0,2 до 500 мВт
- дальність без ретранслятора від 10 до 1500 м
- час безупинної роботи від декількох годин до декількох років.

Взагалі провести класифікацію радіо мікрофонів можна за багатьма ознаками, такими як :

- Технологія виготовлення (дискретна, інтегральна ,гібридна)
- Ступінь складності(прості, складні)
- Місце установки(в приміщенні, будівлі, електромережі, електро та радіоприладах, телефонних апаратах)
- Тип джерела живлення (автономне, електромережа ,телефонна мережа)
- Спосіб передавання інформації (радіо каналом ,спеціальними лініями , існуючими лініями ,електромережею , телефонною лінією , трубами та елементами конструкцій будівель ,накопичення інформації без передавання .)
- Конструкторське виконання (камуфльовані , окремі модулі)
- Спосіб управління (без керування , з акустичним автоматом ,такі що керуються дистанційно . які керуються за програмою)

- Тип датчика (мікрофонний , вібраційно контактний)
- Вид модуляції(аналогова .імпульсна ,цифрова, комбінована)
- Дальність передавання інформації(локальна, необмежена).
- Довжина хвиль, які використовуються для передавання(декаметрові(ВЧ), метрові(ДВЧ), дециметрові (УВЧ),
- Потужність випромінювання(мала(до 10мВт), середня(до 100мВт), велика(більше 100мВт))
- Вид модуляції(проста(АМ,ЧМ,ФМ), імпульсна(АІМ,ШІМ,ФІМ), цифрова, складна(шумоподібна, з псевдо випадковою перебудовою частоти)
- Спосіб модуляції сигналу(безпосередня модуляція несучої частоти, модуляція проміжної частоти)
- Стабілізація частоти(без стабілізації, схемотехнічна стабілізація, стабілізація за допомогою кварцу)
- Режим роботи передавача(безперервний, робота на коротких часових інтервалах, робота за заданим алгоритмом)
- Дистанційне управління (з дистанційним та без дистанційного управління)
- Маскування сигналу передавача(без маскування, маскування під сигнали радіомовлення ,маскування під сигнали РЛС та радіонавігаційних систем)
- Закриття інформації, яка передається(без закриття, аналогове скремблювання , цифрове шифрування, застосування складних видів модуляції)

Отже, якщо порівняти радіо закладку з апаратурою зв’язку то можна виділити низку її особливостей :

- Мініатюрність;
- Мала потужність і ,як наслідок, обмежений радіус дії,
- Симплексний режим роботи від джерела до одержувача повідомлення;
- Постійний вид сигналу;
- Мала кількість каналів ;
- Простота протоколу входження у зв'язок ;
- Робота на одній частоті (зрідка на двох);
- Наявність конструктивного маскування.

З останніх розробок найкращі характеристики мають закладки з сигналами схожими на шуми . Наприклад закладки :

-COF-335(діапазон частот (890-980)МГц, ширина смуги 8МГц, вид модуляції BPSK, потужність 100МВт)

-PR-9000P(діапазон частот (400-500)МГц, ширина смуги 5МГц, вид модуляції BPSK, потужність 100МВт, є дистанційне керування) .

Існують також закладки, які працюють в режимі накопичування та прискореного передавання . Наприклад закладка РЗУ-1 ,яка працює в діапазоні (300-1000)МГц, потужність 200мВт ,вид модуляції імпульсний цифровий потік, час запису інформації 6 годин ,час швидкісного передавання 10 хвилин, дальність дії 200м, є дистанційне керування.

Більш докладні дані по конкретних моделях наведено в табл. 4.1[2]. Як видно з даної таблиці, дальність дії, габарити і час безупинної роботи знаходяться в дуже тісній залежності одне від одного. Справді, для збільшення дальності необхідно насамперед підняти потужність, одночасно зростає струм, споживаний від джерела живлення, що швидше витрачає свій ресурс, а виходить, скорочується час безупинної роботи. Щоб збільшити цей час, збільшують ємність батарей живлення, але це збільшує габарити радіомікрофона. Можна збільшити тривалість роботи передавача введенням у його склад пристрою дистанційного керування (вимикання-вмикання-вимикання), однак це також збільшує габарити. Крім того, потрібно мати на увазі, що збільшення потужності передавача полегшує можливість його виявлення.

Таблиця 4.1.

Технічні дані радіомікрофонів промислового виготовлення

Модель	Габарити	Тип живлення, напруга	Вага	Тип корпуса	Дальність дії	Канали	Час роботи	Додаткові дані
СА-201	128х70х18	Лужн.бат. АМ-3 (1,5У)х2	100г	Закамуфльований під калькулятор	100-200 м	3(А,В,С)	150 годин	Вбудований високочутливий мікрофон. Можна одночасно користатися калькулятором
DX-400	84х56х22 мм	Літієва бат. 2СВ-5 (6В)х1	130г	Пластмасовий прямокутний корпус	1000-1500	3(А,В,С)	15 годин	Мікрофон у вигляді шпильки для краватки передає звук і переривчастий тональний сигнал
ТК-400	166х27х 14мм	Літієва бат. СВ-12600SE	52г	Пластмасовий прямокутний	1500-1000	3(А,В,С)	130 годин	Забезпечують висока якість звуку
ТК-400М	аналогічно ТК-400	аналогічно ТК-400	52г	Аналогічно ТК-400	500-1000 м	3(А,В,С)	130 годин	Мікрофон у вигляді шпильки для краватки, зовнішній мікроскопічний мікрофон,

								мікрофон у вигляді голки
CA-205	180x135x 40мм	Мережа 220В та акуму. бат.	350г	Настільний калькулятор	100-200 м	3(A,B, C)	не обмеж.	12-разрядний калькулятор і мікрофон можуть працювати одночасно
N-110N-2	62x18x9 мм	мережа 110В мережа 220В	20г	Пластма-совий	100-200 м	3(A,B, C)	не обмеж.	Таємний секретар. Схований передавач з живленням від мережі змінного струму. Найбільш зручно помістити в сполучену настінну розетку
РК-ЗОО	Довжина 130 мм	батареї SR-48W бат. (1.5В)х2	120г	Авторучка	100-200 м	3(A,B, C)	15 годин	Одна з найбільш цікавих моделей. Ручкою можна користуватися не викликаючи підозр.
CD-500S	86x545 x4.5мм	Літієва бат CR-2430(3В)	20г	Кредитна картка	200-300 м	3(A,B, C)	30 годин	Плоский, як кредитна карта, передавач. Легко використовувати при будь-яких обставинах.
AZ-110A	70x35x20 мм	Від мережі 110 чи 220 В	45г	Трійник-подовжувач для побутових апаратів	100-200 м	3(A,B, C)	не обмеж.	Працює від мережі змінного струму й одночасно використовуєть-ся як трійник для побутової апаратури.

Наявність такої великої кількості моделей радіомікрофонів пояснюється тим, що в різних ситуаціях потрібно визначена модель. Дуже часто подібні вироби пропонуються комплектами. Наприклад, професійний комплект АТ-17 складається з різних радіомікрофонів, автоматичного приймача і індикатора випромінювань. Діапазон частот 350-450 МГц. Комплект розміщається в портфелі.

Склад комплекту:

- Портфель.
- Індикатор випромінювань.
- Приймач сигналів.

- Антена приймача.
- Антена індикатора.
- Головні телефони.
- Радіомікрофон Р1 і Р2.
- Радіомікрофон РЗ.
- Радіомікрофон Р5 (Р6)
- Елементи живлення.
- Шнур запису.

Комплект доповнюється антенами "хвильовий канал" чи "метелик". До складу входять кілька видів радіомікрофонів. Вони відрізняються потужністю передавача: радіомікрофон Р2 має потужність випромінювання 15 мВт і дальність дії до 300 м, габарити - 58х51х15 мм, а РЗ, наприклад, - потужність 3 мВт, дальність дії до 150 м і, відповідно, менші габарити - ЗЗх27х7 мм. РЗ – це радіомікрофон з вбудованим мікрофоном і провідниками для підключення зовнішнього електроживлення 1.5В. Включення радіопередавача настає в момент приєднання зовнішнього електроживлення. Корпус пластиковий, антена гнучка. Несуча частота в діапазоні 350 - 450 МГц. Потужність випромінювання 3 мВт. Дальність дії до 150 м. Габарити - ЗЗх27х7 мм.

Розповсюдженим явищем є маскування радіомікрофонів під пристрої подвійного призначення: запальнички, калькулятори, годинники і т. ін. Наприклад, красива кулькова авторучка може працювати як радіомікрофон з дальністю до 200 м. Вбудований мікрофон забезпечує високоякісний акустичний контроль. Електроживлення від годинникових батарейок безупинно до 15 ч. Частоти фіксовані (канал А чи В) у діапазоні 350-450 МГц. Габарити - довжина 130 мм, діаметр 14 мм, вага – 20 г. Цікавими є вироби СА-201 і СА-205, замасковані під калькулятори, з живленням від мережі. Це дозволяє заодно вирішити і проблему живлення, тому що вбудовані акумулятори мають можливість зарядки від мережі.

Існують моделі, виконані у виді шпильки чи затиску для краватки, наручних годинників та ін., які підключаються до передавача чи магнітофону, в залежності від мети операції. Високочутливі мініатюрні мікрофони в авторучці, наручному годиннику, у значку й ін. дозволяють записати важливу бесіду в зручному місці. Електроживлення від годинникової батарейки забезпечує безупинну роботу вбудованого підсилювача впродовж декількох місяців. За допомогою мініатюрного мікрофона з підсилювачем зручно контролювати приміщення, наприклад, через наявні вентиляційні отвори. До проводу, що виходить від такого мікрофона в сусіднє приміщення, підключається або радіопередавач, або магнітофон. Для запису розроблені і широко представлені на ринку спеціальні магнітофони. Одна з моделей – професійний мікрокасетний магнітофон з автореверсом і системою VOX (системою включення при наявності голосу). Крім того, ця модель обладнана вбудованим

мікрофоном і лічильником стрічки і має дві швидкості запису. У повний комплект входить пульт дистанційного керування (ДК), адаптер для електроживлення від мережі, навушники, мікрокасета МС-60, чохол. Габарити - 73х52х20 мм, вага - 90 г. Дуже поширений "джентльменський набір", який містить у собі мікрофон зі шпилькою, телефон з вушним кріпленням, кнопку включення передавача, а також гніздо для підключення до різних радіостанцій та магнітофонів. Вага - 55 г. Така схема дозволяє агенту записати на магнітофон і передати на прийомний пристрій потрібну інформацію.

Ще більш цікавою є схема оперативного застосування радіомікрофона, реалізована у виробі SIPE-PS. Це комплект, що складається з безшумного пістолета з прицільною відстанню 25 м і радіомікрофона-стрели. Він призначений для установки радіомікрофона в місцях, фізичний доступ до яких неможливий. Радіомікрофон у виді наконечника стріли в ударостійкому виконанні надійно прикріплюється до поверхонь з будь-якого матеріалу - металу, дерева, бетону, пластмаси і т. ін. Тактика застосування його наступна: стріла вистрелюється через, наприклад, відкриту кватирку і прикріплюється до стіни. У реальних умовах міста дальність дії радіомікрофона не перевищує 50 м, і ця обставина знижує оперативну цінність системи.

Аналогічний комплект фірми CCS включає арбалет і кілька стріл-дротиків. Це модель STG 4301. Мікрофон забезпечує контроль розмови в радіусі до 10 м, а передавач передає сигнал на приймач, що знаходиться на відстані до 100 м. Як уже говорилося, обмежуючим фактором є живлення. Для збільшення часу функціонування намагаються збільшити ємність батарей, але цей шлях має свої межі. Як приклад оригінального рішення цієї проблеми можна привести факт виявлення співробітниками однієї з організацій, що займається захистом комерційної інформації, при перевірці в одному з офісів радіомікрофона, встановленого в макеті вітрильного корабля. Сам макет був заповнений елементами живлення на півтора року безупинної роботи. Такелаж моделі використовувався як антена[2].

Широко практикується застосування радіомікрофонов з живленням від зовнішніх джерел, у тому числі від телефонної і радіомережі. Уже згадувалися вироби CAL-201 і CAL-205. Можна сказати про вітчизняний прилад ЛСТ-4, який встановлюється в розетках електроживлення, і ЛСТ-51, який встановлюється в телефонній розетці. Оригінальною є модель HR560 LICHT WUD. Це радіомікрофон, вбудований у цоколь звичайної лампочки накалювання, з дальністю дії до 250 м. Ще одна модель радіомікрофона, призначеного для контролю приміщень і встановлюваного в телефонній розетці, – це ЧМ радіомікрофон AD-45-3. Електроживлення здійснюється від телефонної лінії. Дальність – до 150 м. Габарити – 22х16х12 мм, вага – 210 г. Не можна не сказати про радіомікрофон SIPE MT. Цей радіомікрофон із ЧМ передавачем і з живленням від сонячної батареї виконаний у вигляді склянки для віскі. Елементи сонячної батареї замасковані орнаментом на дні склянки. Для

підвищення скритності радіомікрофон має два режими: включений, якщо склянка стоїть на столі, і відключений, якщо його підняти чи змінити положення в просторі. Дальність дії передавача в діапазоні 130-150 МГц складає 100 м. Аналогічний прилад фірми CCS моделі STG 4104 виконаний у вигляді керамічної попільниці, що варто визнати найбільш вдалим прикладом маскування, хоча застосування батарей, схованих у покритому повстю дні попільниці, і обмежує час його безупинної роботи. Вбудований ртутний вимикач відключає передавач, якщо попільницю перевернути. Застосування батарей, а також більш солідна вага попільниці дозволили збільшити радіус дії приладу до 600 м. Передавач працює на частоті 130-150 МГц.

Одним з перспективних напрямків збільшення скритності і часу ефективного використання є застосування дистанційного включення. Прикладами є вироби TRM-1530 і TRM-1532. Це радіомікрофони з живленням від батарей, габаритами 87х54х70 мм, вагою близько 100 г, із ЧМ передавачем діапазону 380-400 МГц чи 100-150 МГц і дальністю до 300 м. Дистанційне вмикання-вимикання дозволяє довести час ефективної роботи виробу до 1 року при часі безупинної роботи 280-300 годин. Подібна апаратура, але більших габаритів, починає надходити в продаж і від вітчизняних виробників. Дуже перспективним є застосування радіомікрофонов з активацією від звуку – музики, мови і т.д. Така модель STG-4001. Включення пристрою здійснюється від звуку, вимикання – автоматично через 5 секунд після зникнення звуку. Застосування функції вмикання за голосом дозволило довести час ефективної роботи до 300 годин. Прилад має дуже незначні розміри - 20х38х12 мм, вага з батареями - 18 г, забезпечує дальність до 500 м, частоти - 130-150 МГц. Варто підкреслити, що такого роду радіомікрофони досить важко знайти. У складних випадках можлива побудова системи передавачів. Наприклад, при русі об'єкта за шляхом проходження заздалегідь розміщаються радіомікрофони, що працюють на різних частотах.

Далі наведемо приклади схемної реалізації радіомікрофонів на рівні радіоаматора(Рис.4.1-4.7).

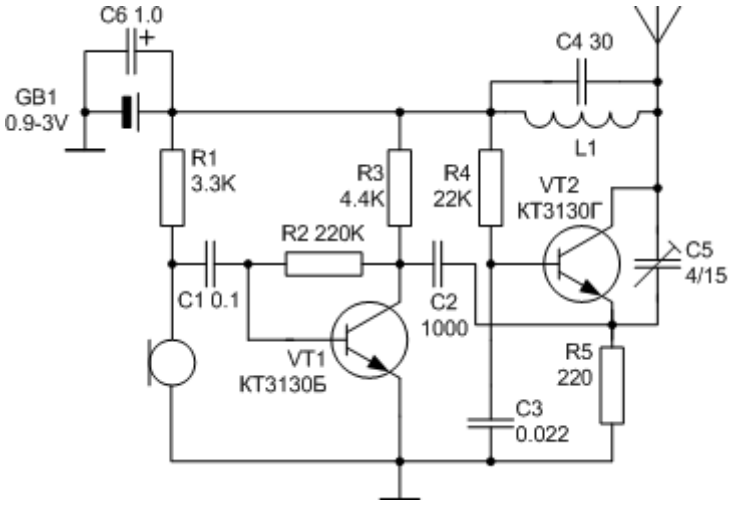


Рис. 4.1. Схема передавача ДВЧ - діапазону з частотною модуляцією

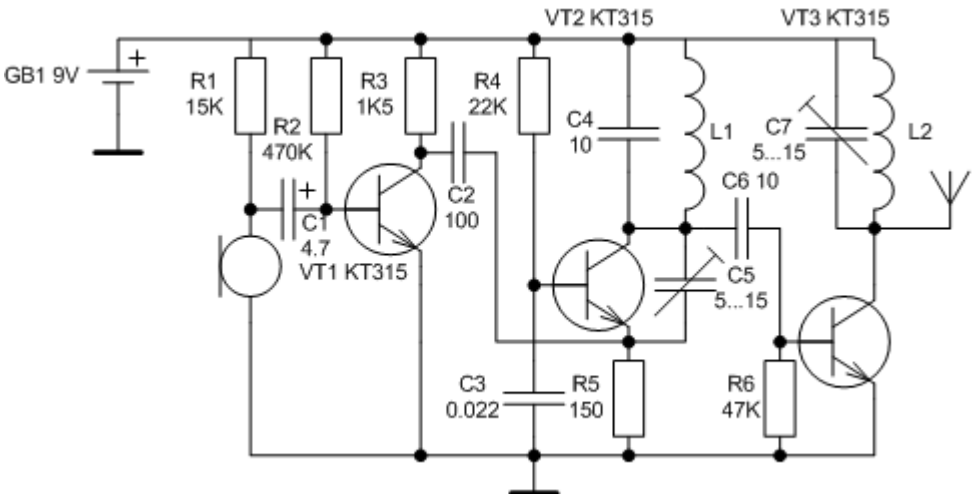


Рис.4.2. Схема передавача з амплітудною модуляцією

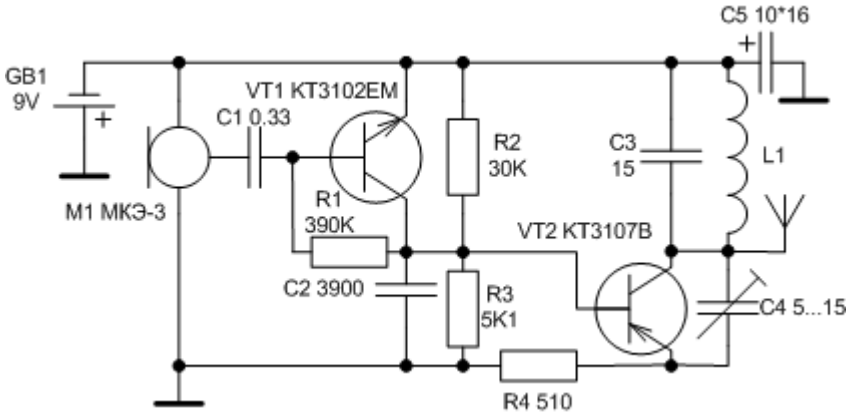


Рис.4.3. Схема передавача з амплітудною модуляцією

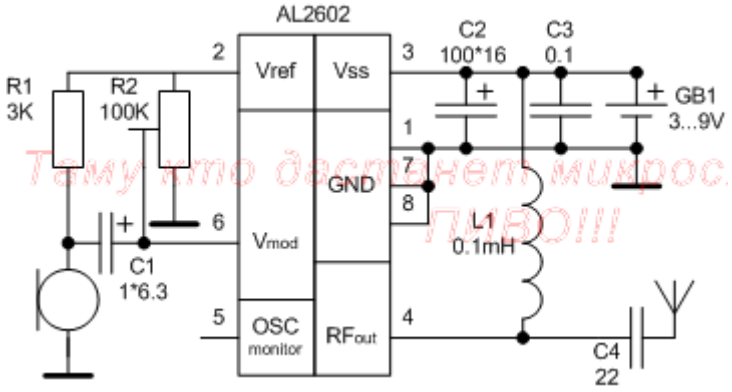


Рис.4.4. Схема передавача в мікроелектронному виконанні

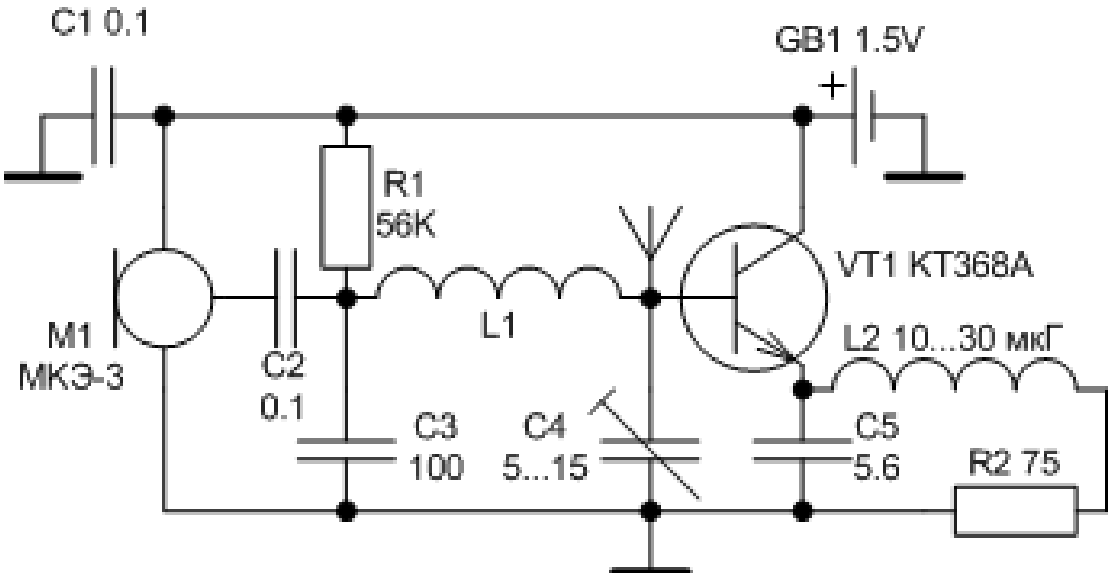


Рис.4.5.Схема простого одно транзисторного передавача

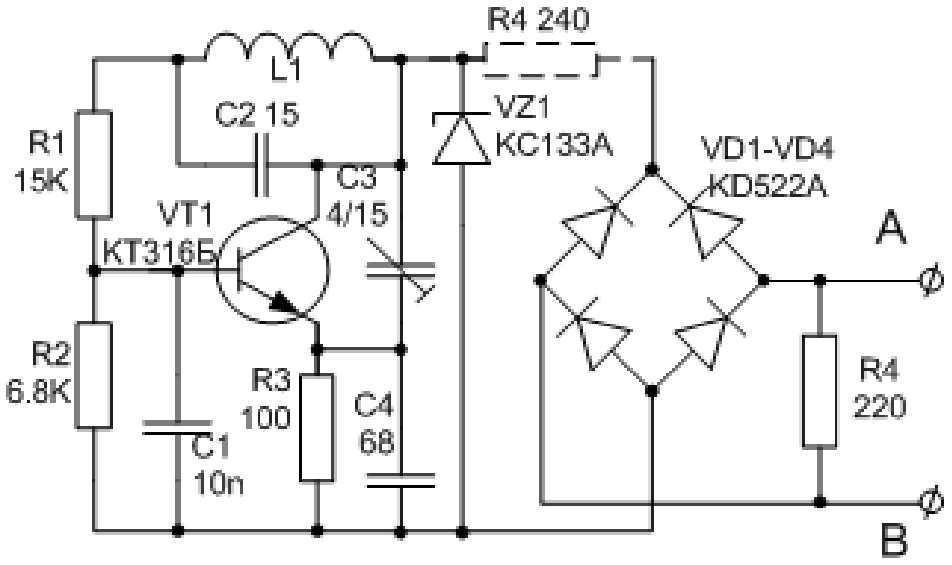


Рис.4.6. Схема передавача для вмикання в телефону лінію

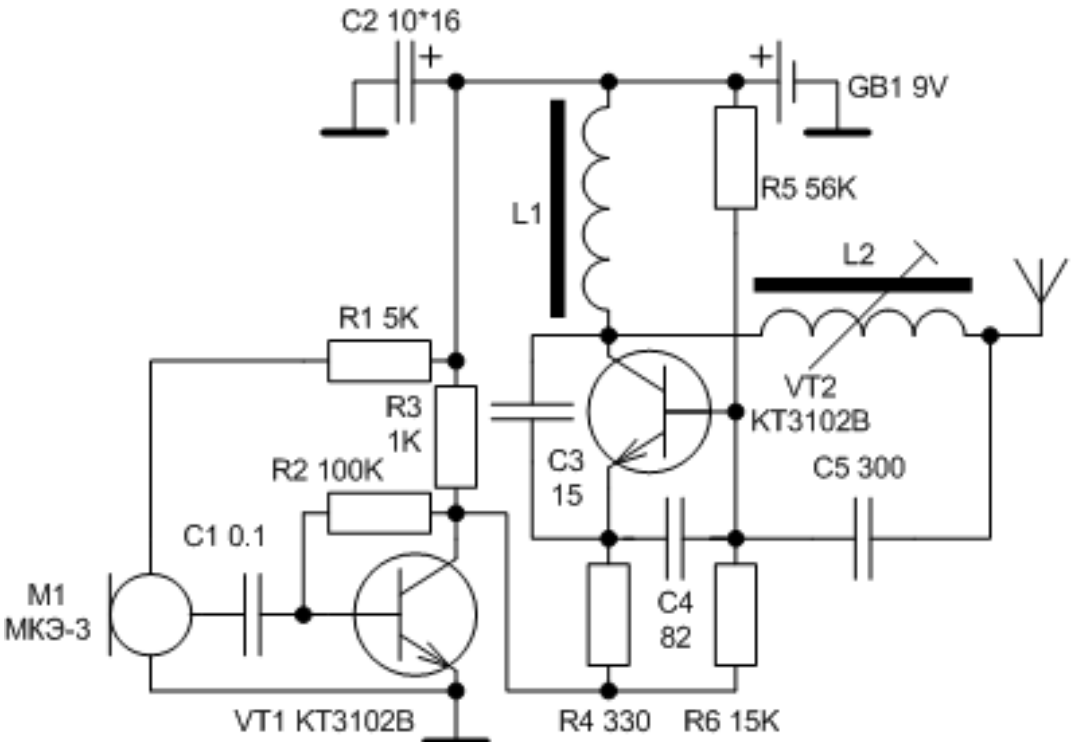


Рис.4.7. Схема передавача з робочою частотою 27 МГц.

Як було сказано вище, прийом сигналу від радіомікрофонів здійснюється за допомогою багатоканального приймача. Можлива побудова схеми з використанням передавача-ретранслятора. Потужність радіомікрофона робиться дуже невеликою (для збільшення часу роботи і підвищення скритності), а на невеликій відстані, наприклад, у сусіднім приміщенні, встановлюється передавач-ретранслятор, габарити і потужність якого піддаються набагато меншим обмеженням. Як уже говорилося вище, дальність дії радіопередавачів визначається в істотному ступені якостями радіоприймальних пристроїв, насамперед, чутливістю. У якості приймачів часто використовують побутові радіоприймальні пристрої. У цьому випадку кращим є застосування магнітол, тому що з'являється можливість одночасного ведення запису. До недоліків таких пристроїв відносяться низька чутливість і можливість налаштовування сторонніх осіб на частоту передавача. Частково ці недоліки можна усунути перебудовою частотного діапазону, у тому числі за допомогою конверторів, а також переналагодженням підсилювачів для підвищення чутливості. Достоїнством таких систем є низька вартість, а також те, що вони не викликають підозр. Але все-таки кращим варто вважати застосування спеціальних приймальних пристроїв. Технічні дані деяких приймачів, призначених для роботи з радіомікрофонами, наведені в табл. 4.2[2].

Як приклад одного з таких пристроїв розглянемо портативний приймач АД-17-2. Діапазон частот складає 360-400 МГц. Приймач здійснює автоматичне сканування і захоплення сигналу передавача. Автоматичне підстроювання частоти здійснюється в режимі прийому. Застосовується АРП (автоматичне регулювання підсилення) проміжної частоти й

АРП сигналу низької частоти. Чутливість - не гірше 2 мкВ. Електроживлення – 6-10 В від елементів типу АА. Опір антенного входу - 50 Ом. Споживання - 3мА.. Амплітуда сигналу на низькочастотному виході – 0,5 В. Габарити - 147х70х38 мм. Як приклад стаціонарного сучасного приймача коротко опишемо радіоприймач ICOM R7100. Це багатофункціональний скануючий приймач, розрахований на діапазон частот від 25 до 2000 МГц. Має можливість прийому радіосигналів з будь-якими видами модуляції, у тому числі контроль телевізійних сигналів на виносний відеомонітор, а також режими ручного й автоматичного настроювання і сканування, 999 каналів пам'яті розділені на 9 груп, що дає можливість сканування за заздалегідь обраними групами каналів/частот. Обладнаний системою автоматичного пошуку і запису в пам'ять значень виявлених частот і вбудованого годинника для керування режимами роботи. Є можливість керування всіма режимами від комп'ютера за допомогою спеціальних програм. Чутливість – від 0,35 до 1,6 мкВ, в залежності від діапазону. Крок настроювання - від 0,1 до 1000 Гц. Є гнізда для підключення магнітофона, монітора і т. ін.

Таблиця 3.2.

Технічні дані приймачів, призначених для роботи з радіомікрофонами

N моделі	Діапазон частот, МГц	Чутливість при с/ш 20дБ, мкВ	Програм. канали	Фіксов. канали	Тип антени	Сканув. і авто-пошук	Акусто мат	Тип живлен-ня	Струм спожив, мА	Габарити, мм	Вага, кг
2220	80-150	5	-	-	мережний провід	-	-	мережа	50-110	160x90x45	0.25
2240	25-550 800-1300	0.35 1.0 1.0	20	-	Телескоп. зовнішній кабель	+	+	батарея мережа адаптер	60-700	470x390x130	8
2254	135-145	0.5	200	-	Всеспря-мована	-	+	батарея мережа адаптер	60-700	470x390x180	8
2270	0.09-34 34-60 114-174 423-450	0.5-3	200	-	-	+	-	110/220 12-16В	35ВА	330x130x280	8.5
2301	25-550 800-1300	0.35 1	20	-	Телескоп. виносна	+	-	адаптер 12В	500	80x138x200	1.2
2303	380-440	0.5	-	2	Вбудов.	-	-	6В	15-40	125x60x20	0.18
2307	26-29,99 60-88 115-178 210-260 410-520	0.7 1.5	16	-	Вбудов.	+	-	адаптер 6В	120-170	185x80x37	0.47
2308	60-89 118-136 140-174	0.7 1.5	20	-	Вбудов.	+	-	адаптер 4В	100	145x65x44	0.56
2309	20-1000	1	30	-	Активна пассивна	+	-	батарея адаптер	500-800	188x71x212	3
2310	20-1000	0.5	100	-	-	+	-	110/220 батарея	60Вт	433x132x465	15

4.3. Пристрої перехоплення телефонних повідомлень

4.3.1. Основні методи прослуховування телефонних ліній

Цінність інформації, переданої по телефонних лініях, а також існуюче переконання про масовий характер такого прослуховування викликає найбільше занепокоєння у організацій і приватних осіб за збереження конфіденційності своїх переговорів саме по телефонних каналах. Для захисту своїх секретів необхідно знати методи, за допомогою яких можуть бути здійснені операції по перехопленню. Але при цьому потрібно врахувати, що організація масового прослуховування (в існуванні якої переконано дуже багато людей) неможлива з причин технічного і фінансового характеру. Справді, для аналізу записаних повідомлень потрібно тримати величезну кількість людей і техніки. Як затверджує колишній глава КДБ В. Бакатін, 12 відділ КДБ прослухував у Москві приблизно 300 абонентів. Крім того, для організації прослуховування в даний час потрібна санкція прокуратури. Більш ймовірна організація прослуховування без санкції, у комерційних чи інших цілях. За американськими даними імовірність витоку інформації по телефонних каналах складає від 5 до 20%. В даний час на ринку представлені сотні типів пристроїв перехоплення телефонних повідомлень, як вітчизняних, так і імпортних. Можна виділити шість основних зон прослуховування (рис. 4.8)[1]:

- - телефонний апарат;
- - лінія від телефонного апарата до розподільної коробки;
- - кабельна зона;
- - зона АТС;
- - зона багатоканального кабелю;
- - зона радіоканалу.

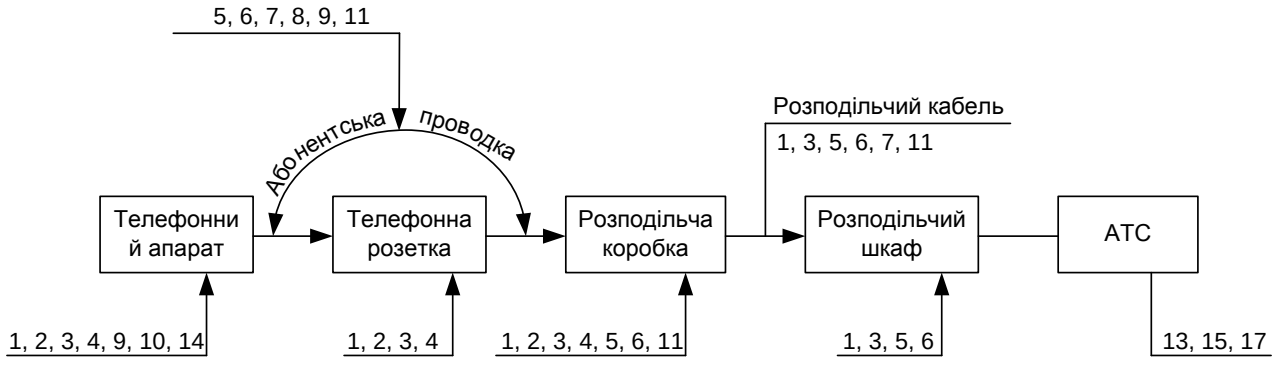


Рис. 4.8. Структурно-топологічна схема абонентської телефонної лінії.

1 – радіозакладка паралельного підключення;

2 – комбінована телефонно-акустична радіозакладка;

3 – радіозакладка послідовного підключення;

4 – закладка типу „довге вухо”;

5 – низькоомний адаптер;

6 – високоомний адаптер;

7 – безконтактний адаптер;

8 – наводки телефонного сигналу на інші кола;

9 – акустоелектричне перетворення;

10 – ВЧ випромінювання схем телефонного сигналу;

11 – ВЧ нав’язування;

12 – паразитні випромінювання підсилювача;

13 – зняття інформації на АТС;

14 – радіовипромінювання телефонного подовжувача;

15 – перехват інформації з лінії зв’язку;

16 – складна високочутлива апаратура;

17 – виток інформації на лініях відводу від АТС (позавідомча охорона, тощо).

Найбільш імовірна організація прослуховування перших трьох зон, тому що саме в цих зонах найлегше підключитися до телефонного лінії. Фахівці, що займаються захистом інформації, стверджують, що найчастіше використовується прослуховування за допомогою паралельного апарата. У більшості випадків для цього навіть не потрібно прокладати додаткові проводи – телефонна мережа настільки заплутана, що завжди є невикористані лінії. Крім того, неважко підключиться в парадній до розподільної коробки. Підключення в третій зоні менш поширено, тому що необхідно проникати в систему телефонних комунікацій, що складається з труб із прокладеними всередині них кабелями, а також розібратися в цій системі й визначити потрібну пару серед сотень інших. Однак не слід вважати, що це нездійсненна задача, оскільки існує вже необхідна для цього апаратура. Як приклад можна привести американську систему "Кріт". За допомогою спеціального індуктивного датчика, що охоплює кабель, знімається передана по ньому інформація. Для установки датчика на кабель використовуються колодязі, через які проходить кабель. Датчик у колодязі фіксується на кабелі і для ускладнення виявлення проштовхується в трубу. Сигнал записується на диск спеціального магнітофона. Після заповнення диска видається сигнал і агент, при сприятливих умовах, замінює диск. Апарат може записувати інформацію, передану одночасно по 60 каналах. Тривалість безупинного запису складає 115 годин. Такі пристрої знаходили в Москві. Для різних типів підземних кабелів розроблені різні датчики: для симетричних високочастотних – індуктивні для відводу енергії з коаксіальних кабелів, для кабелів з надлишковим тиском – пристрої, що виключають його зниження. Деякі

прилади забезпечуються радіопередавачем для передачі записаних повідомлень чи перехоплення їх у реальному масштабі часу.

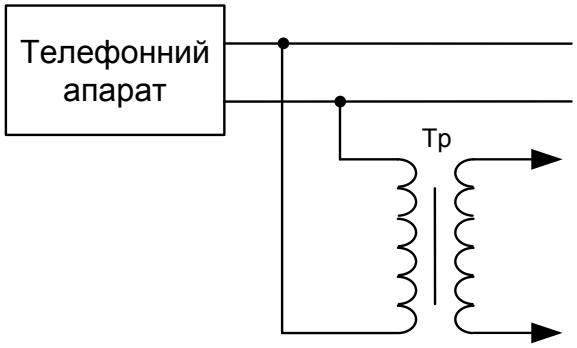


Рис. 4.9. Підключення за допомогою узгоджувального пристрою

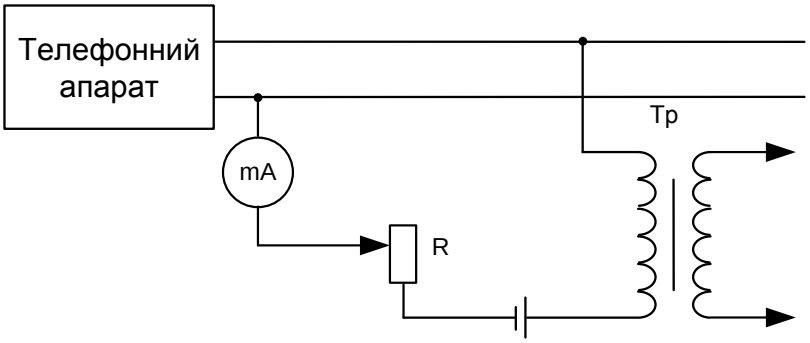


Рис. 4.10. Підключення з компенсацією напруги

4.3.2. Способи підключення до телефонної лінії і запис переговорів

У технічному плані найпростішим способом є контактне підключення. Можливо тимчасове підключення до абонентської проводки за допомогою стандартної "монтерської трубки". Однак підключення такого типу легко виявляється за допомогою найпростіших засобів контролю напруги телефонної мережі. Зменшити ефект спадання напруги можна шляхом підключенням слухавки через резистор опором 0,6-1 кОм. Підключення здійснюється за допомогою дуже тонких голок і тонких, покритих лаком, проводів, що прокладаються в якій-небудь існуючій чи виготовленій щілині. Щілина може бути зашпакльована і пофарбована так, що візуально визначити підключення дуже важко. Кращим є підключення за допомогою узгоджувального пристрою (рис. 4.2). Такий спосіб істотно менше знижує напругу в телефонній мережі й ускладнює виявлення факту прослуховування. Відомий спосіб підключення до ліній зв'язку апаратури з компенсацією спадання напруги (рис. 4.3). Істотними недоліками контактного способу підключення є порушення цілісності проводів і вплив підключеного пристрою на характеристики ліній зв'язку. З метою усунення цього недоліку застосовується індуктивний датчик, виконаний у вигляді трансформатора. Існують також датчики, принцип роботи яких заснований на ефекті Холла. У табл. 4.3 наведено характеристики датчиків адаптерів підключення до телефонної

лінії. Вартість подібних пристроїв коливається від $20 до $250. У якості пристроїв запису застосовуються стандартні диктофони, спеціальні мініатюрні, як OLIMPUS L-400, а також стаціонарні багатоканальні диктофони, як, наприклад, АД-25-1. Як правило, схема прослуховування організована так, що магнітофон включається з появою сигналу в лінії. Як приклад мініатюрного магнітофона можна привести модель N2502, рекламовану як магнітофон, що неможливо знайти за допомогою сучасних детекторів записуючої техніки. У цьому магнітофоні є гнізда для підключення зовнішнього мікрофона, пульта дистанційного керування і головних телефонів. Як правило, спеціальні багатоканальні магнітофони для запису телефонних переговорів використовуються в складі спеціальної апаратури для контролю особливо режимних робіт. У цьому випадку використовуються спеціальні прийоми, що дозволяють за ключовими словами переривати чи записувати телефонну розмову. Випадки комерційного прослуховування на міських АТС вкрай рідкі, тому що це неможливо без наявності там "своєї" людини з обслуговуючого персоналу[1].

Таблиця 4.3.

Адаптери підключення до лінії

Марка	Габаритні розміри	Живлення	Додаткові функції
ЛСТ-АД	45x35x5	автономне	Автоматичне вкл./викл.
БД-1	-	автономне	Індуктивний датчик
PRO-1213	95x58x25 50x22x10	автономне 9В	Ефект Холла
UM-122	100x50x18	автономне 3В	Контактна голка
STG-4525	125x75x25	автономне 9В	Індуктивний зонд
PK-135S	16x35	не потрібно	Включення за голосом

Однак не можна виключати випадків такого прослуховування на існуючих і організованих на деяких підприємствах місцевих АТС. Таке прослуховування може бути організоване за допомогою наявних на ринках США, Німеччині і Японії спеціальних багатоканальних магнітофонів, призначених для стаціонарного запису телефонних переговорів і розрахованих на значне число каналів(від 10 до 100). Технічні характеристики деяких з таких пристроїв приведені в табл. 4.4.

Таблиця 4.4.

Технічні характеристики записуючих пристроїв

Модель	Число каналів	Габаритні розміри, мм	Вага, кг	Час запису	Додаткові функції
РК-115-S	10	500x360x150	9.8	немає даних	автоматичне включення підключення принтера, прив'язка до часу
РК-100-55	1 10 50 100	209x1666x290 1100x550x380 110x890x660 7900x1890x600	2,9 60 220 430	4 10x4 50x4 100x4	автоматичне включення. підключення принтера. прив'язка до дати і часу
АД-25	8	480x350x190	16	немає даних	прив'язка до часу, дистанц. керування
ТМ	9 20 31 42	немає даних	немає даних	до 1000	прив'язка до дати і часу відео контроль
CU-1	10	немає даних	немає даних	немає даних	реєстрація часу, дати, номера абонента, підрахунок числа дзвоників

Розглянемо приклади схемної реалізації методів перехоплення телефонних переговорів. Наприклад, простий підсилювач, на вхід якого підключена котушка індуктивності. Котушку-датчик можна виконати на броньованому сердечнику. У якості котушки для знімання інформації можна використовувати магнітну головку від магнітофона. У цьому випадку один із телефонних проводів розташовують поряд із зазором. Котушку-датчик можна виготовити і з малогабаритного низькочастотного трансформатора.

На рис 4.11 наведена схема підсилювача безконтактного знімання інформації з телефонної лінії[2].

При використанні у якості датчика магнітофонної головки L1 доцільно використати конденсатор С6, який з L1 утворює коливальний контур, налаштований на 1кГц-1.5кГц, Це дозволяє збільшити рівень сигналу від датчика (і збільшити співвідношення сигнал/шум).

Елементи для схеми на мал.4.4 Rl=R2=5к-10к (дорівнює або трохи вище максимального опору датчика в робочому діапазоні частот), R3=5к~10к (підстроювання посилення, K=l+R4/R3), R4=1M-2M, R5=10 Ом;

С1=4.7мкф-20мкф, С2=10мкф-50мкф, СЗ=0.1-0.47, С4=100мкф-200мкф, С5=0.1;

ОП - КР1407УД2, КР140УД20, КР1401УД2Б**,** 140УД8 або аналогічні ОП в їхньому типовому включенні й бажано із внутрішньою корекцією;

Tl, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

Т - ТМ-2А або аналогічні.

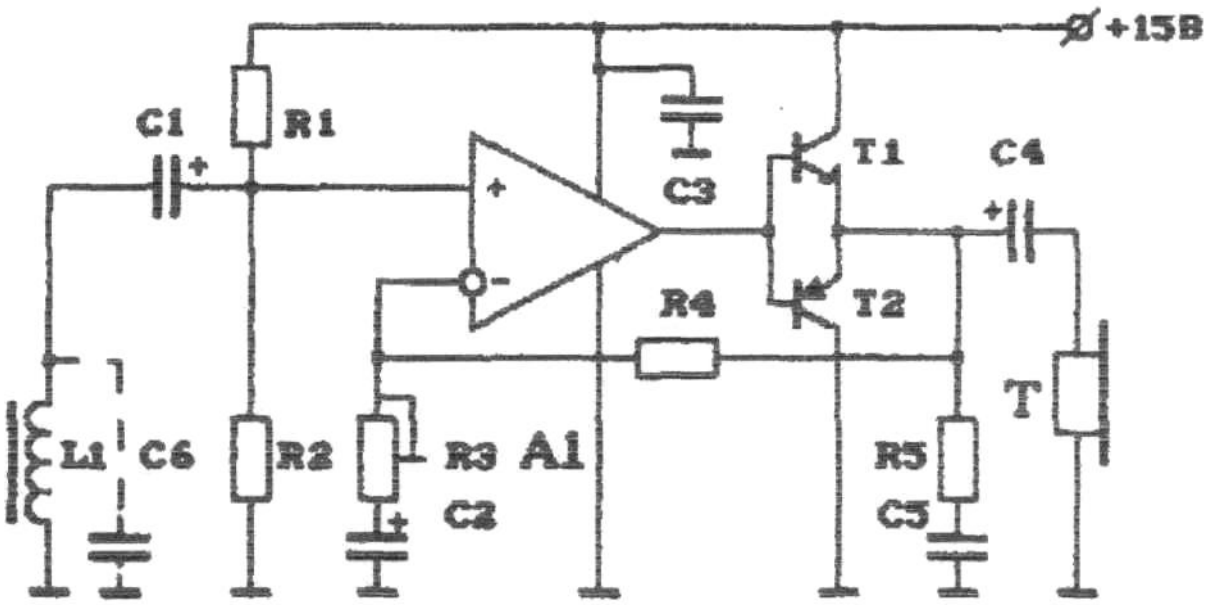


Рис. 4.11. Схема підсилювача безконтактного знімання інформації з телефонної лінії на ОП.

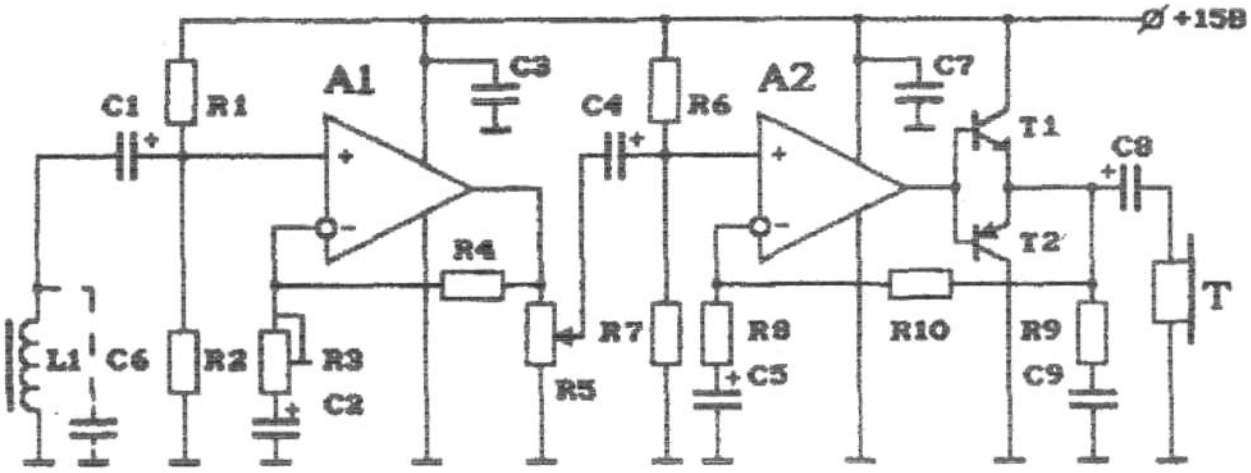


Рис. 4.12. Схема підсилювача безконтактного знімання інформації з телефонної лінії на 2 ОП з регулюванням гучності

На рис. 4.12 наведена схема підсилювача безконтактного знімання інформації з телефонної лінії на двох ОП з можливістю регулювання гучності[2].

R1=R2=5к-10к (дорівнює або трохи вище максимального опору датчика в робочому діапазоні частот), R3=5к-10к (підстроювання посилення, K=l+R4/R3), R4=100К-300К, R5=3к-10к (регулятор рівня гучності), R6=R7=100К-200К, R8=3к-5к, R9=10, R10=30к-50к;

С1=4.7мкф-20мкф, С2=10мкф-50мкф, С3=0.1-0.47, С4=1.0мкф-10мкф**,** С5=10мкф-50мкф, С7=0.1-0.47, С8=100мкф-200мкф, С9=0.1;

ОУ - КР1407УД2, КР140УД20, КР1401УД2Б, К140УД8**.** КР140УД12 або аналогічні ОП;

Т1.Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні)

транзистори:

Т - ТМ-2А або аналогічні

4.3.3 Телефонні радіо ретранслятори

Телефонні радіо ретранслятори (рис. 4.13) надзвичайно популярні та являють собою радіо подовжувачі для передачі телефонних розмов по радіоканалах. Більшість телефонних закладок автоматично включаються при піднятті слухавки і передають інформацію до пункту перехоплення і запису. Джерелом живлення для радіопередавача є, як правило, напруга телефонної мережі. Тому що в даному випадку не потрібно ані батарейок, ані вбудованого мікрофона, розміри ретранслятора можуть бути дуже невеликими. Недоліком подібних пристроїв є те, що вони можуть бути виявлені за радіовипромінюванням[1].

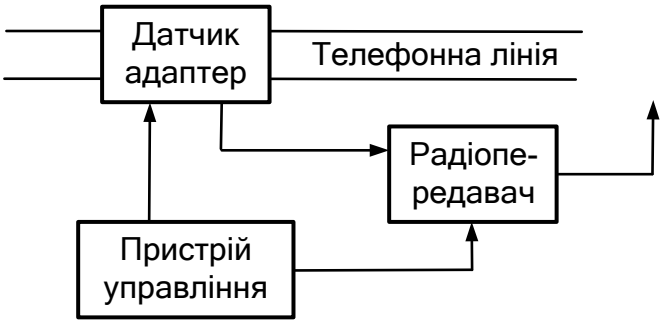


Рис. 4.13. Структурна схема радіо ретранслятора

Наприклад, малогабаритний кварцовий передавач AD-31 призначений для контролю телефонної лінії. Дальність дії – до 300 м і більше. Діапазон частот - 350-450 МГц. Має канали А, В чи С. Включається в розрив телефонної лінії. Габарити - 18х38х10 мм, вага - 15 г. Компактний ЧМ передавач FD-45-4 для контролю телефонної лінії. Закамуфльований у телефонну розетку. Дальність дії – до 150 м. Габаритні розміри – 22х16х12 мм. Вага - 210 г. Щоб зменшити можливість виявлення радіовипромінювання, застосовують той же спосіб, що й у випадку з радіо мікрофоном – зменшують потужність випромінювання передавача, установленого на телефонній лінії. А в безпечному місці встановлюють більш потужний ретранслятор, що перевипромінює сигнал на іншій частоті й у зашифрованому вигляді. Варто врахувати, що не можна виключати можливість застосування радіопередавачів, що використовують псевдо шумові сигнали і (чи) працюючих "під шумами". У цьому випадку виявлення радіозакладок ще більш ускладнюється. Для маскування телефонні радіо ретранслятори випускаються у вигляді конденсаторів, фільтрів, реле й інших стандартних вузлів елементів, що входять до складу телефонної апаратури. Існують ретранслятори, виконані у вигляді мікрофона слухавки (наприклад, модель CRISTAL фірми Sipe). Подібні вироби дуже легко і швидко можна встановити в цікавлячий телефонний апарат. Тут не можна не сказати, що дуже часто не потрібно пробляти навіть і такі прості операції. Дуже поширені телефонні апарати з кнопковим номеронабирачем типу ТА-Т, ТА-12. Завдяки

особливостям своєї конструкції вони перевипромінюють інформацію на десятках частот СХ, КХ і УКХ діапазону на відстань до 200 м. Ще більш просто підслухати розмову, якщо використовується телефон з радіо подовжувачем, що представляє собою дві радіостанції: одна змонтована в трубці, інша – у самому телефонному апараті. У цьому випадку потрібно тільки налаштувати приймач на необхідну частоту. Для подібних цілей випускаються і спеціальні розвідувальні приймачі. Наприклад, приймач "Мініпорт" фірми "Роде і Шварц" з діапазоном частот 20-1000 МГц. Цей приймач має невеликі габарити (188х74х212), універсальне живлення й вбудований процесор. Запам'ятовуючий пристрій може зберігати в пам'яті до 30 значень частот і здійснювати сканування в заданому діапазоні зі змінним кроком[1].

4.3.4 Системи прослуховування повідомлень, переданих по стільникових, пейджингових каналах та факсу

Стільниковою називається система зв'язку, що складається з деякої кількості осередків, що, зв'язуючись між собою, утворять мережу, чи стільники. Кожен осередок може працювати з визначеною кількістю абонентів одночасно. Стільникові мережі мають можливість нарощування, а також можуть стикуватися один з одним. Радіус дії базової стільникової станції складає 5-15 км, а перехоплення повідомлень у цьому випадку, може проводитися на відстані до 50 км. Як приклад реалізації подібної системи можна привести стільникові системи спостереження Cellmate-10B та Cellscan. Cellmate-10B контролює одночасно до 10 телефонних номерів, тобто один осередок стільникового зв'язку. Існує можливість програмованого перебору осередків. Потрібна розмова може визначатися за голосом абонента чи за змістом розмови. Перехоплені один раз номери при бажанні переводяться програмою в особливий режим спостереження. Вбудований запам'ятовуючий пристрій запам'ятовує останні параметри настроювання. Запис починається автоматично, коли об'єкт спостереження починає користуватися телефоном. Інформація про номери телефонів, параметри настроювання, ідентифікацію за голосом зчитується з кольорового рідиннокристалічного дисплея, так само визначаються коди доступу[2].

Система Cellscan, аналогічна за функціями Cellulate-10B та також розміщується в аташе-кейсі. Стверджується, що кількість програмувальних номерів не обмежена. У режимі сканування на дисплей виводиться інформація про 895 каналів. Спостерігається вся телефонна система, та вибираються канали, по яких відбуваються дзвоники. За допомогою комплекту стільникових карт визначається район, у якому відбувається підозріла розмова, ідентифікована сканером за змістом чи голосом. Можна відключити канали, перехоплення яких ви не хочете здійснювати. Використовується покращений стільниковий телефон OKI, що може застосовуватися у якості звичайного стільникового телефону. Вага системи – 9 кг.

Сучасні системи стільникового зв'язку можуть використовувати різні системи кодування і (чи) настроювання на частоти за випадковим законом. Існують і спеціальні комплекти радіоперехоплення з можливістю аналізу зашифрованих повідомлень, наприклад, Sigint/Commt Spektra фірми Hollandes Signal, але така апаратура дуже дорога. У СНД розроблені і пропонуються програмно-апаратні системи перехоплення пейджингових повідомлень[2]. До складу такої системи входять сканер (AR-ЗОООА, IC-7100 і ін.), пристрій перетворення, комп'ютер і спеціальне програмне забезпечення. Система дозволяє здійснювати прийом і декодування текстових і цифрових повідомлень, переданих у системі радіо пейджингового зв'язку і зберігати всі прийняті повідомлення (з датою і часом передачі) на жорсткому диску персонального комп'ютера. При цьому може вироблятися фільтрація потоку повідомлень, виділення даних, адресованих конкретним абонентам. Перехоплення факс-повідомлень принципово не відрізняється від перехоплення телефонних повідомлень. На закінчення приведемо приклад організації прослуховування Агенцією національної безпеки США, що має в 6 разів більше службовців, ніж ЦРУ. Чотири тисячі сто двадцять могутніх центрів прослуховування на базах у Німеччині, Туреччині, Японії і т.д., а також на кораблях, підводних човнах, літаках і супутниках збирають і аналізують майже всю інформацію, передану електронним способом, включаючи випромінювання систем сигналізації автомобілів, квартир і т. ін[2].

4.3.5 Використання телефонної лінії для прослуховування приміщень

Телефонна лінія використовується не тільки для передачі телефонних повідомлень, але і для прослуховування приміщення (рис. 4.14). Щоб увімкнути такий пристрій, потрібно набрати номер абонента. Перші два гудки "ковтаються" пристроєм, тобто телефон не дзвонить. Після цього необхідно покласти трубку і через визначений час (30-60 секунд) подзвонити знову. Тільки після цього система включається в режим прослуховування. Подібним чином працюють, наприклад, пристрої ST-01 ELSY, UM103. Ціна таких пристроїв – від $15 (вітчизняні) до $250 (закордонні). Як приклад одного з таких пристроїв розглянемо БОКС-Т. Цей пристрій дозволяє контролювати приміщення з будь-якого місця земної кулі по телефону. Для цього досить набрати номер телефону, де вже встановлений прилад "Бокс-Т", і зробити увімкнення мікрофона. Для вимикання досить покласти слухавку. Модель TS-20-1

дозволяє додатково контролювати підключені до неї датчики охоронної сигналізації. Модель TS-10-T2 включається за допомогою блоку виклику. Електроживлення всіх моделей здійснюється від телефонної лінії з напругою 60 В. Блок виклику моделі TS20-T2 живиться напругою 9 В від батареї типу "Крона"[2].

Для розуміння фізики процесів, які виникають при цьому, розглянемо види акустичних перетворень, що дозволяють перехоплювати інформацію.

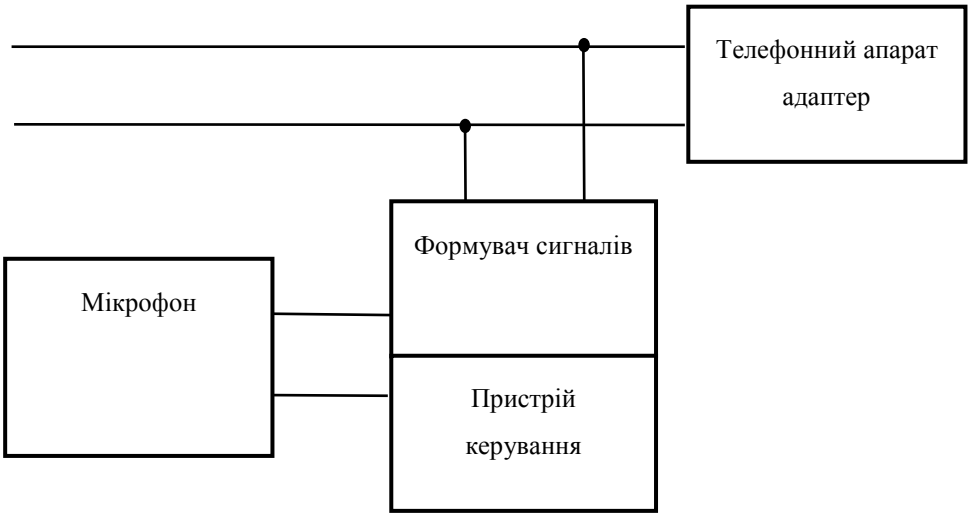


Рис. 4.14. Використання телефонної лінії для прослуховування приміщень

Як відомо, під час розмови утворюються звукова хвиля, яка може викликати механічні коливання елементів електричної апаратури, що в свою чергу приводить до появи електромагнітного випромінювання. Види акустоелектричних перетворювань наведені на рис. 4.15. Найбільш чутливі до акустичних впливів є котушки індуктивності та конденсатори змінної ємності.

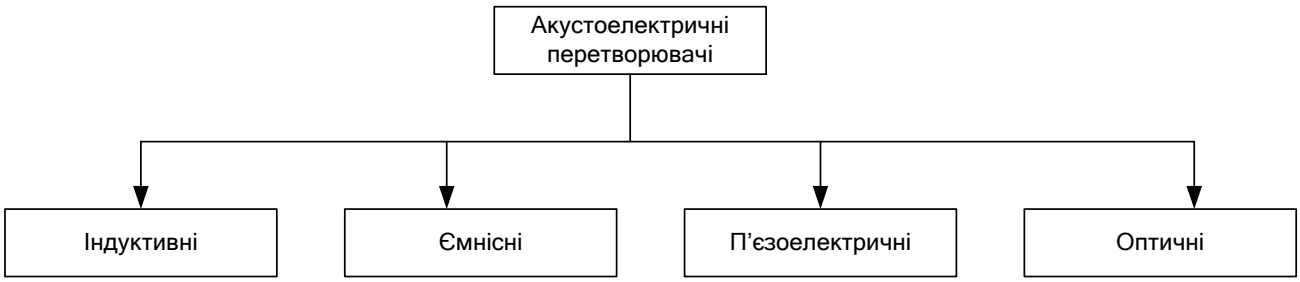


Рис. 4.15. Види акустоелектричних перетворень

Розглянемо акустичну дію на котушку індуктивності з серцевиною. Механізм та умови виникнення електрорушійної сили (ЕРС) індукції у такій котушці зводиться до наступного:

– під дією акустичного тиску P з'являється вібрація корпусу та обмотки котушки;

– вібрація викликає коливання.

Проводи обмотки у магнітному полі, що й призводе до появи ЕРС індукції на кінцях котушки. Ця ЕРС визначається за формулою

$$E = \frac{d}{dt}\left(N_{фс} + N_{фн}\right) = \frac{d}{dt} B_0 \left[S_c(t) \frac{\mu_c(t)}{\mu_0(t)} \cos\varphi_c(t + S_0'(t)\cos(t) \right],$$

де $N_{фс}$ – магнітний потік, який замикається через серцевину; $N_{фн}$ – магнітний потік, який замикається через обмотку по повітрю; B_0 – вектор магнітної індукції; $\mu_c(\epsilon)$ – магнітна проникливість сердечника; $\mu_0(\epsilon)$ – магнітна постійна; $\varphi_c(t)$ – кут між вектором B_0 та віссю осердя; $\varphi_0(t)$ – кут між векторами B_0 та віссю котушки.

Індуктивні перетворювачі поділяються на електромагнітні, електродинамічні та магнітострикційні.

До електромагнітних перетворювачів відносяться такі пристрої, як гучномовець, електричні дзвінки (в тому числі й визивні дзвінки телефонних апаратів), електро радіовимірювальні прилади.

Прикладом безпосереднього використання цього ефекту для кіл акустичного перетворення є електродинамічний мікрофон. ЕРС на виході котушки визначається за формулою

$$E = -L\frac{dI}{dE},\ L = kL\pi\mu_0 N^2 \frac{S}{I}, \tag{4.2}$$

де L – індуктивність, k – постійний коефіцієнт; I – довжина намотки котушки; d – діаметр котушки; μ_0 – магнітна проникність; S – площа поперечного перерізу; N – кількість витків котушки.

Виникнення ЕРС на вході такого перетворювача прийнято називати мікрофонним ефектом. Можна стверджувати, що мікрофонний ефект здатний проявлятися як у електродинамічній, так і в електромагнітній, конденсаторній та інших конструкціях, які широко застосовуються в мікрофонах різного призначення та використання.

Електромеханічний дзвоник виклику телефонного апарату — типовий приклад індуктивного акустоелектричного перетворювача, мікрофонний ефект якого виявляється при покладеній телефонній трубці.

ЕРС мікрофонного ефекту дзвоника може бути визначена за формулою:

$$E_м = \eta P, \tag{4.3}$$

де η – акустична чутливість дзвоника, P – акустичний тиск.

$$\eta = \frac{VS\mu_0 NS_м}{d^2 Z_м},$$

де V – магніторушійна сила постійного магніту; S – площа якоря; μ_0 – магнітна проникність осердя; N – кількість обмоток котушки; $S_м$ – площа смугового наконечника; d – величина проміжку; $Z_м$ – механічний опір.

За таким же принципом (принципом електромеханічного дзвоника) утворюється мікрофонний ефект і в окремих типах електромагнітних реле різного призначення та навіть у електричних дзвінках виклику побутового призначення.

Акустичні коливання діють на якір реле та викликають його коливання. Коливання якоря змінюють магнітний потік реле, який замикається по повітрю, що приводить до появи на виході котушки реле ЕРС мікрофонного ефекту.

Мікрофонний ефект мають також побутові гучномовці, ЕРС яких визначаються за формулою

$$E_м = \eta P, \quad \eta = \frac{BIS}{Z_m}, \tag{4.4}$$

де η – акустична чутливість дзвоника; I – довжина провідника, який рухається в магнітному полі з індукцією B; B – магнітна індукція; S – площа поверхні, яка підпадає під вплив тиску акустичного поля; Z_m – механічний опір.

Необхідно мати на увазі, що існують так звані "беззаходові" системи передачі акустичної інформації з телефонних ліній, що дозволяють прослуховувати приміщення без установки якого-небудь додаткового устаткування. Також використовуються недоліки конструкції телефонного апарата: акустичні коливання впливають на якір дзвоника, який, коливаючись, викликає появу в котушці мікрострумів, модульованих мовою. ЕРС, що наводиться в котушці, у цьому випадку може досягати декількох мілівольтів. Дальність цієї системи не перевищує (через загасання) декількох десятків метрів. Прийом здійснюється на якісний підсилювач низкою частоти з малим рівнем шуму. Другий варіант "беззаходової" системи пов'язаний з реалізацією ефекту "нав’язування". Коливання частотою від 150 кГц і вище подаються на один провід телефонної лінії, до другого проводу приєднується приймач. Загальний провід передавача і приймача з’єднані між собою чи з загальною «землею», наприклад, водопостачальною мережею. Через елементи схеми телефонного апарата високочастотні коливання надходять на мікрофон, навіть якщо він відключений від мережі, і модулюються мовою. Детектор приймача виділяє мовну інформацію. Через істотне загасання ВЧ сигналу в двопроводної лінії дальність також не перевищує декількох десятків метрів (без ретранслятора).

4.4. Спеціальні пристрої прослуховування

4.4.1. Спрямовані мікрофони

Звичайні мікрофони здатні реєструвати людську мову на відстані, що не перевищує декількох десятків метрів. Для збільшення дистанції, на якій можна робити прослуховування. практикують застосування спрямованого мікрофона. Іншими словами, цей пристрій збирає звуки тільки з одного напрямку, тобто має вузьку діаграму спрямованості. Такі пристрої широко застосовуються не тільки у розвідці, але і журналістами, мисливцями, рятувальниками і т.д. Можна виділити два основних типи спрямованих мікрофонів:

- з параболічним відбивачем;
- резонансний мікрофон.

У мікрофоні з параболічним відбивачем власне мікрофон розташований у фокусі параболічного відбивача звуку. Спрямований параболічний мікрофон з підсилювачем AD-9 9 концентрує звуки і підсилює їх. Простий у експлуатації і настроюванні. У комплект входить мікрофон, підсилювач, кабель і головні телефони. Електроживлення - від батареї 9 В. Випускаються кілька моделей. Загалом у конструкції всіх цих мікрофонів є наявність рукоятки пістолетного типу, параболічного відбивача діаметром близько 40 см і підсилювача. Діапазон сприйманих частот складає від 100-250 Гц до 15-18 кГц. Усі мікрофони мають автономне живлення і мають гнізда для підключення до магнітофона. Гостра "голчаста" діаграма спрямованості дозволяє при відсутності перешкод контролювати людську мову на відстані до 1200 м. У реальних умовах (в умовах міста) можна розраховувати на дальність до 100 м[2].

Резонансний мікрофон заснований на використанні явища резонансу в металевих трубках різної довжини. Наприклад, в одній з модифікацій такого мікрофона використовується набір з 37 трубок довжиною від 1 до 92 см. Звукові хвилі, що приходять до приймача по осьовому напрямку, приходять до мікрофона в однаковій фазі, а з бічних напрямків (через відмінну швидкість поширення звукових хвиль у металі, а також різної довжини трубок) - виявляються зрушеними по фазі. З погляду схованого контролю звуку застосування спрямованих мікрофонів ускладнено через найчастіше неприйнятні їхні габарити і джерела акустичних перешкод. Крім того. для того, щоб не бути прослуханим в автомобілі, досить просто підняти скло.

Таким чином можна констатувати, що на цей час на ринку існує багато засобів перехоплення інформації за допомогою спрямованих мікрофонів. Але, такі пристрої можна виготовити й самостійно, маючи необхідний рівень підготовки в галузі електроніки. Розглянемо деякі рекомендації щодо виготовлення спрямованих мікрофонів.

З великого листа паперу з ворсом (під оксамит) слід зробити трубу діаметром 10-15 см та довжиною 1.5 – 2 м. У один кінець цієї труби вставляють чутливий мікрофон. Найкраще за все, якщо це буде динамічний або конденсаторний мікрофон. Наприклад, динамічний мікрофон типу МД-64, МД-200 або навіть мініатюрний МКЕ-3. у крайньому випадку можна використати звичайний побутовий мікрофон.

Мікрофон слід підключати за допомогою екранованого кабелю до чутливого підсилювача з малим рівнем власних шумів. Якщо довжина кабелю перевищує 0.5 м, тоді краще використовувати мікрофонний підсилювач, який має диференціальний вхід, наприклад, підсилювач нижніх частот (ПНЧ) на операційних підсилювачах (ОП). Це дозволяє зменшити синфазну складову завад, які є наводками від найближчих електромагнітних пристроїв (фон 50 Гц від мережі 220В і т. ін.).

Отже, якщо вільний кінець труби направити на джерело звука, то можна почути розмову на відстані 100 м і навіть більше. Ця відстань може бути збільшена шляхом застосування спеціальних селективних фільтрів, які дозволяють виділити та придушити сигнал у вузькій смузі частот. Це дає можливість підвищити співвідношення рівня корисного сигналу на фоні існуючих завад. У спрощеному варіанті замість спеціалізованих фільтрів можна застосовувати смуговий фільтр у ПНЧ, або скористатися звичайним еквалайзером (багато смуговим регулятором тембру), а в крайньому випадку традиційним регулятором тембру НЧ та ВЧ з двома смугами.

При конструюванні чутливого та з малим шумом підсилювача слід пам’ятати, що найбільший вплив на якість звучання та розбірливість мови мають амплітудно-частотна характеристика (АЧХ) підсилювача, рівень його шумів, параметри мікрофона, а також їх взаємна узгодженість з підсилювачем. Підсилювач з мікрофоном повинен мати коефіцієнт підсилення 60 дБ – 80 дБ (або 1000 – 10000 разів). Враховуючи особливості прийому корисного сигналу та його малу величину в умовах дії значного рівня завад, корисно в конструкції підсилювача передбачити можливість корегування АЧХ, тобто частотної селекції сигналу, який підлягає обробці. Слід також враховувати, що найбільш інформативною смугою частот є смуга в діапазоні 300 Гц – 3500 Гц, де розташовані основні форманти звуків. Використання смугового фільтра в підсилювачі дозволяє збільшити дальність прослуховування в 2 та більше разів. Ще більшої дальності можна досягти використанням у складі ПНЧ селективних фільтрів з великою добротністю, які дозволяють виділяти та придушувати сигнал на визначених частотах[2].

Сучасна елементна база дозволяє створювати сучасні ПНЧ на основі мало шумових операційних підсилювачах типу К548УН1, К548УН2, К548УН3, КР140УД12, КР140УД20 і таке інше.

Можливо також використовувати сучасні мало шумові транзистори, особливо в першому каскаді. Це можуть бути або мало шумові біполярні транзистори з високим коефіцієнтом підсилення типу КТ3102, КТ307 або польові транзистори. Велике значення мають і параметри інших елементів. Так слід використовувати оксидні конденсатори К53-1, К53-14, К50-35, неполярні КМ6, МБМ, резистори – не гірше традиційних 5% МЛТ-0,25 та МЛТ-0,125, найкращий варіант резисторів – дротові, резистори без індукції. Вхідний опір ПНЧ повинен відповідати опору джерела сигналу – мікрофона, або датчика, який його заміняє. Звичайно вхідний опір ПНЧ намагаються зробити рівним або дещо більшим опору джерела – перетворювача сигналу на основних частотах.

Для мінімізації електричних завад треба для підключення мікрофона до ПНЧ використовувати екрановані провідники мінімальної довжини. Електретний мікрофон МЕК-3 слід монтувати безпосередньо на платі першого каскаду мікрофонного підсилювача. При необхідності значного віддалення мікрофона від ПНЧ треба використовувати підсилювач з диференціальним входом, а підключення здійснювати витою парою проводів у екрані. Екран підключається до схеми в одній точці загального проводу максимально близько до першого каскаду підсилювача. Це забезпечить мінімізацію рівня наведених у проводах електричних завад.

Для підвищення направленої дії мікрофона та зниження акустичних завад використовують параболічний рефлектор, який являє собою параболічний концентратор звука. Мікрофон розташовують у цьому разі у фокус рефлектора.

Ще більший ефект може дати поєднання параболічного рефлектора з декількома спеціально розрахованими акустичними резонаторами, які виготовлені з труб. Такі акустичні резонатори виготовляють з алюмінієвих труб різної довжини. В залежності від довжини та діаметра кожна труба має свою резонансну частоту. Тому, коли їх використовується декілька, можна забезпечити підсилення у тій смузі частот, яка цікавить дослідника.

Наприклад, якщо взяти 7 труб-резонаторів з алюмінію діаметром 10 мм, то за формулою, яка дозволяє розрахувати резонансну частоту в залежності від довжини труби (L=165/f), можна підібрати потрібну довжину труби. Так, для отримання резонансної частоти 300 Гц потрібно взяти трубу довжиною 550 мм, а для частоти 1100 Гц відповідно 150 мм.

Набір, отриманих таким чином резонаторів закінчується параболічним концентратором, у фокусі якого знаходяться ці резонатори. Велика кількість резонаторів дозволяє створити мікрофон з вузькою діаграмою направленості та збільшити дальність прослуховування до 1 км і більше.

На рис. 4.16 представлений приклад ПНЧ на основі спеціалізованої мікросхеми - ИС К548УН1А, що містить 2 ОП з малим шумом. ОП й ПНЧ, створений на базі цих ОП (ІС К548УН1А), розраховані на напругу живлення 9В з однією полярністю. У наведеній схемі

ПНЧ перший ОП включений у варіанті, що забезпечує мінімальний рівень шумів ОП. Вихідні транзистори даної схеми ПНЧ працюють без початкового зсуву (з Іспокою=0). Спотворення типу "сходинка" практично відсутні завдяки глибокому негативному зворотному зв'язку, що охоплює другий ОП мікросхеми й вихідні транзистори. При необхідності зміни режиму вихідних транзисторів (Іспокою=0) схему необхідно відповідним чином відкоригувати: включити в схему резистор або діоди між базами Т1 і Т2, два резистори по 3-5к з баз транзисторів на загальний провід і провід живлення. До речі, в ПНЧ у двотактних вихідних каскадах без початкового зсуву добре працюють уже застарілі германієві транзистори. Це дозволяє використати з такою структурою вихідного каскаду ОП з відносно низькою швидкістю наростання вихідної напруги без небезпеки виникнення спотворень, пов'язаних з нульовим струмом спокою. Для виключення небезпеки збудження підсилювача на високих частотах використається конденсатор С3, підключений поруч із ОП, і ланцюжок R8C8 на виході ПНЧ (досить часто RC на виході підсилювача можна виключити). На рис.4.16.а - схема ПНЧ на ОП ІС К548УН1А. На рис. 4.16.б - схема підключення динамічного мікрофона. На рис. 4.16.в - схема підключення мікрофона МЕК-3. На рис. 4.16.г - схема підключення мікрофона до ПНЧ.

Елементи для схеми на рис. 4.16 :

R1 =240-510, R2=2.4K, R3=24k-51k (підстроювання посилення), &4=3кЮк, R5=1k-3k, R6=240K, R7=20k-100k (підстроювання посилення), R8=1G; R9=820-1.6k (для 9У);

С1=0.2-0.47, С2=10мкф-50мкф, С3=0.1, С4=4.7мкф-50мкф, С5=4.7мкф=50мкф, С6=10мкф-50мкф, С7=10мкф-50мкф, С8=0.1-0.47, С9=100мкф-500мкф;

ОП 1 і 2 - ОП ІС К548УН1А (Б), двох ОП в одному корпусі ІС; Т1, Т2 - КТ315, КТ361 або КТ3102, КТ3107 або аналогічні;

D1 - стабілітрон, наприклад, КС133, можна використати світло діод у звичайному включенні, наприклад, АЛ307;

М - МД64, МД200 (б), МЭК-3 або аналогічний (в), Т - ТМ-2А .

На рис. 4.17 представлений приклад ПНЧ на транзисторах. У перших каскадах транзистори працюють у режимі мікро струмів, що забезпечує мінімізацію внутрішніх шумів ПНЧ. Тут доцільно використати транзистори з більшим коефіцієнтом підсилення, але малим зворотним струмом. Це можуть бути, наприклад, 159НТ1 В (1кО=20нА) або КТ3102 (1кО=50нА). або аналогічні. Використання подібних транзисторів дозволяє забезпечити не тільки сталу роботу транзисторів при малих колекторних струмах, але й досягти добрих підсилювальних характеристик при низькому рівні шумів. Вихідні транзистори можуть використатися як кремнієві (КТ315 і КТ361, КТ3102 і КТ3107, і т.п.), так і германієві (МП38А и МП42Б и т.п.). Настроювання схеми зводиться до установки резистором R2 і

резистором R3 відповідної напруги на транзисторах: 1.5В - на колекторі Т2 і 1.5В - на емітерах Т5 і Т6.

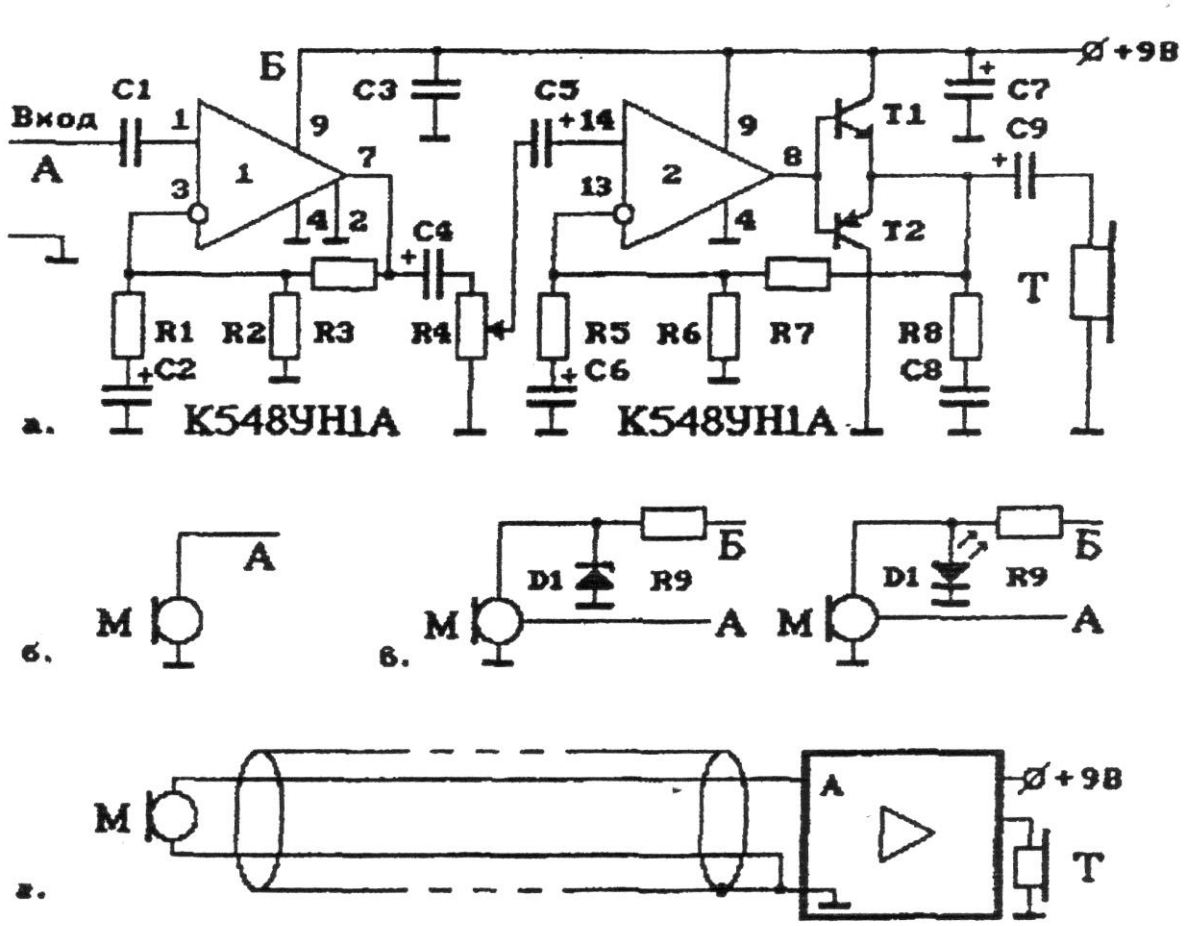


Рис. 4.16. Схема УНЧ на ОП К548УН1А і варіанти підключення мікрофонів

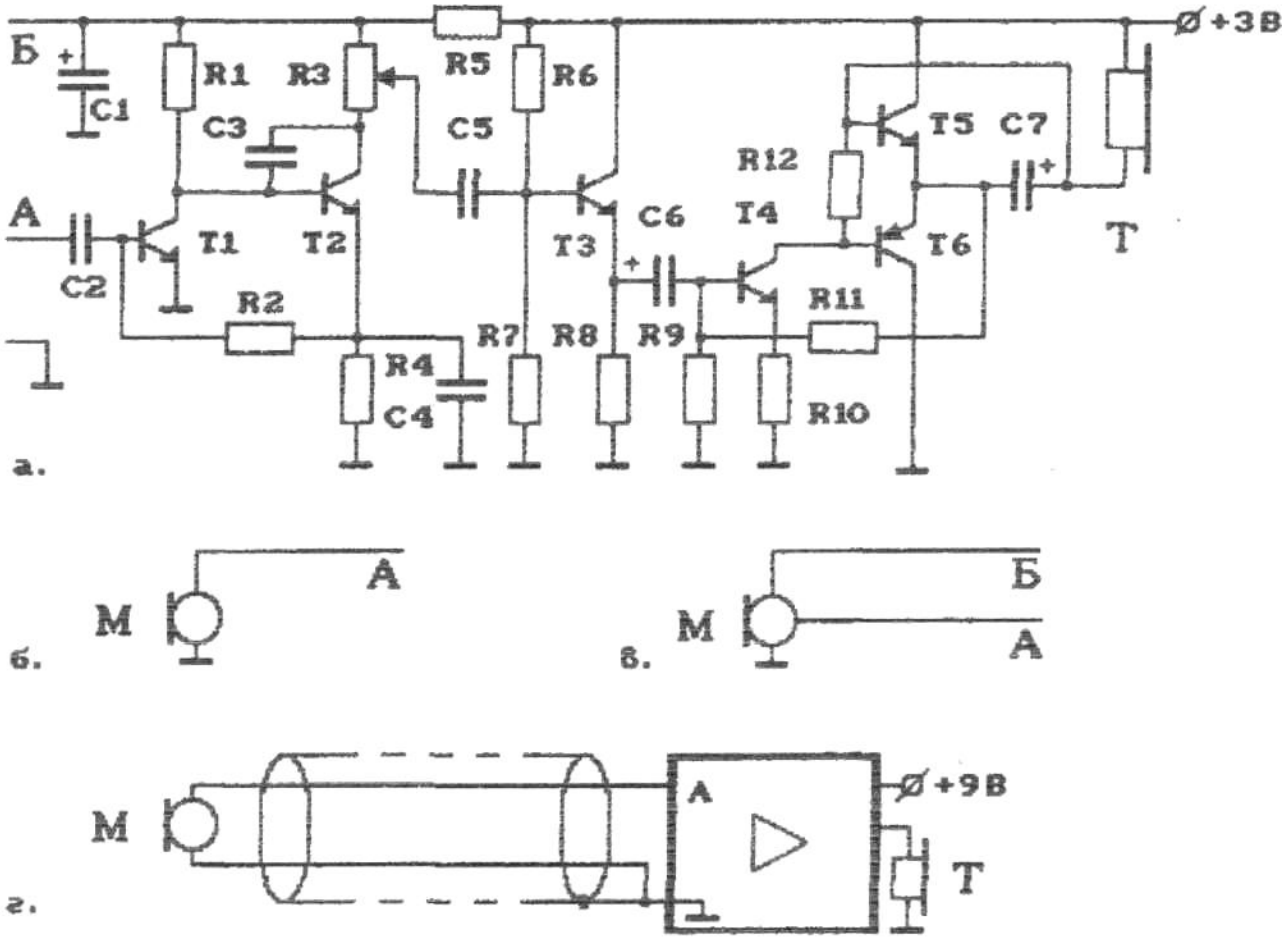


Рис. 4.17. Схема ПНЧ на транзисторах і варіанти підключення мікрофонів:

а - ПНЧ на транзисторах, б - підключення динамічного мікрофона, в - підключення електронного мікрофона, м - підключення вилученого мікрофона.

На рис. 4.17.а - схема ПНЧ на транзисторах.

На рис. 4.17.б - схема підключення динамічного мікрофона.

На рис.4.17.в - схема підключення мікрофона МЭК-3.

На рис. 4.17.г - схема підключення вилученого мікрофона до ПНЧ.

Елементи для схеми на мал. 4.17 :

R1=43к-51К, R2=51 О (підстроювання, Uкт2=1.2В-1.8В), R3=5.6К-б.8К (регулятор гучності), R4=3К, R5=750, R6=150К, R7=150К, R8=33К; R9=820-1.2К, R10=200-330, Rll = 100К (підстроювання), R 12=1К (підстроювання струму спокою Т5 і Т6, 1-2 ма);

С1 = 10мкф-50мкф, С2=0.15мкф-1мкф, СЗ=1800, С4= 10мкф-20мкф, С5=1мкф, С6=10мкФ~50мкф, С7=100мкФ~500мкф;

Т1, Т2, ТЗ - 159НТ1В, КТ3102Е або аналогічні, Т4, Т5 - КТ315 або аналогічні, але можна й МП38А, Т6 - КТ361 або аналогічні, але можна й МП42Б; М - МД64, МД200 (б), МЭК-3 або аналогічний (в), Т - ТМ-2А.

На рис. 4.18 представлений приклад ПНЧ на ОП з диференціальним входом. Правильно зібраний і настроєний ПНЧ забезпечує значне придушення синфазної перешкоди (60 дб і більше). Це забезпечує виділення корисного сигналу при значному рівні синфазних перешкод. Варто нагадати, що синфазна перешкода - перешкода, що надходить у рівних фазах на обидва входи ОП ПНЧ, наприклад, перешкода, наведена на обоє сигнальних проводів від мікрофона. Для забезпечення коректної роботи диференціального каскаду необхідно точно виконати умову: Rl =R2, R3=R4. Резистори доцільно підібрати за допомогою омметра серед 1 % - резисторів з відповідною температурною стабільністю. Для забезпечення необхідного балансу рекомендується один із чотирьох резисторів (наприклад, R2 або R4) виконати змінним. Це може бути високоточний змінний резистор-настроювач із внутрішнім редуктором. Для мінімізації шумів вхідний опір ПНЧ (значення резисторів R1 і R2) повинне відповідати опору мікрофона або його датчика, який його замінює. Вихідні транзистори ПНЧ працюють без початкового зсуву (з Іспокою=0). Спотворення типу «сходинка» практично відсутнє завдяки глибокому негативному зворотному зв'язку, що охоплює другий ОП й вихідні транзистори. При необхідності схему включення транзисторів можна змінити. Настроювання диференціального каскаду: подати синусоїдальний сигнал 50 Гц на обидва входи диференціального каналу одночасно, підбором величини R3 або R4 забезпечити на виході ОП 1 нульовий рівень сигналу 50 Гц. Для настроювання використається сигнал 50 Гц, тому що електромережа частотою 50 Гц дає максимальний внесок у сумарну величину напруги перешкоди. Хороші резистори й ретельне настроювання дозволяють досягти придушення синфазної перешкоди 60дб-80дб і більше Для підвищення стійкості роботи ПНЧ доцільно зашунтувати виводи живлення ОП конденсаторами й на виході підсилювача включити RC-ланцюжок (як у схемі підсилювача на рис. 4.10). Для цієї мети можна використати конденсатори КМ6.

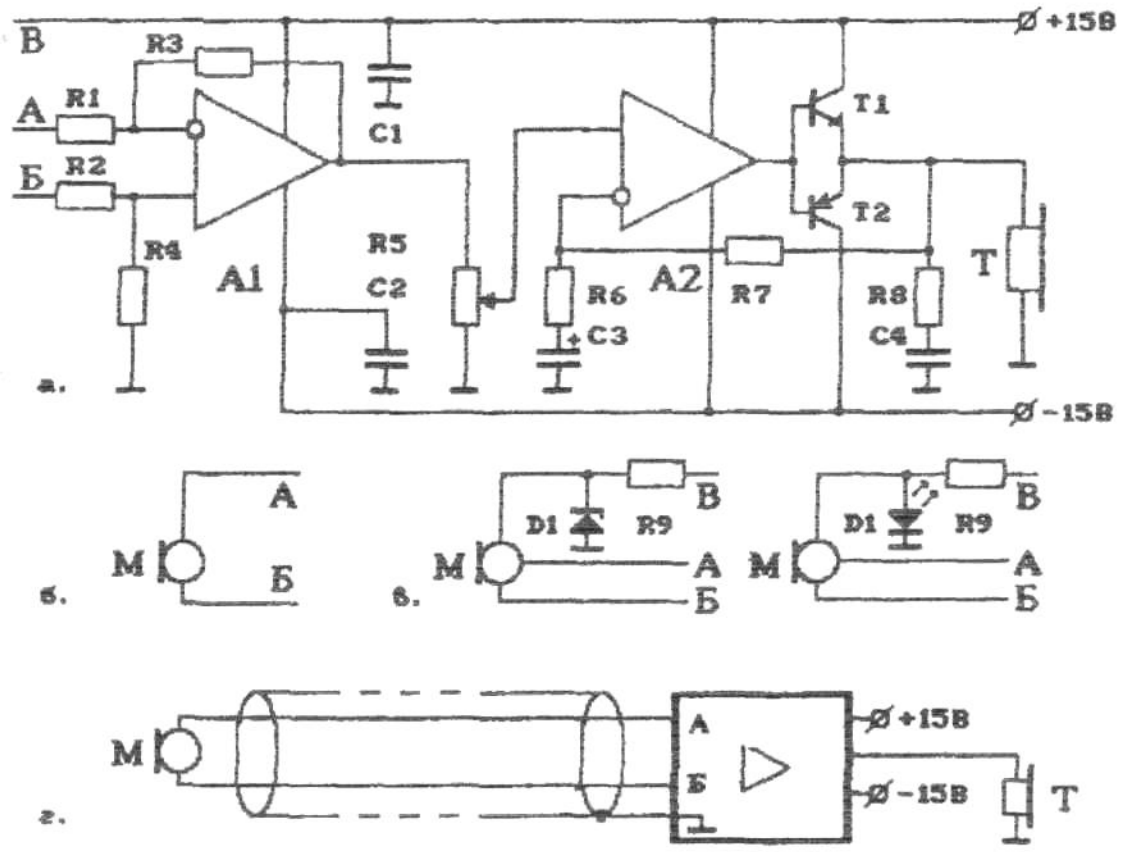


Рис. 4.18. Схема ПНЧ на ОП з диференціальним входом і варіанти підключення мікрофонів :

а - ПНЧ із диференціальним входом, б - підключення динамічного мікрофона, *в* - підключення електретного мікрофона, м - підключення вилученого мікрофона

Елементи для схеми на рис. 4.18:

Rl=R2=20К (дорівнює або трохи вище максимального опору джерела в робочому діапазоні частот), R3=R4=1М-2М, R5=2до-10К, R6=1К-3К, R7=47К-300К (підстроювання посилення, К=l+R7/R6), R8=10, R9=1.2К-2.4К;

З1-0.1-0 22, 02=0.1-0.22, СЗ=4.7мкф-20мкф, З4=0.1;

ОП - КР1407УД2, КР140УД20, КР1401УД2Б, К140УД8 або інші ОП в типовому включенні, бажано із внутрішньою корекцією:

Tl, Т2-КТ3102, КТ3107або КТ315, КТ361, або аналогічні:

D1 - стабілітрон, наприклад, КС133, можна використати світло діод у звичайному включенні, наприклад, АЛ307;

М - МД64, МД200 (б), МЕК-3 або аналогічний (в), Т - ТМ-2А .

Застосування у вихідних каскадах ПНЧ ОП з низькою швидкістю та експлуатація кремнієвих транзисторів у підсилювачах потужності в режимі без початкового зсуву (струм спокою дорівнює нулю - режим В) може, як це вже відзначалося вище, привести до перехідних спотворень типу "сходинка". У цьому випадку для виключення даних спотворень

доцільно змінити структуру вихідного каскаду таким чином, щоб вихідні транзистори працювали з невеликим початковим струмом (режим АВ).

На рис 4.19 представлений приклад подібної модернізації наведеної схеми підсилювача з диференціальним входом.

Елементи для схеми на рис. 4.19 :

Rl=R2=20K (дорівнює або трохи вище максимального опору джерела в робочому діапазоні частот), R3=R4=1M-2M; P5=2к-10к, R6=1к-3k, P7=47к-300к (підстроювання посилення, K=l+R7/R6), R8=10, P10=10к-20к, Rll = l0к-20к:

Cl =0.1-0.22. C2=0 1-0.22, C3=4.7мкф-20мкф, C4=0.1;

ОП -К140УД8, КР1407УД2, КР140УД12, КР140УД20, КР1401УД2Б або інші ОП в типовому включенні й бажано із внутрішньою корекцією:

T1, T2 - КТ3102. КТ3107 або КТ315, КТ361, або аналогічні,

D2.D3 - КД523 або аналогічні,

М - МД64, МД200, МЭК-3 або аналогічний (в),

Т - ТМ-2А .

На рис 4.19 представлений приклад ПНЧ на транзисторах. У перших каскадах транзистори працюють у режимі мікро струмів, що забезпечує мінімізацію шумів ПНЧ. Схема багато в чому аналогічна схемі на рис 4.17. Для збільшення відношення корисного сигналу низького рівня до перешкод у схему ПНЧ включений смуговий фільтр, що забезпечує виділення частот у смузі 300 Гц -3.5 кГц. У даній схемі також доцільно використати транзистори з більшим коефіцієнтом підсилення, але малим зворотним струмом колектора (1к0), наприклад, 159НТ1У (1к0=20на) або КТ3102 (1к0=50на), або аналогічні. Вихідні транзистори можуть використатися як кремнієві (КТ315 і КТ361, КТ3102 і КТ3107, ит.п.),так і германієві (застарілі транзистори МП38А и МП42Б и т.п.)- Настроювання схеми, як і у випадку схеми ПНЧ на рис. 4.19, зводиться до установки резистором R2 і резистором R3 відповідних напруг на транзисторах Т2 і Т5, Т6 : 1.5В - на колекторі Т2 і 1.5В - на емітерах Т5 і Т6.

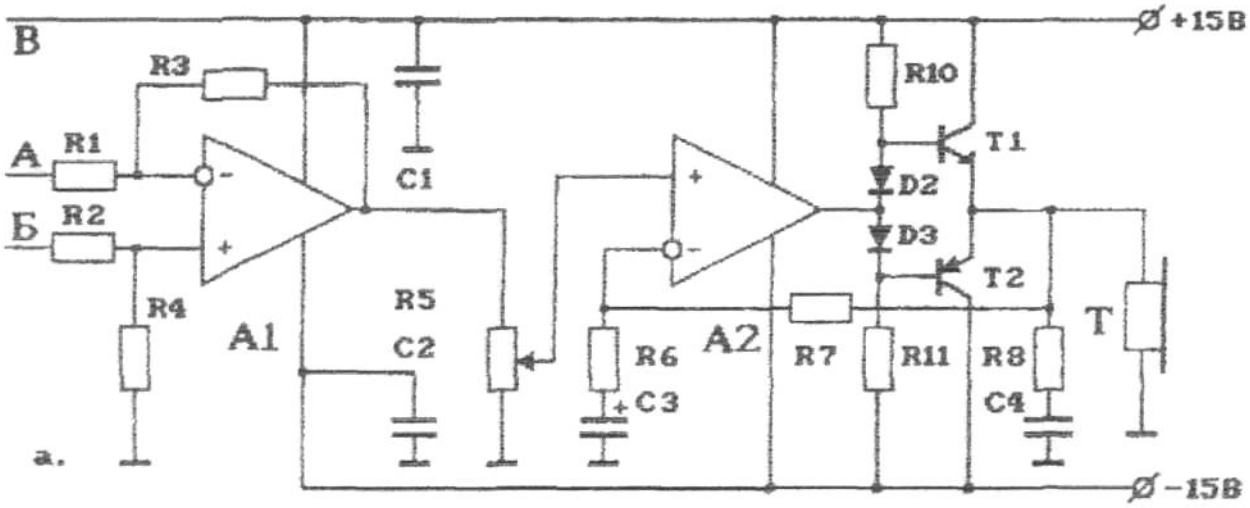


Рис. 4.19. Схема ПНЧ на ОП з диференціальним входом і з низьким рівнем спотворень вихідного каскаду.

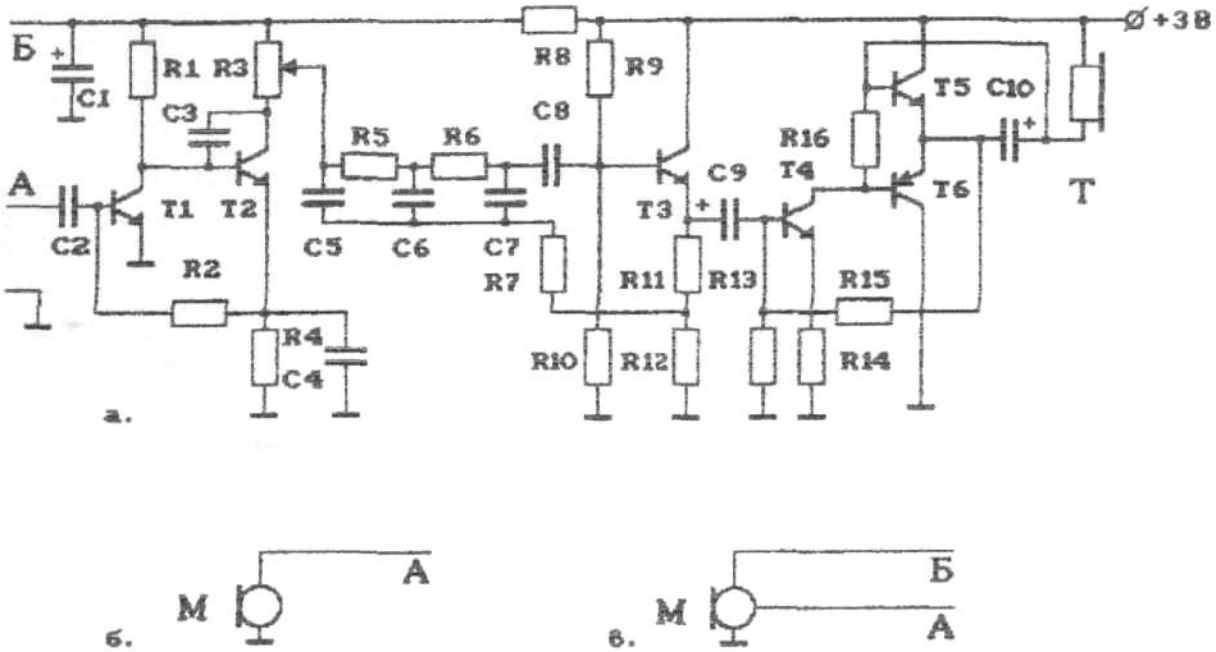


Рис. 4.20. Схема ПНЧ на транзисторах зі смуговим фільтром і варіанти підключення мікрофонів:

а - ПНЧ зі смуговим фільтром,

б - підключення динамічного мікрофона,

в - підключення электретного мікрофона.

На рис. 4.20.а - схема ПНЧ на транзисторах зі смуговим фільтром. На рис. 4.20.б - схема підключення динамічного мікрофона.

На рис. 4.20.в - схема підключення электретного мікрофона МЕК-3, МЕК-333 та аналогічних.

Елементи для схеми на рис. 4.20 :

R1=43к-51к, R2=510к (підстроювання), R3=5.6к-6.8к (регулятор гучності), R4=3К, R5=8.2К, R6=8.2К, R7=180, R8=750; R9=150К, R10=150К, R11 = 33К, R12=620, R 13=820-1 2к, R14=20G-330, R15 = 100К (підстроювання), R16=1К (підстроювання струму спокою Т5 і Т6, 1-2ма);

С1 = 10мкф-50мкф,С2=0.15-0.33,СЗ=1800, С4-10мкф-20мкф, С5=0.022, С6-0.022, С7=0.022, С8=1мкф, С9=10мкф-20мкф, С10=100мкф-500мкф;

Т1.Т2.ТЗ-159НТ1В, КТ3102Е або аналогічні;

Т4, Т5 - КТ3102, КТ315 або аналогічні, але можна й застарілі, германієві транзистори, наприклад, МП38А,

Т6 - КТ3107 (якщо Т5 - КТ3102), КТ361 (якщо Т5 - КТ315) або аналогічні, але можна й застарілі, германієві транзистори, наприклад, МП42Б (якщо Т5-МП38А);

М - МД64, МД200 (б), МЕК-3 або аналогічний (в), Т - ТМ-2А

Замість смугового фільтра іноді можна використати традиційні, з двома смугами регулятори тембру НЧ і ВЧ але, як правило, з гіршим результатом придушення завад, ніж смугові фільтри.

На рис. 4.21 представлений один із численних прикладів схем регуляторів тембру НЧ і ВЧ для ПНЧ на транзисторах. Наведеній електронній схемі передує каскад з низьким вихідним опором, наприклад, емітерний повторювач (каскад із загальним колектором) або ОП. Це забезпечує низький вихідний опір попереднього каскаду й нормальну роботу даного регулятора.

Елементи для схеми на рис 4.21 :

R1=47к, R2 = 100к, R3=47к, R4=39к. R5=5.6к, R6=100к, R7=180к, R8 = 33к, R9=3.9к, R1О=1к,

С1 = 39н, С2=ЗОмкФ-100мкф, СЗ=5мкф-20мкф, С4=2.2н, С5=2.2н. С6=ЗОмкФ-100мкФ:

Т1 - КТ3102, КТ315 або аналогічні.

На рис 4.22 представлений приклад схеми регулятора тембру НЧ і ВЧ для ПНЧ на ОП з двома смугами. Даній електронній схемі передує каскад на ОП. Це забезпечує низький вихідний опір попереднього каскаду й нормальну роботу даного регулятора. Для підвищення стійкості роботи схеми (на ВЧ) доцільно зашунтувати виводи живлення ОП конденсаторами 0.1 мкф, наприклад, типу КМ6, Конденсатори підключаються максимально близько до ОП.

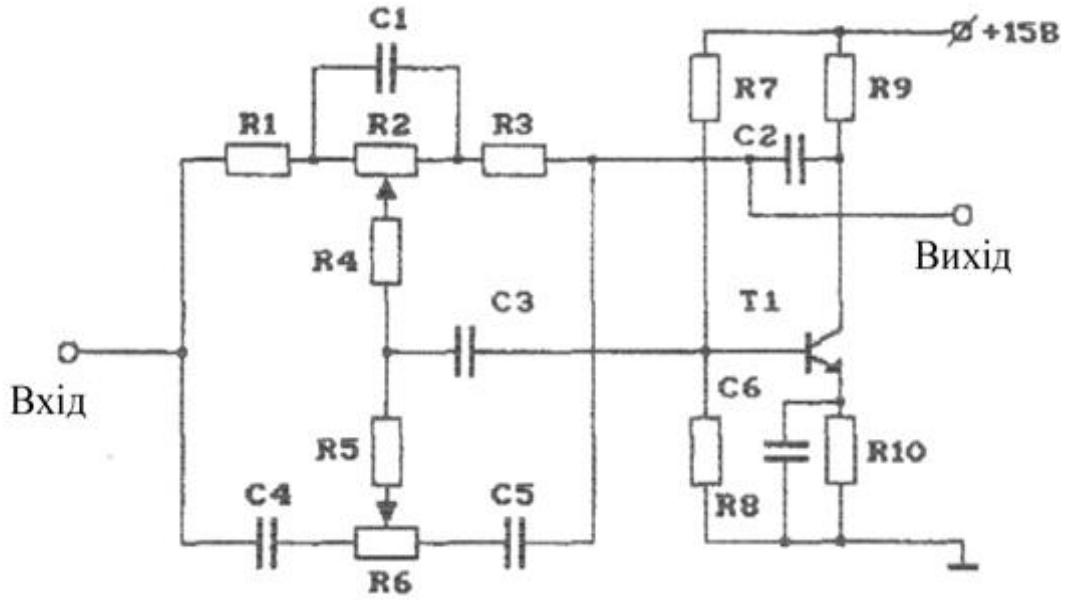


Рис. 4.21. Схема регулятора тембру (НЧ, ВЧ) на транзисторі з двома смугами.

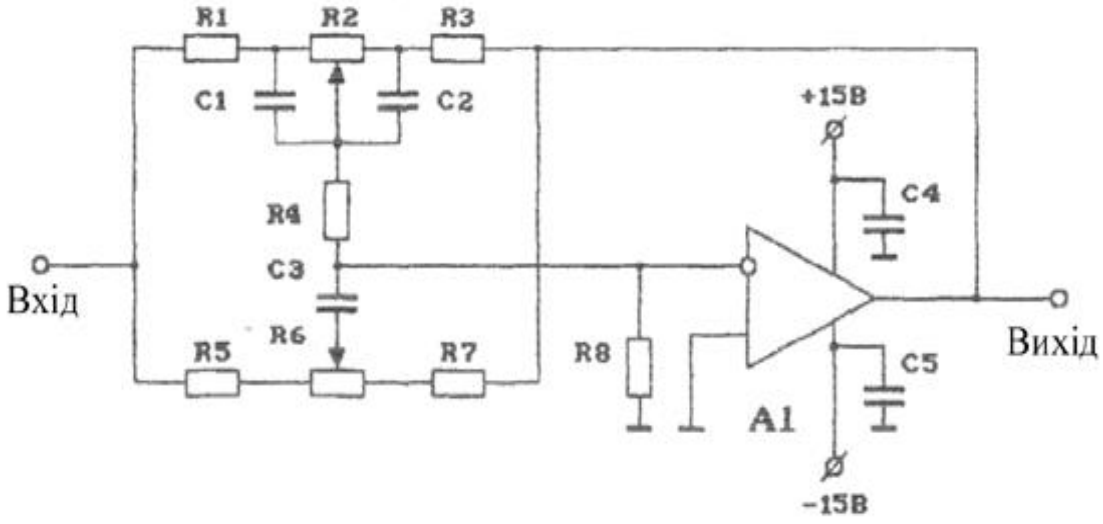


Рис. 4.22. Схема регулятора тембру (НЧ, ВЧ) на ОП з двома смугами.

Елементи для схеми на рис. 4.22:

R1 = 11к,R2=1ООк, R3 = 11к,R4=11к,R5=3.6к,R6=5ООк, R7=3.6к, R8=750;

С1=005мкф, С2=0.05мкф, СЗ=0.005мкф, С4=0,1 мкф-0.47нкф, С5=0.1 мкф-0.47мкф;

ОП - 140УД12, 140УД20, 140УД8 або будь-які інші ОП в типовому включенні й бажано із внутрішньою корекцією;

Регулятор тембру з трьома смугами дає кращий результат придушення завад, ніж регулятор з двома смугами.

На рис. 4.22 представлений приклад схеми регулятора тембру НЧ, СЧ і ВЧ для ПНЧ на ОП з трьома смугами. Даній електронній схемі передує каскад на ОП. Це забезпечує

низький вихідний опір попереднього каскаду й нормальну роботу даного регулятора. Для підвищення стійкості роботи схеми (на ВЧ) доцільно зробити шунтування виводів живлення ОП конденсаторами 0.1 мкф. Конденсатори підключаються максимально близько до ОП.

Елементи для схеми на рис. 4.24 :

R1 = 11к, R2=100к, R3 = 11к, R4=11к, R5=1.8к, R6=500к, R7=1.8к, R8=280, R9=3.6к, R10=100к , R11 = 3.6к.

C1 = 0.05 мкф, C2 – відсутній, C3 = 0.005 мкф, C4 = 0.1 мкф – 0.47 мкф, C5 = 0.1 мкф – 0.47 мкф, C6 = 0.005 мкф, C7 = 0.0022 мкф, C8 = 0.001 мкф.

ОП – 140УД8, 140УД20, або будь-які інші із внутрішньою корекцією.

4.4.2. Лазерні мікрофони

У тому випадку, якщо ви підняли скло в автомобілі чи закрили кватирку, може бути використаний лазерний мікрофон. Перші їхні зразки були прийняті на озброєння американськими спецслужбами ще в 60-і роки. Як приклад розглянемо лазерний мікрофон ПР-150 фірми "Hewlett-Packard" з дальністю дії до 1000 м. Він сконструйований на основі гелій-неонового чи напівпровідникового лазера з довжиною хвилі 0.63 мкм (тобто у видимому діапазоні; сучасні пристрої використовують невидимий 14 діапазон). Промінь лазера, відбитий від скла приміщення, у якому ведуться переговори, виявляється промодульованим звуковою частотою. Прийнятий фотоприймачем відбитий промінь детектується. звук підсилюється і записується. Приймач і передавач виконані окремо, є блок компенсації перешкод. Вся апаратура розміщена в кейсі і має автономне живлення. Подібні системи мають дуже високу вартість (більш $10 тис.) і крім того, вимагають спеціального навчання персоналу і використання комп'ютерної обробки мови для збільшення дальності. Існує вітчизняна система ЛСТ-ЛЛ2 з дальністю дії менше 100 м і досить скромною вартістю. Слід зазначити, що ефективність застосування такої системи зростає зі зменшенням освітленості оперативного простору.

На рис. 4.23.а наведений приклад схеми використання лазерного мікрофона, що складається із лазера з оптичною системою, фотоприймача й відповідних електронних пристроїв. Лазерний мікрофон дозволяє здійснювати дистанційне прослуховування приміщень по коливаннях шибки (О. Скла). Дані коливання модулюють промінь лазера, що відбивається від поверхні скла й попадають на фотоприймач (Ф. приймач) для відповідного перетворення й декодування за допомогою електронних пристроїв.

Існують різні системи лазерних мікрофонів, що відрізняються складом і схемами використання.

На рис. 4.23.б і рис.4.23.в у представлені приклади схем інфрачервоних передавача (Іч - передавача) і приймача (Іч - приймача). Дані пристрої дозволяють "зчитувати" акустичну

інформацію із шибки (звукові коливання шибки), що дозволяє, як і у випадку лазерного мікрофона, здійснювати дистанційне прослуховування приміщень. Для цього сфальцьований промінь Іч - передавач направляється на шибку. Іч - приймач приймає сигнал з модуляцією.

Елементи для схеми Іч - передавача на мал. 4.23.б:

R1 =50к-100к (R1 і C1 задають частоту генератора несучої – 30кГц-60кГц), R2=lк, R3=8-10к (задає струм через Іч –світло діод, середній струм через діод -250мА-300мА) :

C1 = 150, C2=1000мкф-4000мкф ,

DD1 (DD1.1, DD1.2) - К561 ;

Т1 - КТ3102, КТ315 або аналогічні транзистори;

Т2 - КТ815, КТ807, КТ801 або аналогічні, можливе використання замість Т1 і Т2 одного транзистори КТ827.

Елементи для схеми Іч - приймача на рис. 4.23.в :

R1 =100-500 (регулювання чутливості ОП1: K=l +R3/R1), R2=200к-300к, R3=300к-500к, R4=30к-100к (регулювання гучності), R5=1к-5к (регулювання чутливості ОП2: K=l+R7/R5), R6=200к-300к, R7=10к-50к, R8=10, R9=300к-500к, R10=300к-500М, R11 = 16К-24к (R11 і C4 можуть бути виключені зі схеми, у цьому випадку R4=16к-25к);

C1=0.1-0.2, C3=0.1-0.3,З4=0.3-5мкф, C5=1мкф-10мкф, C6=5мкф-20мкф,

C7=50мкф-500мкф,C8=0.1,C9=100мкф-500мкф,C10 = 0.1-0.2, C11=0.3-1мкф,

C12=9н-15н;

L1 C2 налаштовується на частоту 30-50 кГц, L1 - 400-500 витків ПЕЛ 0.05-0.07 на каркасі від фільтра ПЧ радіоприймача.

D1 - ФДК261 або аналогічний Іч –фото діод;

D2, D3 - ГД507 або аналогічні (германієві - менше поріг);

А1.А2 – ОП КР548УН1А;

Т1, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

Т - ТМ-2А або аналогічні.

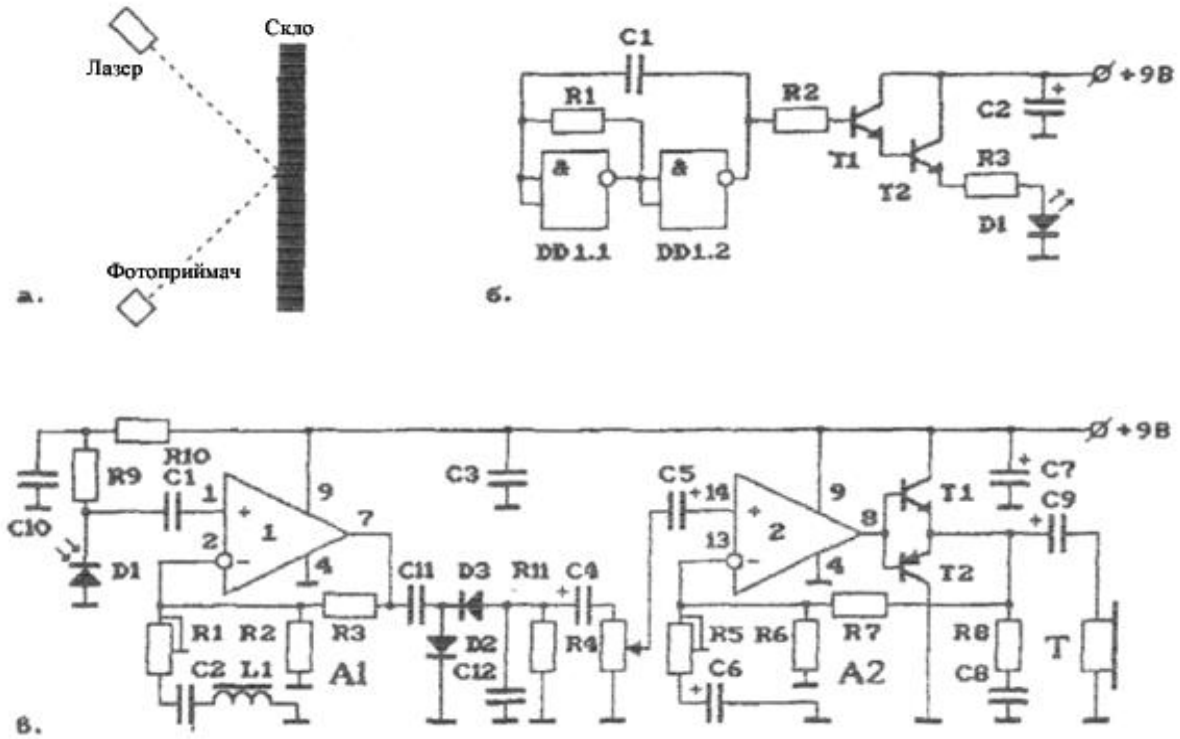


Рис. 4.23. Лазерний мікрофон і інфрачервоний приймач передавач :

а - схема використання лазерного мікрофона,
б - Іч-передавач,
в - Іч - приймач на 2 ОП.

4.4.3. Гідроакустичні датчики

Звукові хвилі поширюються у воді з дуже невеликим загасанням. Гідроакустики ВМФ навчилися прослухувати шепіт у підвідних човнах, що знаходяться на глибині десятків метрів. Цей же принцип можна застосовувати, використовуючи рідину, що знаходиться в системах водопостачання і каналізації. Таку інформацію можна перехоплювати в межах будинку, але радіус прослуховування буде дуже сильно залежати від рівня шумів, особливо у водопроводі. Переважніше використовувати датчик, встановлений у батареї опалення. Ще більш ефективним буде використання гідроакустичного передавача, встановленого в батареї приміщення, що прослухується.

4.4.4. ПВЧ та ІЧ передавачі

Для підвищення скритності в останні роки стали використовувати інфрачервоний канал. Як передавач звуку від мікрофона використовується напівпровідниковий лазер. Як приклад розглянемо пристрій TRM-1830. Дальність дії вдень складає 150 м. уночі - 400 м. час безупинної роботи - 20 годин. Габарити не перевищують 26х22х20 мм. До недоліків подібної системи можна віднести необхідність прямої видимості між передавачем і

приймачем і вплив перешкод. Підвищити скритність одержання інформації можна також за допомогою використання каналу НВЧ діапазону - більш 10 ГГц. Передавач, виконаний на діоді Ганца, може мати дуже невеликі габарити. До переваг такої системи можна віднести відсутність перешкод, простоту і відсутність у даний час ефективних засобів контролю. До недоліків варто віднести необхідність прямої видимості, хоча й у меншому ступені, тому що НВЧ сигнал може все-таки обгинати невеликі перешкоди і проходить (з ослабленням) крізь тонкі діелектрики, наприклад, штори на вікнах.

4.4.5. Стетоскопи

Стетоскоп являють собою вібродатчик, підсилювач і головні телефони. Вібродатчик спеціальною мастикою прикріплюється до стіни, стелі і т. ін. Розміри датчика, на прикладі пристрою DTI. складають 2.2х0.8 см., діапазон частот - 300-3000 Гц, вага – 126г, коефіцієнт підсилення - 20000. За допомогою подібних пристроїв можна здійснювати прослуховування розмови через стіни товщиною до 1 м. Стетоскоп може оснащуватися проводом, радіо чи іншим каналом передачі інформації. Основною перевагою стетоскопа можна вважати труднощі виявлення, тому що він може встановлюватися в сусідніх приміщеннях. Як приклад приведемо два пристрої - SIPE RS і SIPE OPTO2000, що відрізняються каналом передачі. Мікрофон-стетоскоп розміром 2х3 см забезпечує прослуховування через стіни товщиною до 50 см і віконні рами з подвійними стеклами. Потужність передавача SIPE RS - 20 мВт. дальність - 250 м. Розміри передавача складають 44х32х14 мм, маса – 41г. час безупинної роботи - 90 годин. ІЧ система SIPE OPTO 2000 забезпечує радіус дії 500 м і має широку діаграму спрямованості. Існують стетоскопи, у яких чуттєвий елемент, підсилювач і радіопередавач об'єднані в одному корпусі. При дуже невеликих габаритах радіо стетоскоп досить прикріпити за допомогою спеціальної липкої маси до стіни, підлоги чи стелі в сусіднім приміщенні. Стетоскоп АД-50 дозволяє не тільки прослухувати розмови через стіни, віконні рами, двері, але і передавати інформацію по радіоканалу. Має високу чутливість і забезпечує гарну розбірливість мовного сигналу. Робоча частота складає 470 МГц. Дальність передачі - до 100 м. Час безупинної роботи - 24 години, розміри - 40х23 мм Більшістю фахівців прогнозується постійний ріст випадків застосування стетоскопів, що насамперед пояснюється зручністю застосування подібної техніки, а також тим, що їх надзвичайно важко знайти.

На аматорському рівні вирішити проблему застосування стетоскопів можна таким чином. Треба, просто, взяти п’єзокристал та приклеїти його епоксидним клеєм до стіни а потім підключити його до підсилювача короткими провідниками. У якості мікрофонів-стетоскопів краще використовувати великі та плоскі п’єзокристали. Знайти такий

п’єзокристал можна в звичайному застарілому програвачі (ГЗП-308), електронних годинниках, іграшках (ЗП-1, ЗП-22 і таке інше).

Нижче наведені приклади схемної реалізації ПНЧ з малим шумом, які застосовуються для мікрофонів-стетоскопів.

На рис. 4.24 представлена схема простого ПНЧ із високим вхідним опором і подвійним джерелом живлення. Джерелом сигналу служить п’єэозлемент або п’езовипромінювач. Мікрофон-стетоскоп. R4C4, С2, СЗ забезпечують стійкість ПНЧ (на ВЧ). Конденсатори С2, СЗ розміщають максимально близько до ОП

Елементи для схеми на рис. 4.24 :

R1 =100К-1М (регулювання гучності), R2=l0к-20к (регулювання чутливості), R3=1М-2М, R4=10:

С1=0.1мкф-1.0мкф, С2=0.1 – 0.3мкф, СЗ=0.1 – 0.3мкф, С4=0.1мкф;

Al - ОП - 140УД12, 140УД20, 140УД8 або будь-які інші ОП Із внутрішньою корекцією;

Т1, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

В1 - п’єзоелемент ГЗП-308, ПЭ-1 або аналогічні;

В2- п’єзовипромінювач ЗГИ, ЗП-22 або аналогічні. Т - ТМ-2А або аналогічні.

На рис. 4.25 представлено схему простого ПНЧ із високим вхідним опором і одним джерелом живлення. Джерелом сигналу служить п’єзоелемент або п’езовипромінювач. Мікрофон-стетоскоп. R4C4, С2 забезпечують стійкість ПНЧ (на ВЧ). Конденсатор С2 розміщають максимально близько до ОП.

Елементи для схеми на рис. 4.25:

Rl = l00к-1 м (регулювання гучності), R2=l0к-20к (регулювання чутливості), R3=1м-2м, R4=10, R5=R6=1М-2М;

С1=0.1мкф-1.0мкф, С2=0.1 – 1.3мкф, С4=0.1мкф, С5=0.1мкф-1.0мкф;

АЧ - ОП - 140УД8, 140УД12, 140УД20 або будь-які інші ОП із внутрішньою корекцією (бажано) і в типовому включенні;

Т1, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

В1 - п’єзоелемент ГЗП-308, ПЭ-1 або аналогічні ;

В2 - п’езовипромінювач ЗП-1, ЗП-22 або аналогічні ; Т - ТМ-2А або аналогічні.

На мал. 4.26 представлена схема ПНЧ із високим вхідним опором, подвійним джерелом живлення й коректором АЧХ. Джерелом сигналу служить п’єзоелемент або п’езовипромінювач. Мікрофон-стетоскоп з досить високими параметрами. Перший каскад ПНЧ (ОП А1) забезпечує попереднє посилення сигналу й узгодження з коректором АЧХ.

Після коректора й регулятора гучності сигнал подається на підсилювач потужності на ОП А2 і Т1 і Т2. На виході - телефон або динамічний гучномовець (Т1 і Т2 - КТ502 і КТ503). R8, С4, С5, С6, С7, С8 забезпечують стійкість ПНЧ (на ВЧ). Конденсатори С5, С6, С7, С8 розміщають максимально близько до ОП. С2, R5 забезпечують гальванічну розв'язку між ОП А2 і попередньою схемою. Це мінімізує розбаланс нуля на виході ОП А2. Підключення датчика до ПНЧ здійснюється за допомогою екранованого проводу.

Елементи для схеми на рис. 4.26 :

R 1 =100к-1 м, R2=l0к-20к (регулювання чутливості), R3=100k-200k, R4=5к-100к (регулювання гучності), R5=lOOк-1 м (R5>>R4), R6=l Ок-20до (регулювання чутливості), R7=100k-200k, R8=10;

Cl =0.1 мкф-1.0мкф, С2=0.1 мкф-1.0мкф, СЗ=0.1 мкф-1.0мкф, С4=0.1 мкф, С5=0.1 – 0.3мкф, С6=0.1 – 0.3мкф, С7=0.1 – 0.3мкф, С8=0.1 – 0.3мкф;

А1 - ОП - 140УД8, 140УД12, 140УД20 або будь-які Інші ОП із внутрішньою корекцією (бажано) і в типовому включенні;

Т1, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

В1- п’єзоелемент ГЗП-308, ПЭ-1 або аналогічні ;

В2- п’єзовипромінювач ЗП-1, ЗП-22 або аналогічні ; Т - ТМ-2А або аналогічні.

Цей же експеримент можна повторити, але вже із шибкою. У цьому випадку п’єзокристал кріпиться до скла. При цьому для забезпечення скритності п’єзокристал кріпиться до скла близько у рамі. Прикріпити його до скла можна й з боку вулиці. При цьому добре чутно все, що відбувається в кімнаті. Непогано чутно навіть якщо прикріпити кристал до зовнішнього скла у випадку подвійної рами. Навіть подвійна рама не захищає повністю! І можна повірити, що при використанні п’єзокристала щодо великої площі (1-2 кв. см), з малим шумом й чутливого підсилювача звук буде досить голосним і виразним.

Аналогічний досвід може бути проведений зі столом. Виявляється, традиційна ДСП - плита стола із прикріпленим п’єзокристалом може бути прекрасним мікрофоном, що забезпечує гарну якість звуку.

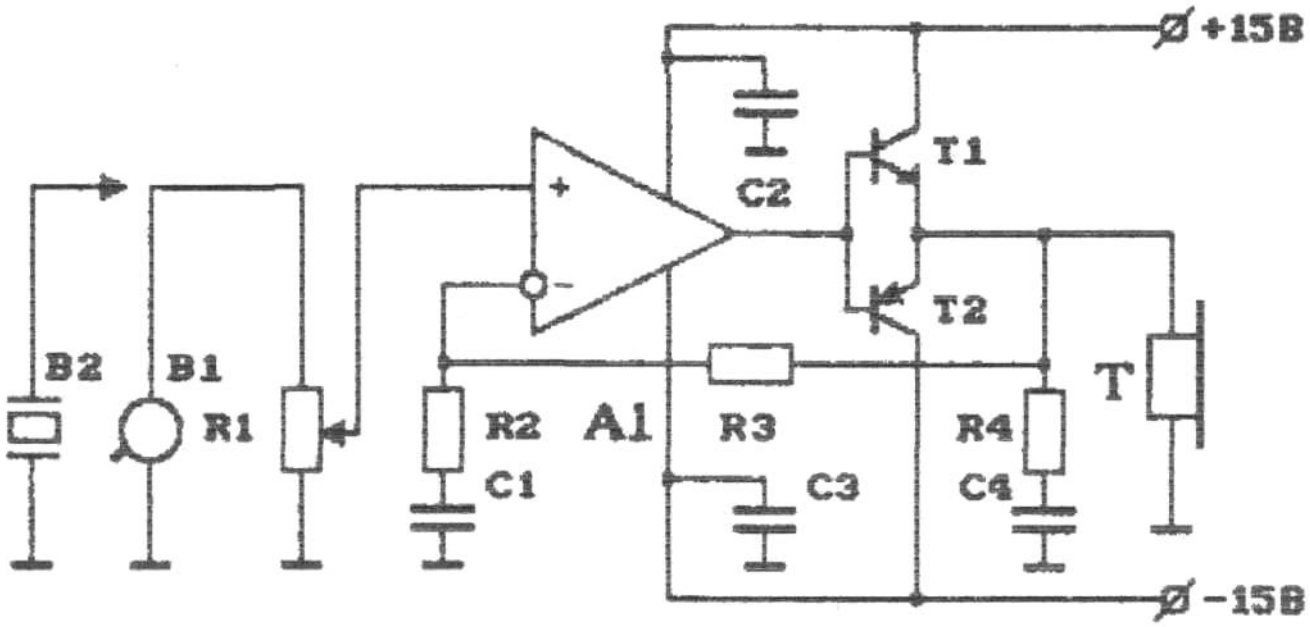


Рис.4.24. Схема простого ПНЧ із високим вхідним опором і дво полярним джерелом живлення. (Мікрофон-стетоскоп).

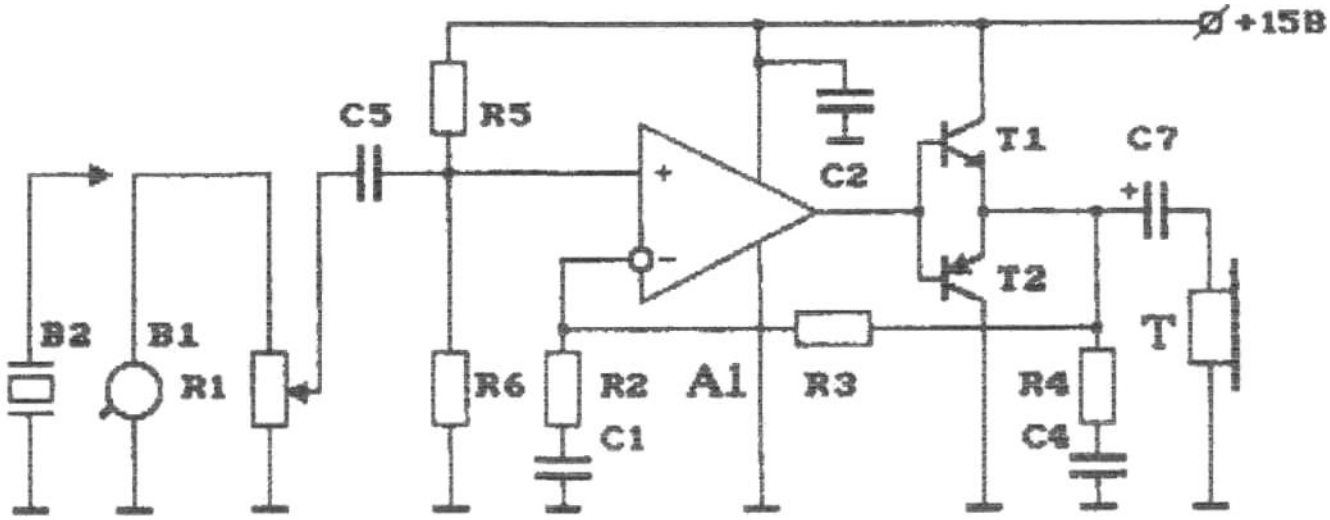


Рис. 4.25. Схема простого ПНЧ із високим вхідним опором і одно полярним джерелом живлення. (Мікрофон-стетоскоп).

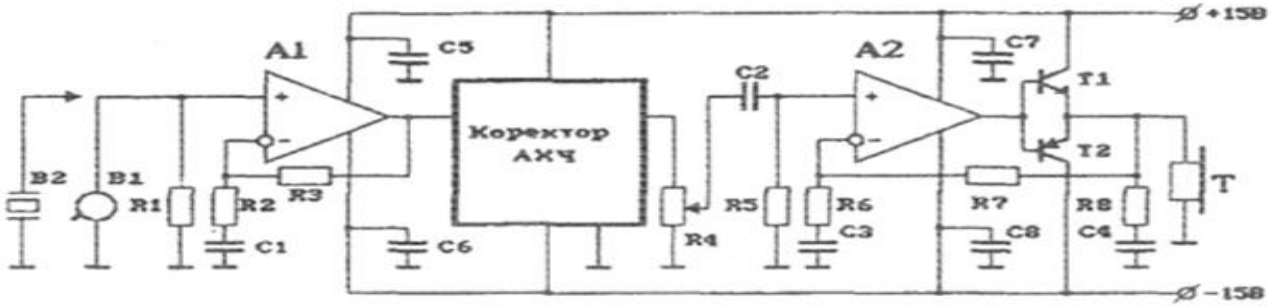


Рис. 4.26. Схема простого ПНЧ із високим вхідним опором, дво полярним джерелом живлення та коректором АЧХ. (Мікрофон-стетоскоп).

На рис. 4.27. а представлена схема ПНЧ із диференціальним входом, високим вхідним опором, подвійним джерелом живлення й коректором АЧХ. Джерелом сигналу служить п’єзоелемент або п’єзовипромінювач. Мікрофон-стетоскоп з досить високими параметрами. Перший каскад ПНЧ (ОП А1) забезпечує попереднє підсилення сигналу при ослабленні синфазної складової завади, а також узгодження з коректором АЧХ. Після коректора АХЧ і наступного регулятора гучності сигнал подається на підсилювач потужності на ОП А2 і Т1 і Т2. На виході - телефон або динамічний гучномовець (Т1 і Т2 - КТ502 і КТ503). R8, С4, С5, С6, $С7_7$ С8 забезпечують стійкість ПНЧ. Конденсатори С5, С6, С7, С8 розміщають максимально близько до ОП. С2, R5 забезпечують гальванічну розв'язку між ОП А2 і попередньою схемою. Це мінімізує розбаланс нуля на виході ОП А2. Для забезпечення коректної роботи диференціального підсилювача необхідно виконати умову R1=R2, R3 = R4 (або точніше R3/R1=R4/ R2) з максимальною точністю (1%, 0.1% і т.д.): чим точніше, тим краще. Для забезпечення необхідного балансу рекомендується один з резисторів виконати змінним, як такий змінний резистор доцільно використати високоточний резистор-настроювач із внутрішнім редуктором. Підключення датчика до ПНЧ здійснюється за допомогою крученої пари в екрані.

Елементи для схеми на мал. 4.27.а :

Rl=R2=100к-500к, R3=P4=1м-5м, R0=5к-100к (регулювання гучності), R5=100к-1м (R5>>RO), R6=10к-20к (регулювання чутливості), R7=100к-200к, R8=10;

С1 відсутній, С2=0.1мкф-1.0мкф, СЗ=0.1мкф-1.0мкф, С4=0.1мкф, С5=0.1 – 0.3мкф, С6=0.1 -0.3 кф, С7=0.1мкф – 0.3мкф, С8=0.1 – 0.3мкф;

А1 - ОП - 140УД8, 140УД12, 140УД20 або будь-які інші ОП із внутрішньою корекцією (бажано) і в типовому включенні;

Т1, Т2 - КТ3102, КТ3107 або КТ315, КТ361, або аналогічні комплементарні (парні) транзистори;

В1- п’єзоелемент ГЗП-308, ПЭ-1 або аналогічні ;

В2- п’єзовипромінювач ЗП-1, ЗП-22 або аналогічні ; Т - ТМ-2А або аналогічні.

На рис. 4.24.б - схема підключення віддаленого п’єзодатчика (п’єзоелементу або п’єзовипромінювача) до підсилювача з диференціальним входом та високим вхідним опором - ПНЧ, схема якого представлена на рис.4.27.а.

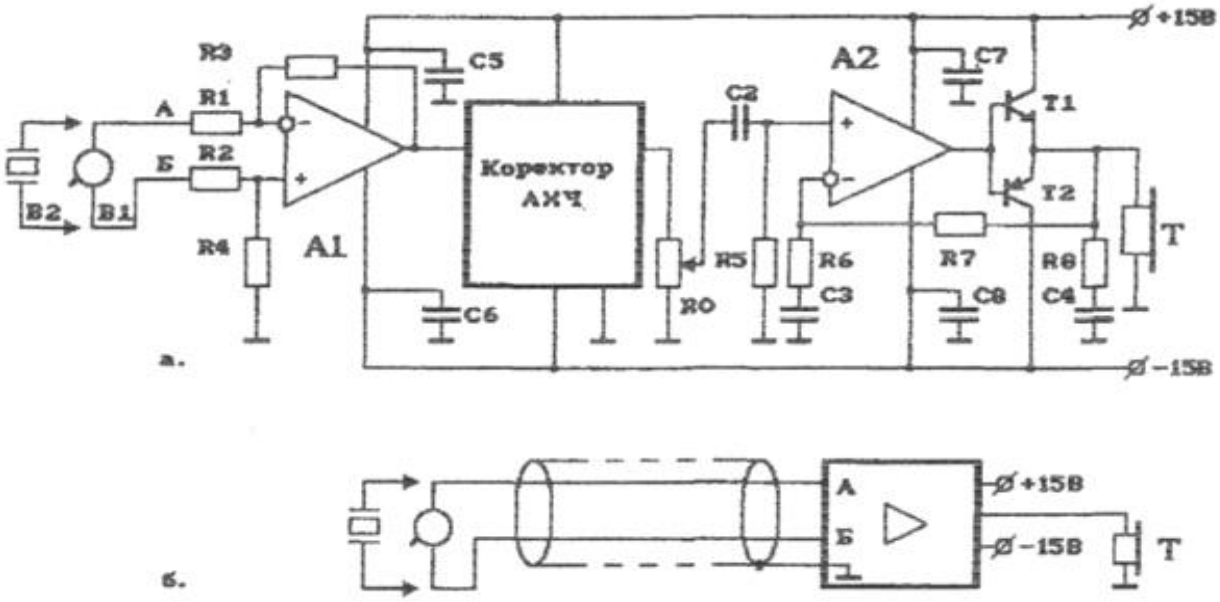


Рис. 4.27. Схема простого ПНЧ із високим вхідним опором, диференціальним входом, дво полярним джерелом живлення, коректором АЧХ (а) і підключенням вилученого п’єзодатчика (б). (Мікрофон-стетоскоп).

4.5. Системи і пристрої відеоконтролю

4.5.1. Загальна інформація

Системи і пристрої відео контролю одержали могутній імпульс свого розвитку в зв'язку зі створенням мініатюрних відеокамер і відеомагнітофонів. Якщо історія застосування фотокамер у розвідці нараховує 90-100 років, то застосування відеотехніки стримувалося неприйнятними її габаритами та вагою. В даний час габарити відеокамер (без відеомагнітофонів) часто можуть бути менше самих мініатюрних фотокамер. Тим часом, застосування відеотехніки в комерційній розвідці часто дає переваги, недосяжні для фото і кінотехніки. Насамперед це те. що за допомогою відеотехніки легко здійснити запис, передачу на великі відстані й оперативний аналіз зорової і звукової інформації в реальному масштабі часу. У спрощеному вигляді система відео спостереження складається з відеокамери. відеомагнітофона та (чи) передавача.

4.5.2. Мікро відеокамери

Відеокамери з прийнятними характеристиками, пропоновані до реалізації для цілей комерційної розвідки мають, в основному, імпортне походження. Вітчизняні камери за габаритними характеристиками придатні поки тільки для систем відео контролю (службові приміщення, відео домофони, магазини і т. ін.). Зупинимося більш докладно на характеристиках деяких конкретних моделей камер закордонного виробництва. Найбільший інтерес у даному випадку представляє опис без корпусних відеокамер. Об'єктив і електронна схема керування розміщаються на одній платі розміром 4.2х4.2 см. Стандартний об'єктив має

фокусну відстань 3,6 мм. З цим об'єктивом камера має габарити 4.2х4.2х2.1 см і кут огляду 92°±. З крапковим об'єктивом габарити складають 4.2х4.2х1.2 см. кут огляду - 88°±. Незалежно від типу об'єктива, камера має наступні характеристики: мінімальна освітленість - 0.4 лк. кількість ліній 380 . живлення - 12 В. вага - 12 г. Стандартний об'єктив має фокусну відстань 5.6 мм, кут обзору 56°±, дозвіл: PAL -512(Н)х582(У). Камера може працювати при освітленості до 2.5 лк. Габарити 4.2х8.4х3.0 см зі стандартним і 4,2х8,4х1.2 см із крапковим об'єктивами. Вага - ЗО г. Ці та їм подібні камери можуть монтуватися як разом з об'єктивом, так і з винесеним об'єктивом. Маскування може бути будь-яким: у розетках електроживлення, радіоприймачах, настінному і настільному годинник, одязі, окулярах, датчиках пожежної сигналізації, приладах освітлення і І. ін. Відеокамери можуть забезпечуватися різними змінними об'єктивами. Потрібно мати на увазі, що деякі матеріали, застосовувані для маскування об'єктів (типу "чорне скло"), пропускають тільки невелику частину спектра н можуть успішно працювати при сонячному освітленні, при освітленні ІЧ прожектором чи звичайними лампами накалювання. але їхнє застосування неможливе при освітленні об'єкта люмінесцентними чи галогенові лампами. Становить інтерес опис відеокамери з передавачем. Наприклад, це може бути OVS-25-5. Розрізнювальна спроможність цієї камери - 380 ліній. Чутливість - 0.5 лк. об'єктив з фокусною відстанню 1,6 мм і автоматичним регулюванням діафрагми. Вбудований передавач працює в діапазоні 400-500 МГц і має потужність 40 мВт. Живлення зовнішнє 12 В. споживаний струм - 120 ма. Габарити -3,8х4,5х5,9 см. вага - 20 г.

4.5.3. Пристрої дистанційного керування, відео детектор руху

Пристрій керування служить для наведення камери на заданий об'єкт, вмикання-вимикання передавача, відеомагнітофона. інфрачервоного освітлювача. У найпростішому випадку цей пристрій задає швидкість і кут сканування. Наприклад, поворотний пристрій OVS-32. керування яким здійснюється за допомогою виносного пульта. Спеціальний поворотний пристрій для відеокамер має наступні можливості:

- кут повороту автоматичного сканування складає ± 180 задається за допомогою пульта керування.
- плавну та безшумну роботу поворотного механізму.
- можливість кріплення на стіні за допомогою спеціального кронштейна.
- максимальне навантаження - 7 кг.
- габаритні розміри - 146х124 мм. вага - 1,4 кг.

Для мініатюрних камер можна застосувати, наприклад, пристрій PTI-II. що має габарити 6.5хз.З см. Мініатюрний прилад наведення застосовується в приміщенні. Максимальне навантаження - не більш 0.4 кг. Призначений для використання з камерами

типу Watec, має циліндричний корпус, кут горизонтального обертання - 350±. швидкість обертання регулюється. Кут нахилу - 180°±. швидкість також регулюється. Напруга живлення - 12 В постійного струму (60 мА). Більш складні пристрої дистанційного керування мають функції дистанційного увімкнення (наприклад, через нормально-розімкнуте реле). Включення може здійснюватися за допомогою таймера, вимикача беспроводного активатора (наприклад, з використанням радіоканалу), дверних контактів, а також детектора руху. Як приклад такого керуючого пристрою можна привести виріб N 92444 виробництва США. Процесор даною пристрою програмується в режимі таймера, ручного керування чи у черговому режимі. Має генератор часу і дати для фіксації моменту здійснення запису події, а також дозволяє запрограмувати титри з двох рядків по 20 знаків. Габарити 14х18х4 см. Відео детектор руху служить для активізації апаратури при зміні положення на об'єкті, що спостерігається. Як приклад такого пристрою опишемо модель N 94501. Цей детектор має регульовану чутливість, виключає помилкові спрацьовування при зміні освітленості, можливе автоматичне настроювання. Розмір зображення регулюється від 5 до 90% від об'єкта спостереження, мається вихід для подачі сигналу тривоги.

4.5.4. Інфрачервоні освітлювачі

Застосування . інфрачервоних освітлювачів (ІЧ-освітлювачів) буває необхідно при роботі в умовах недостатньої видимості, а також у тому випадку, якщо для маскування об'єктива відеокамери застосовані непрозорі у видимому діапазоні матеріали. Інфрачервоні освітлювачі можуть випускатися або окремо, або сполученими з відеокамерами. Як приклад сполученого з камерою ІЧ освітлювача можна привести виріб фірми SANYO - VDC-9212. Ця чорно-біла відеокамера може працювати в повній темряві. Розрізнювальна здатність – 400 ліній, габарити - 10х5 см. Окремо виконаний ІЧ освітлювач N 91101 використовує випромінюючий елемент на основі галієво-алюмінієвого арсеніду (GaALAs) зі спектром випромінювання в районі 880 нм, поміщений в алюмінієвий корпус. Споживаний струм - 600 мА. Габарити - 10х5х4.5см.

4.5.5. Мініатюрні відеомагнітофони

Найпоширенішим режимом відео спостереження є режим з одночасним записом на відеомагнітофон. Найбільш широко для цих цілей застосовуються відеомагнітофони, розраховані на роботу з 8 мм відеокасетою. Відеомагнітофони мають, як правило, функцію дистанційного керування, звук записується в режимі стерео. Деякі моделі обладнані відео монітором. Приведемо характеристики деяких моделей таких відеомагнітофонів. OVS-9 має дві швидкостей запису, час запису - до 5 годин, живлення здійснюється від вбудованого акумулятора чи зовнішнього джерела живлення напругою 7,5 В. Споживана потужність - 4 Вт, габарити - 148х130х62 мм, вага - 670г Модель OVS-9-1 являє собою відеомагнітофон

OVS-9 із вбудованим кольоровим плоским монітором. Монітор зручний при монтажі і настроюванні прихованих відеокамер. а також для контролю діючих відео систем і перегляду знятого відео матеріалу. Габарити -1 50х 1 35х70 мм, вага - 700 г.

4.5.6. Безпроводні лінії передачі і прийому відеоінформації

Робоча частота комплекту WVL-9() складає від 904 до 928 МГц. Лінія здатна передавати кольорове чи чорно-біле зображення на відстань від 300 до 900 м, у залежності від типу використовуваної антени (вбудована плоска антена чи зовнішня антена високого посилення типу WVLA-902), відношення сигнал/шум не менше 45 дБ. Живлення від зовнішньою джерела живлення - 10-25 В. споживаний струм передавача - не менше 50 мА, приймача – не менше 20 мА. Габарити передавача - 23х6.3х9.5 см., приймача -23х70х12 см. Комутатор застосовується у випадку роботи одночасно з декількома відеосигналами. Він передає сигнал одночасно на відеомагнітофон і (чи) монітор. Наприклад, комутатор моделі OVS-31 дозволяє виводити на монітор сигнали від 4 до 12 відеокамер. Час показу сигналу регульоване - від 1 до 20 с. Можливе виключення будь-якої камери з режиму перегляду. Живлення від мережі, габарити - 6,0х26.5х24.0 см. - вага 3,3 кг. Характеристики одного з моніторів, використовуваного в подібних лініях. розглянемо на прикладі виробу OVS-27. Розрізнювальна здатність – 850 ліній, екран з діагоналлю 25 см, вбудований динамік, частота горизонтальної розгортки - 15625 Гц (15.750 Гц), частота вертикальної. розгортки 50 Гц (60 Гц), електроживлення від мережі, споживана потужність - 30 Вт. габарити - 235х220х250 мм, вага - 6,2 кг.

Питання для самоперевірки:

1. Назвіть основні групи пристроїв та систем технічної розвідки.
2. Яке призначення радіомікрофона?
3. Назвіть основні технічні характеристики радіомікрофонів.
4. Яким може бути конструктивне виконання радіомікрофонів?
5. Охарактеризуйте пристрої прийому інформації, одержаної за допомогою радіомікрофона.
6. Назвіть основні методи прослуховування телефонних ліній.
7. Які способи підключення до телефонних ліній ви знаєте?
8. Для чого використовуються телефонні радіоретранслятори?
9. Як можна використати телефонну лінію для прослуховування принципів?
10. Назвіть які існують спеціальні пристрої прослуховування?

Розділ 5. Методи захисту інформації в системах зв'язку та передавання даних.

5.1. Класифікація засобів технічного захисту інформації в каналах загального користування.

Враховуючи те, що системи авіаційного зв'язку працюють, як правило, на каналах загального користування (ТФЗК) будемо проводити класифікацію засобів технічного захисту інформації (ЗТЗІ) для каналів ТФЗК.

Задача класифікації ЗТЗІ в загальному вигляді може бути представлена таким чином. Нехай є повна множина апаратури ЗТЗІ, яка має призначення для роботи в каналах ТФЗК:

$$\{a_i\} \in A; i = \overline{1,n}, \qquad (5.1)$$

де a_i - елемент (зразок апаратури ЗТЗІ), який належить повній множині A; n – число елементів в множині A.

Згрупуємо елементи a_i множини A у підмножини A_j за заданими критеріями класифікації, тоді отримаємо:

$$\{A_j\} \in A; i = \overline{1,k}, \qquad (5.2)$$

де k - кількість підмножин A_j множини.

У результаті об′єднання підмножини A_j утворена така множина, елементами

$$B = \bigcup_{j=1}^{k} A_j \qquad (5.3)$$

якої є всі елементи множини.

При цьому співвідношення кількості елементів множин до кількості елементів множини визначається нерівністю

$$N(B) \geq N(A) \qquad (5.4)$$

де $N(A)$ - кількість елементів множини,

$$N(B) = \sum_{j=1}^{k} N(A_j), \qquad (5.5)$$

де $N(B)$ - кількість елементів множини B.

Для цього випадку завдання класифікації зводиться до вибору критерію для формування підмножини A_j з елементів множини A таким чином, щоб мінімізувати коефіцієнт вкладення множин:

$$K_в = \left(1 - \frac{F - D}{F}\right), \qquad (5.6)$$

де $F = \sum_{j=1}^{k} N(A_j)$;

$$D = \sum_{i=1}^{C_k} N\left(n^2 A_{(2)i}\right) - \sum_{i=1}^{C_k} N\left(n^3 A_{(3)i}\right); \quad (5.7)$$

$$C_n^l = \frac{n(n-1).....(n-l)}{l!}; \quad (5.8)$$

$$N_p^l = N^{(l)} A_{(p)l}, \quad (5.9)$$

де N_p - кількість елементів, які належать ділянці перетинання множин; l – кількість множин, які перетинаються одночасно (кратність перетинань); $A_{(p)l}$ - ділянка, яка утворена перетинанням l множин.

Формула (10.27) дає можливість оцінити якість класифікатора, тобто формування підмножин A_j.

За заданих обмежень (умов) для формування класифікатора (підмножин A_j) найкращим буде класифікатор, для якого $K_в = 0$. Це означає, множина (10.24) містить підмножини A_j (10.23), які не перетинаються. За умов, що всі елементи множини А належать множині, тобто

$$A \subseteq B \quad (5.10)$$

B вкладена та дорівнює множині A.

На практиці добрим результатом класифікації можна вважати результат, для якого $K_в \le 0{,}1$.

Взагалі завдання формування підмножин A_j не має суворо визначеного рішення. Це пояснюється багатьма причинами, серед яких визначальним є неоднозначність у виборі формулювання критеріїв класифікації ЗТЗІ. Тому завдання формування класів ЗТЗІ значною мірою має суб'єктивний характер. З метою зменшення суб'єктивізму на усунення неоднозначності у формуванні класів ЗТЗІ скористаємось таким підходом. Розіб'ємо завдання класифікації ЗТЗІ на два етапи (аналізу і синтезу).

На першому етапі (аналізу) безвідносно конкретних типів апаратури ЗТЗІ створимо множини класів, які не перетинаються та сформованим за способами технічного захисту інформації в СПД і за видами технічних каналів витоку, з якими взаємодіють ЗТЗІ (тобто за двома класоутворюючими параметрами).

Таким чином, утворюється теоретично можлива та повна множина класів ЗТЗІ, сформована за типами захисту та видам технічних каналів витоку.

На другому етапі (синтезу) проводиться формування класів ЗТЗІ з урахування специфіки діючої апаратури захисту та тієї, що розробляється.

Формування класів ЗТЗІ виконується шляхом синтезу класів із теоретично повного їх набору, які представлені в 16.3. Критеріями для синтезу класів технічних засобів захисту служить взаємодія ЗТЗІ з середовищем поширення та обробки сигналів, за допомогою яких передається інформація, а також взаємодія ЗТЗІ з середовищем розповсюдження та обробки сигналів, за допомогою яких передається інформація, а також взаємодія ЗТЗІ з побічними електромагнітними випромінюваннями та наводками (ПЕМВН), які породжуються середовищем.

У якості критеріїв, які утворюють класи виберемо способи протидії ЗТЗІ технічним каналам витоку інформації. Всі технічні канали витоку інформації можна розділити на дві групи. Перша група – це канали ПЕМВН, які утворені середовищем поширення та обробки сигналів (класи 1,2,3 з розділу 10.3). Друга група – це канали, які утворені за допомогою атакуючої апаратури (прямі канали витоку інформації (класи 5-9)). У свою чергу канали витоку другої групи, утворені за допомогою атакуючої апаратури, можуть бути двох видів – канали, утворені безпосередньо атакуючою апаратурою, та канали витоку, які утворені атакуючою в іншому середовищі поширення сигналів (вторинні канали витоку). До вторинних каналів, які утворюються атакуючою апаратурою відносяться радіочастотний канал, акустичний (ультразвуковий) канал та інфрачервоний канал (ІЧ - канал).

Критерієм класифікації є спосіб захисту інформації, який реалізовано в ЗТЗІ.

Так за способом захисту ЗТЗІ поділяються на засоби виявлення, перешкоджання (ослаблення), маскування (приховування) та знищення.

Слід зазначити, що застосування засобів знищення закладних пристроїв (атакуючої апаратури) в СПД недоцільно через низьку ефективність, а в деяких випадках їх застосування неприпустимо. Це пояснюється такими причинами. Перша – знищенню піддається обмежена кількість типів закладних пристроїв та знищуються тільки ті пристрої, які підключені паралельно лінії зв’язку. Пристрої, які підключені послідовно лінії або за допомогою датчиків (електромагнітних або ємнісних) знищити існуючими ЗТЗІ важко.

Друга причина – під час знищення закладних пристроїв існує велика вірогідність виходу з ладу дорогої апаратури, яка утворює канали .

Третя причина – знищення закладних пристроїв проводиться шляхом подачі імпульсів високої напруги протягом 2-10 хв. При цьому знищуються пристрої , які підключені паралельно лінії та розташовані на відстані не більше 10-20 м. В цих умовах (за термін 2-10 хв) можна відключити та вилучити закладний пристрій, який було виявлено.

Далі виконаємо синтез ЗТЗІ шляхом об’єднання всього теоретично повного набору класів з урахуванням специфіки використання технічних характеристик існуючої та

розроблюваної апаратури захисту інформації в СПД. Критерієм синтезу класів був характер та ступінь взаємодії ЗТЗІ із середовищем поширення та обробки сигналів, що відтворюють дані в СПД. Окремим класом ЗТЗІ (клас 12) виділені технічні засоби канального шифрування СПД.

За характером взаємодії з середовищем поширення та обробки сигналів апаратура розподіляється на дві групи. Перша – така, яка взаємодіє безпосередньо з середовищем (прямі канали витоки).

Друга група – це апаратура, яка взаємодіє з ПЕМВН, що створюється середовищем поширення та обробки сигналів (опосередковані канали витоку).

Перша група апаратури утворює класи ЗТЗІ від п'ятого до десятого та призначена робити протидію атакуючій апаратурі. За ступенем взаємодії з середовищем ЗТЗІ першої групи можуть бути двох видів. Перший вид – це апаратура, яка призначена для послаблення (заважаючим) діям атакуючої апаратури (пасивні ЗТЗІ). Другий вид - це активні ЗТЗІ, тобто апаратура, яка в результаті вимірювань виявляє атакуючу апаратуру та або генерує сигнал, який маскує середовище поширення та обробки сигналів. В свою чергу активні засоби захисту діляться на ЗТЗІ, які протидіють атакуючій апаратурі, яка утворила канал витоку в іншому фізичному середовищі (вторинні канали витоку) та на ЗТЗІ, які протидіють апаратурі, яка не утворює такі канали. Вторинні канали, які створюються атакуючою апаратурою як правило перебувають в радіочастотному. інфрачервоному та ультразвуковому діапазоні.

ЗТЗІ другої групи (від ПЕМВН) також, які як і ЗТЗІ від атакуючої апаратури за ступенем взаємодії поділяються на два види. При цьому створюються класи ЗТЗІ від другого до п'ятого.

Окремий клас (клас 11) виділено ЗТЗІ, які здійснюють моніторинг ліній зв'язку та тестування інженерних комунікацій (джерел живлення, систем сигналізації, електрифікації, ліній місцевого зв'язку, пожежоохоронної сигналізації та інше) з метою виявлення каналів витоку інформації в цих системах.

Засоби моніторингу це, як правило, складні програмно-апаратні комплекси, створені на базі комп'ютерів. Ці комплекси мають призначення для моніторинга багатоканальних телекомунікаційних систем, на них також покладаються функції захисту інформації в телекомунікаційних системах (виявлення несанкціонованого підключення до ліній зв'язку, виявлення випромінювань атакуючої апаратури в широкому діапазоні радіочастот, акустичному та ІЧ діапазоні, нелінійні локатори ліній зв'язку, генератори сигналів схожих на шум та у широкому діапазоні радіочастот та ін.).

Засоби тестування комунікацій призначені для виявлення та нейтралізації атакуючої апаратури в системах інженерних комунікацій, які проходять через приміщення, де

розташовані СПД. Таким чином, в результаті досліджень було розроблено класифікатор засобів технічного захисту інформації в СПД, якій представлено в таблиці 10.11.

Таблиця 5.1

Класифікатор ЗТЗІ в СПД

Код класу ЗТЗІ	Найменування класу ЗТЗІ	Вид каналу витоку, що закривається
01	Засоби виявлення ПЕМВН	ПЕМВН (побічні електромагнітні випромінювання та наводки), які утворюються СП
02	Засоби ослаблення або придушення ПЕМВН	
03	Засоби маскування інформації для протидії ПЕМВН	
04	Засоби виявлення побічних електромагнітних або магнітних полів, які утворюються пристроями запису інформації на фізичні носії	Несанкціоноване копіювання інформації
05	Засоби зменшення ефективності або знешкодження пристроїв запису інформації на фізичні носії	
06	Засоби виявлення або визначення місця знаходження атакуючої апаратури, яка підключена до лінії зв’язку	Несанкціоноване знімання інформації
07	Засоби зменшення ефективності або знешкодження атакуючої апаратури шляхом включення в лінію зв′язку нелінійних елементів або загороджувальних фільтрів	
08	Засоби виявлення ультразвукового випромінювання (поля)	Несанкціонований ультразвуковий канал передавання інформації, який створюється атакуючою апаратурою
09	Засоби виявлення інфрачервоного випромінювання (поля)	Несанкціонований інфрачервоний канал передавання інформації, який створюється атакуючою апаратурою

Продовження табл. 5.1

Код класу ЗТЗІ	Найменування класу ЗТЗІ	Вид каналу витоку, що закривається
10	Засоби виявлення радіочастотного випромінювання (поля)	Несанкціонований радіочастотний канал передавання інформації, який створюється атакуючою апаратурою
11	Технічні засоби моніторингу ліній та каналів	Технічні канали витоку

12	передавання інформації Технічні засоби канального шифрування	інформації в СПД

Велике значення у виборі засобів технічного захисту інформації мають технічні параметри, які характеризують ці засоби та їх можливість виконувати свої функції. Нижче наведені таблиці з основними вимогами до переліку визначальних технічних параметрів для кожного класу, ЗТЗІ в СПД.

Код класу ЗТЗІ 01. Засоби виявлення ПЕМВН Таблиця 5.1

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Детектори (індикатори) електромагнітного поля з широкою смугою	Ширина смуги (діапазону) виявлення Δf (кГц, МГц, ГГц) Нерівномірність амплітудно-частотної характеристики (АЧХ) в смузі вимірювання N, (дБ) при $U_{вх} = const$ де U_{max} - максимальне значення напруги на виході індикатора в смузі виявлення Δf ; U_{min} - відповідно мінімальне значення; $U_{вх}$ - напруга на вході індикатора. Поріг чутливості, якій визначається як мінімальний рівень сигналу, що виявляється (поріг спрацювання індикатора) U_{min} (мкВ, мВ).
Детектори (індикатори) електромагнітного поля з вузькою смугою	Ширина смуги (діапазону) частот виявлення Δf (кГц, МГц, ГГц) Середня робоча частота $f_{ср}$, (кГц, МГц, ГГц) де $f_{ср} = \frac{f_{min} + f_{max}}{2}$ Нерівномірність амплітудно-частотної характеристики (АЧХ) в смузі виявлення вимірювання N (дБ), $N = 20 \lg \frac{U_{max}}{U_{min}}$ при $U_{вх} = const$ Поріг чутливості U_{min} (мкВ) в смузі Δf

Таблиця 5.3

Код класу ЗТЗІ-02. Засоби ослаблення або придушення ПЕМВН

Тип пристрою	Визначальні технічні параметри, одиниці виміру

Екрани захисні	Діапазон допущення частот Δf (кГц, МГц, ГГц) $\Delta f = f_{max} - f_{min}$, де f_{max} - максимальне значення діапазону придушення; f_{min} - мінімальне значення діапазону придушення. Коефіцієнти згасання K (дБ), який визначається на частотах f_{min}, $f_{ср}$, f_{max} за формулою $K = 20 \lg \frac{U_1}{U_2}$, де U_1 (мкВ, мВ) значення напруги внутрішньої сторони екрану; U_2 (мкВ, мВ) значення величини напруги зовнішньої сторони екрану $f_{ср} = \frac{f_{max} - f_{min}}{2}$

Таблиця 5.4

Код класу ЗТЗІ -03. Засоби маскування інформації для протидії ПЕМВН

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Генератори білого шуму	Робочий діапазон або робочі діапазони сигналів, що генеруються Δf (кГц, МГц), який визначається як $\Delta f = f_{max} - f_{min}$, де f_{max} - максимальне значення частоти генерації в робочому діапазоні; f_{min} - мінімальне значення частоти генерації в робочому діапазоні. Спектральна щільність потужності білого шуму в робочому діапазоні ν_0^2 (мВт/кГц, мВт/МГц). Тип антени (антен) Вид поляризації сигналів, що генеруються
Генератори із скануванням	Робочий діапазон або робочі діапазони сигналів, що генеруються Δf (кГц, МГц). Середній рівень потужності сигналів, що генеруються, $P_{ср}$ (мВт) в робочому діапазоні Ширина діапазону перестройки ΔF (МГц), $\Delta F = F_{max} - F_{min}$, де ΔF_{max} та ΔF_{min} - відповідно максимальна та мінімальна частота перестройки Швидкість перестройки (девіації) частоти генерації сигналів (кГц/с) Вид модуляції сигналів, що генеруються Рівень модуляції АМ - сигналів (%) Величина девіації частоти ЧМ - сигналів

Таблиця 5.5

Код класу ЗТЗІ -04. Засоби виявлення побічних електромагнітних або магнітних полів, які створюються пристроями запису інформації на фізичні носії

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Виявлювані апаратури магнітного запису за допомогою індикації поля систем підмагнічування	Ширина смуги (діапазон частот) виявлення Δf (кГц), $\Delta f = f_{\max} - f_{\min}$, де $f_{\max}$, $f_{\min}$ - відповідно максимальна, мінімальна частота виявлення Поріг чутливості, який визначається як мінімальний рівень сигналу, що визначається (спрацювання індикатора) $U_{\min}$ (мкВ, мВ) у смузі Δf
Виявники магнітного поля двигунів	Поріг чутливості, який визначається як мінімальний рівень величини магнітної індукції на вході датчика, при якому спрацьовує індикатор $B_{\min}$ (мкТл) Кількість датчиків

Таблиця 5.6

Код класу ЗТЗІ -05. Засоби зменшення ефективності або знешкодження пристроїв запису інформації на фізичні носії

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Генератори спеціалізовані	Середня частота генерації $f_{\text{ср}}$ (кГц) Середня потужність сигналів, що передаються $P_{\text{ср}}$ (мВт, Вт) Вид модуляції сигналів, що генеруються (для випадку модуляції сигналів) Тип випромінювача антени (антен). Рівень модуляції АМ – сигналів (%) Величина девіації частоти ЧМ – сигналів (кГц)

Таблиця 5.7

Код класу ЗТЗІ -06. Засоби виявлення та визначення місця знаходження атакуючої апаратури, яка підключена до лінії зв’язку

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Прилади виявлення паралельно підключених закладних пристроїв	Максимальне значення вхідного опору закладного пристрою, на яке реагує прилад $R_{\max}$ (кОм, МОм) Діапазон величин напруги, що вимірюється в лінії зв′язку (В) Діапазон величин струму, що вимірюється в лінії зв′язку (мкА, мА)
Прилади виявлення послідовно підключених закладних пристроїв	Мінімальне значення вхідного опору закладного пристрою, на яке реагує прилад $R_{\min}$ (Ом) Діапазон величин напруги, що вимірюється в лінії зв’язку (В) Діапазон величин струму, що вимірюється в лінії зв’язку (мкА, мА)
Нелінійні локатори	Мінімальна відстань до закладного пристрою, що виявляється (м, см) Максимальна відстань до закладного пристрою, що виявляється (м)

	Частота локації (МГц) Похибка вимірювань коефіцієнту нелінійних спотворень Δ (%) $\Delta = \frac{\left\|K_{\text{н.вм}} - K_{\text{н.д}}\right\|}{K_{\text{н.д}}} \cdot 100\%$, де $K_{\text{н.д}}$ - дійсне значення коефіцієнта, $K_{\text{н.д}} = \frac{\sqrt{U_2^2 + U_3^2 + ...U_n^2}}{U_1} \cdot 100\%$, де U_1 - напруга першої гармоніки сигналу; $U_2, U_3 ..... U_n$ - напруга другої, третьої, n -ї гармонік сигналу; $K_{\text{н.вм}}$ - виміряне значення $K_{\text{н}}$

Таблиця 5.8

Код класу ЗГ39 – 07. Засоби зменшення ефективності або знешкоджування атакуючої апаратури за допомогою включення в лінію зв'язку нелінійних елементів та або загороджувальних фільтрів

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Нелінійні загороджувальні пристрої	Величина коефіцієнту передавання при високому рівні сигналу на вході пристрою $К_{вис}$ (дБ) на частоті сигналу 1800 Гц, який визначається як $К_{вис} = 20$ $K_{\text{вис}} = 20 \lg \frac{U'_{\text{вх}}}{U_{\text{вих}}}$, де $U'_{\text{вх}}$ - значення напруги сигналу на вході пристрою при високому рівні сигналу, $U_{вих}$ – значення напруги сигналу на виході пристрою Величина коефіцієнту передавання при низькому рівні сигналу на вході пристрою $К_{низ}$ на частоті 1800 Гц $K_{\text{низ}} = 20 \lg \frac{U''_{\text{вх}}}{U_{\text{вих}}}$, де $U''_{\text{вх}}$ - значення пристрою при низькому рівні сигналу Величина коефіцієнту нелінійних спотворень $К_н$ на частоті сигналу 1800 Гц $K_{\text{низ}} = \frac{\sqrt{U_2^2 + U_3^2 + ...U_n^2}}{U_1} 100\%$, де U_1 – напруга першої гармоніки сигналу; $U_2, U_3 ..... U_n$, - напруги другої, третьої, та n – ї гармонік сигналу
Загороджувальні електричні фільтри ВЧ сигналів	Величина коефіцієнту значення в смузі пропускання частот каналу тотальної частоти (300 – 3400) Гц; $К'_В$ (дБ); $K'_{\text{В}} = 20 \lg \frac{U_{\text{вх}}}{U_{\text{вих}}}$, при $U_{\text{вх}} = const;$ де $U_{\text{вх}}$ – значення напруги на вході фільтра (мкВ, мВ) $U_{\text{вих}}$ – значення напруги на виході фільтра (мкВ, мВ) Нерівномірність амплітуд АЧХ у смузі пропускання частот каналу тотальної частоти N (дБ)

	$N = 20 \lg \frac{U_{max}}{U_{min}}$, при $U_{вх} = const$, де U_{max} – максимальне значення напруги на виході фільтра в смузі частот 300 – 3400 Гц; U_{min} – мінімальне значення напруги на виході фільтра в смузі частот 300 – 3400 Гц Мінімальне та максимальне значення частот у смузі придушення фільтра f_{max}, f_{min} (кГц) Величина коефіцієнту загасання в смузі придушення частот фільтра $К''_В(дБ)$; $K''_В = 20 \lg \frac{U_{вх}}{U_{вих}}$, при $U_{вх} = const$; Нерівномірність АЧХ в смузі придушення частот фільтра (дБ), або значення коефіцієнту загасання на двох або трьох фіксованих частотах в смузі придушення фільтра

Таблиця 5.9

Код класу ЗТЗІ – 08. Засоби виявлення ультразвукового випромінювання

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Мікрофони з вузькою діаграмою спрямованості	Тілесний кут спрямованості мікрофона (стер) Діапазон частот виявлення f_{max}, f_{min} (кГц) Мінімальний звуковий тиск, на який реагує прилад, в діапазоні частот виявлення P_{min} (Па)
Датчики магнітострикційні	Діапазон частот виявлення f_{max}, f_{min} (кГц) Мінімальний звуковий тиск, на який реагує датчик, в діапазоні частот виявлення P_{min} (Па)

Таблиця 5.10

Код класу ЗТЗІ – 09. Засоби виявлення інфрачервоного каналу випромінювання поля

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Індикатор І4 – випромінювання	Величина мінімального освітлення, на яке реагує індикатор ($Л_к$).

Таблиця 5.11

Код класу ЗТЗІ – 10. Засоби виявлення радіочастотного каналу передавання інформації

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Приймачі панорамні (частотоміри)	Діапазон перестройки частот (кГц, МГц, ГГц), $\Delta f = f_{max} - f_{min}$ де f_{max} – максимальне значення електромагнітного випромінювання; f_{min} – мінімальне значення електромагнітного випромінювання Кількість діапазонів частот, що перестроюються (n) Термін перестройки в кожному з діапазонів τ (с.) Поріг чутливості в межах частотних діапазонів U_{min} (мкВ)
Аналізатори спектру	Діапазон частот електромагнітного випромінювання, що

	виявляється (кГц, МГц, ГГц) Кількість діапазонів частот, що перестроюються (n) Порогова чутливість в межах частотних діапазонів $U_{\min}$ (мкВ) Розрізнювальна спрямованість в межах частотних діапазонів (мВ/діл)

Таблиця 5.12

Код класу ЗТЗІ – 11. Технічні засоби моніторингу ліній та каналів передавання інформації.

Тип пристрою	Визначальні технічні параметри, одиниці виміру
Аналізатори стану ліній зв'язку	Кількість ліній зв'язку, що аналізується (n) Швидкість сканування ліній зв'язку (лін/с) Діапазон частот, що аналізуються Δf (кГц, МГц, ГГц), $\Delta f = f_{\max} - f_{\min}$ де $f_{\max}$ – максимальне значення частоти аналізу; $f_{\min}$ – мінімальне значення частоти аналізу Кількість частотних діапазонів K Діапазон вимірювань вхідного опору атакуючих пристроїв $R'_{\min}, R'_{\max}$ (Ом, кОм, МОм), де $R'_{\min}$ - мінімальне значення вхідного опору, $R'_{\max}$ - максимальне значення вхідного опору Поріг чутливості в межах частотних діапазонів $U_{\min}$ (мкВ, мВ) Розрізняючи спроможність в межах частотних діапазонів (мВ/діл) Види демодуляції Мінімальна відстань виявлення несанкціонованого підключення $\tau_{\min}(M)$ Максимальна відстань виявлення несанкціонованого підключення $\tau_{\min}(M)$ Точність виявлення підключень до ліній зв'язку (см, М)
Аналізатори систем комунікацій	Типи (за призначенням) ліній, що аналізуються Діапазони частот, що аналізуються Δf (кГц, МГц, ГГц) Кількість частотних діапазонів (n) Поріг чутливості в межах частотних діапазонів $U_{\min}$ (мкВ,мВ) Розрізняючи спроможність в межах частотних діапазонів (мВ/діл)

Таблиця 5.13

Код класів ЗТЗІ – 12. Технічні засоби канального шифрування.

Тип пристрою	Визначальні технічні параметри, одиниці виміру

Засоби канального шифрування	Швидкість шифрування (кБіт/с) Алгоритми шифрування. Режим роботи Тип інтерфейсу Протокол обміну ключовою інформацією Спосіб введення ключів Реалізація функцій зворотного виклику, електронного підпису та інше

5.2 Пристрої захисту інформації в телекомунікаційних системах

5.2.1 Загальні принципи захисту інформації в приміщеннях та мережах зв’язку.

З точки зору безпеки, телефонний зв'язок має такий недолік, який дозволяє перехоплювати мовну інформацію як під час телефонного зв’язку, так і після «відбою». Щоправда, цей недолік мають і будь-які інші провідні лінії.

Отже, в будь якій великій організації треба створити свої служби безпеки, на які покласти в першу чергу проблему захисту телефонних мереж. Цим службам перш за все треба проаналізувати апаратуру захисту, яка серійно випускається. Її можна умовно розділити на дві підгрупи: апаратуру контролю та апаратуру захисту ліній зв‘язку.

До апаратури контролю ліній зв‘язку відносяться:

- аналізатори та індикаторні пристрої;
- кабельні локатори (рефлектометри та прилади, які використовують принципи нелінійної локації);
- детектори поля, частотоміри, спеціальні радіоприймальні пристрої та універсальні комплекси контролю.

До апаратури захисту ліній зв‘язку відносяться:

- багатофункціональні пристрої захисту телефонних ліній;
- пристрої знищення закладок;
- апаратура крипто захисту;
- пристрої захисту від піратських підключень;
- апаратура лінійного та просторового шумо утворення;
- апаратура захисту від ВЧ - нав‘язування.

5.2.2. Пристрої захисту телефонних апаратів.

При організації захисту телефонних ліній необхідно враховувати наступні фактори:

- телефонні апарати можуть використовуватись для підслуховування переговорів, що ведуться в приміщенні, де вони встановлені;
- прослуховування телефонних розмов можливе через безпосереднє підключення до

телефонного апарату, шляхом прийому та обробки випромінювання електромагнітних хвиль телефонним апаратом у простір, в телефонну або енергетичну лінію;

– використання мікрофонного ефекту та ефекту високочастотного нав’язування для зняття інформаційного сигналу з телефонного апарату при покладеній трубці.

Крім цього, телефонні лінії, що проходять в приміщенні можуть використовуватись в якості:

– лінії для передачі отриманої інформації;
– джерела живлення для пристроїв зняття інформації;
– дистанційного керування пристроями зняття інформації.

Як наслідок методи та пристрої захисту телефонних апаратів телефонних ліній повинні бути направлені на виключення:

– використання телефонних апаратів та ліній для прослуховування переговорів, що ведуться у приміщенні;
– безпосереднього прослуховування телефонних апаратів;
– несанкціонованого використання телефонної лінії.

Для захисту телефонного апарату від витоку мовної інформації використовуються пасивні та активні методи та пристрої.

До пасивних методів відносяться:

– амплітудне обмеження небезпечних сигналів;
– фільтрація небезпечних сигналів;
– відключення джерел небезпечних сигналів.

Амплітудне обмеження основане на використанні схем амплітудних обмежувачів на діодах.

Як відомо, вольт-амперна характеристика діодного обмежувача має вигляд

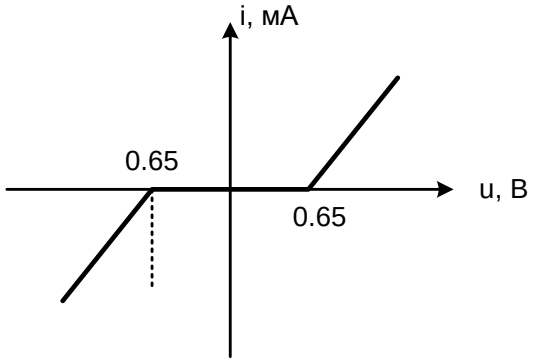


Рис. Вольт-амперна характеристика діодного обмежувача

При такій ВАХ слабкі небезпечні сигнали обмежуються і сильно ослабляються.

Як будь-який електронний пристрій, телефонний і факсимільний апарати, концентратор і з'єднуючі його лінії створюють у відкритому просторі досить високі рівні випромінювання в діапазоні частот аж до 150 МГц (табл. 5.14) [13].

Завдяки малим розмірам джерела випромінювання і, отже, незначній довжині його внутрішніх монтажних проводів, рівень випромінювання самого апарата швидко зменшується відповідно до віддалення від нього.

Крім того, несиметричний внутрішній опір телефонного апарата як джерела випромінювання щодо землі завжди значно більше аналогічного опору телефонної лінії. Унаслідок цієї напруги випромінювання в провідних лініях, обмірювані між ними і землею, звичайно бувають менше, ніж аналогічні напруги, вимірювані між лінійними проводами і корпусом телефонного апарата. Для того щоб цілком придушити усі види випромінювань, створювані телефонними апаратами, необхідно відфільтрувати випромінювання в лінійних проводах, що відходять від апаратів, і проводах мікротелефону, а також забезпечити достатній захист внутрішньої схеми телефонного апарата. Це можливо тільки при значній схемній переробці телефонних апаратів і зміні їхніх електричних параметрів. Зі сказаного випливає, що для того, щоб захистити телефонний апарат, необхідно захистити ланцюг мікрофона, ланцюг дзвоника, двох провідну лінію телефонного зв'язку [13].

Таблиця 5.14

Порівняльні рівні випромінювання

Діапазон частот, МГц	0,0001...0,55	0,55...2,5	2,5...150
Рівень поля на відстані 1 м, мкв	50...500	500...60	60...300

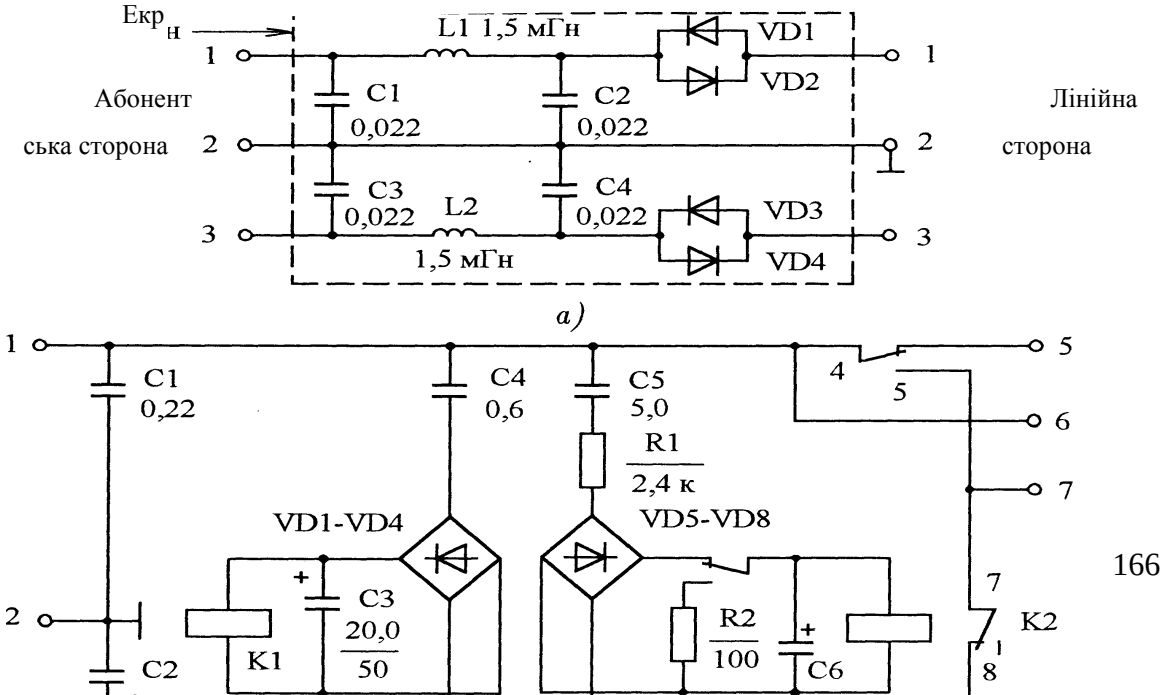


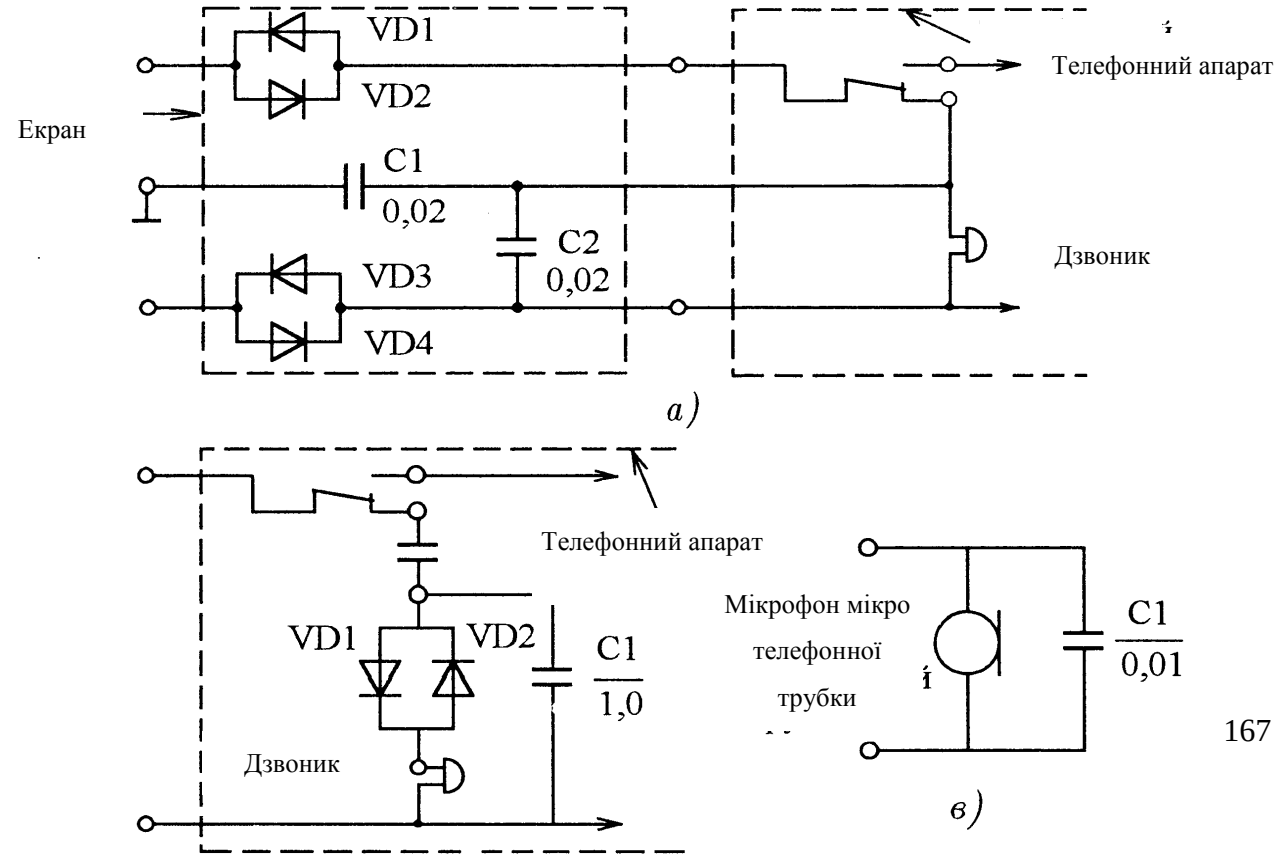
Рис. 5.1**.** Варіанти схемного захисту телефонної лінії (апарата): з допомогою *L, C* та діодів (VD1...VD4 — КД 102А); *б* — за допомогою *R, З,* діодів і реле (VD1...VD8 — КД 405Д; ДО1 — РЭС 15 РС4.591.001; ДО2 — РЭС 9 РС4.524.205 П2).

При створенні схеми захисту телефонного апарата необхідно знати умови роботи, тобто чи виходять лінії телефонного зв'язку за межі контрольованої зони, чи ні. Так, схема, наведена на рис. 5.1, а, дозволяє вносити згасання не менш 65 дБ при Uвх = 0,1 В у смузі частот 300...3400 Гц. Схема на рис. 5.1, б призначена для комплексного захисту телефонних апаратів. Ослаблення сигналу, наведеного на обмотці дзвоника, не менш 120 дб у смузі частот 300...3400 Гц.

На рис. 5.2 наведені конкретні схемні рішення для захисту елементів телефонного апарата від підслуховування при покладеній мікро телефонній трубці.

Для захисту концентраторів, авто набірних пристроїв, пультів зв'язку, факсимільних апаратів і т.д. необхідно використовувати схеми, наведені на рис. 5.1, а і 5.2, а.

Оцінити ефективність заходів захисту телефонних апаратів, концентраторів, авто набірних пристроїв, пультів зв'язку, гучномовців систем радіотрансляції й оповіщення, датчиків пожежної й охоронної сигналізації, кондиціонерів можна за допомогою апаратури

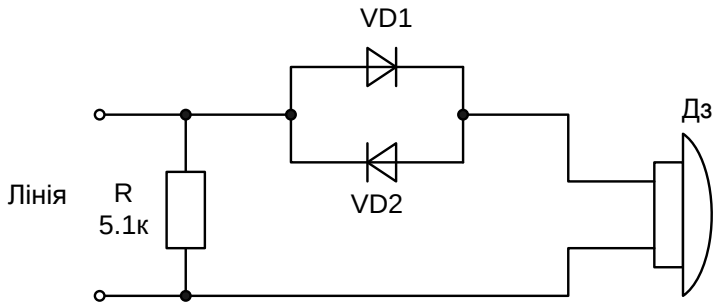


УИП-88 чи аналогічної.

б)

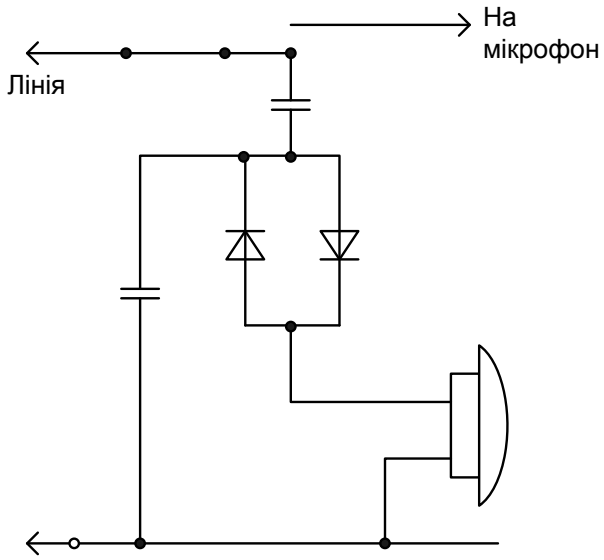
Рис. 5.2. Приклади захисту телефонних елементів: *а* — телефонної лінії (VD1...VD4 — КД 102А); *б* — ланцюга дзвоника (VDl, VD2 — КД 102А); *в* — у ланцюзі мікрофона.

Проста схема захисту дзвінкового кола для нейтралізації мікрофонного ефекту має вигляд (Рис.)



Для захисту від високочастотного нав'язування використовуються фільтри та амплітудні обмежувачі.

Найпростіша схема захисту мікрофона при покладеній телефонній трубці включає в себе конденсатор ємністю 0,01...0,05 мкФ(Рис.5.4в). Глибина паразитної модуляції при цьому зменшується в 10000 і більше разів, що робить неможливим обробку такого сигналу.



Прикладом є пристрій захисту ТА – «Бар'єр - М1», – який автоматично відключає ТА від лінії при покладеній трубці. При подачі в лінію сигналів виклику автоматично підключає ТА до лінії, але через фільтри блокування.

Найбільш ефективним способом захисту при проведенні конфіденційних переговорів є відключення телефонного апарата від лінії.

Активні методи захисту телефонних апаратів від витоку інформації включають в себе подачу в телефонну лінію при покладеній трубці низькочастотної шумової завади маскування (100 Гц... 10 кГц). Пристрої, що формують такі завади називають пристроями

лінійного шумо утворення. При піднятій трубці ТА подача завади в лінію припиняється. Прикладом реалізації такого пристрою є пристрій МП-1А (для аналогових ТА) та МП-1Ц (для цифрових ТА).

Телефонні фільтри звичайно вбудовуються в схему телефонного апарата чи у телефонну розетку і працюють за своїм призначенням (захист приміщення від витоку з нього звукової інформації) при покладеній мікротелефонній трубці (МТТ). Зовнішній вигляд їх представлений на рис. 5.3, а технічні характеристики пристроїв наведені в табл. 5.15.

Таблиця 5.15

Деякі характеристики пристроїв захисту телефонних апаратів

Модель	Призначення	Захист від мікрофонного ефекту	Захист від ВЧ нав'язування	Принцип роботи	Габаритні розміри, мм	Примітки
Корунд	Захист аналогових ТА	Є	немає	Обмеження сигналів	40х13х10	Сертифікат Гостехкомісії Росії
Грань-300	Захист аналогових ТА	Є	є	Фільтрація сигналів	90х55х25	Блокування ТА. Сертифікат Гостехкомісії Росії
МП-1А-Ц	Захист аналогових і чотирьох-провідних цифрових ТА	Є	є	Обмеження сигналів і зашумлення ліній	50х75х35	Сертифікат Гостехкомісії Росії
Гвард	Захист цифрових ТА	Є	немає	Придушення небажаних внутрішніх електромагнітних зв'язків	-	Вбудовується в корпус ТА
ПЗТ	Захист аналогових ТА	є	немає	Внесення додаткового загасання в розрив між ТА і лінією	-	Виконано в металевому корпусі
Граніт	Захист аналогових ТА	є	немає	Внесення додаткового загасання в розрив між ТА і лінією	95х60х25	Мінімальний час безвідмовної роботи не менш 5000 год

Прочерк означає відсутність даних.

Пристрій захисту телефонних апаратів (ПЗТ) має наступні характеристики:

– загасання, внесене в розмовний тракт на частоті 1 кГц при напрузі сигналу

- 10 В, не більше 2 дб;
- загасання, внесене в телефонну лінію на частоті 1 кГц при напрузі сигналу
- 50 мв, не менше 80 дб;
- акустична чутливість пристрою до акустичних полів не більше 0,1 мкв/Па;
- пристрій пасивний, живлення не вимагає.

Пристрій захисту телефонних апаратів «Корунд» призначено для захисту від витоку мовної інформації за рахунок мікрофонного ефекту.

Пристрій захисту телефонних розмов від прослуховування «Корунд-М» також призначено для захисту від прослуховування мови чи будь-яких інших звуків з використанням телефонного апарата, МТТ якого лежить на підоймовому перемикачі, тобто в режимі «Виклик». Пристрій легко встановлюється усередині розетки без обриву типу РТШ-4 і їй подібних [13].

Технічні характеристики: загасання на частоті 1 кГц при напрузі 10 В не більше 2 дБ, при напрузі 50 мв — не менше 80 дБ.

Пристрій захисту від несанкціонованого доступу «Гвард» призначено для захисту цифрових телефонних апаратів від витоку інформації через акустичні перетворювачі самого апарата. Всі акустичні перетворювачі, при встановленому в корпусі телефонного апарата пристрої захисту «Гвард», відключені від телефонного апарата (при цьому здійснюється придушення небажаних внутрішніх електромагнітних зв'язків у діапазоні мовних частот не менш ніж на 80 дБ).

Пристрій захисту «Грань-300» призначено для запобігання можливості прослуховування приміщення через телефонний апарат, що знаходиться в режимі «очікування виклику».

Цей пристрій блокує роботу телефонного апарата, що захищається, при паралельному підключенні іншого апарата чи при знятті мікротелефонної трубки на вже встановленому паралельному апараті.

Технічні характеристики:

- забезпечує загасання сигналів не менше 70 дБ у смузі 300...3400 Гц при покладеній на апарат мікротелефонній трубці, а загасання розмовного сигналу в тій же смузі частот на частоті 25 Гц не більше 2 дБ;
- споживаний струм від лінії АТС не більш 150 мкА;
- працює як з дисковими, так і з електронними номеронабирачами.

Пристрій захисту МП-1А-Ц призначено для захисту телефонних апаратів у цифрових мережах від витоку мовної інформації через апарат при покладеній трубці (для безупинної цілодобової роботи).

Технічні характеристики:

- смуга створюваного шумового сигналу — 0,02...300 кГц;
- струм споживання від лінії — не більше 0,42 мА;
- акустична чутливість — не більше 0,1 мкВ/Па;
- наробіток на відмовлення складає не менше 100000 год. Конструктивно пристрій виконаний у виді друкованої плати з електро радіоелементами і легко встановлюється в телефонну євро розетку.

Позитивні властивості розглянутих пристроїв:

- запобігання перехопленню інформації методом ВЧ - нав'язування;
- запобігання перехопленню мовної інформації через витоки дзвінкового ланцюга;
- запобігання перехоплення за допомогою мікрофонів, що передають мовну інформацію з телефонної лінії в довгохвильовому діапазоні за умови правильного розміщення фільтра на телефонній лінії.

Недоліком таких пристроїв є те, що вони не захищають від іншого різноманіття систем перехоплення.

5.2.2. Аналізатори телефонних ліній

Виявлення підключень до енергонесучих ліній

Прилади першої групи можуть бути орієнтовані на установку і безупинну роботу безпосередньо в тих енергонесучих лініях (телефонна, енергопостачання, радіотрансляція), у яких необхідно своєчасне виявлення факту підключення пристроїв несанкціонованого з'йому інформації (ПНЗІ). У цьому випадку в сучасних розробках усі методики перевірки ліній реалізуються автоматично за програмою, що керує роботою мікропроцесора аналізатора. У випадку появи ознак розпізнавання несанкціонованого підключення, прилад формує спеціальний сигнал і при необхідності включає захист. За запитом зовнішньої ЕОМ такі прилади можуть видавати протокол, що містить результати спостереження за станом лінії. Деякі моделі оснащуються пристроями безупинного запису переговорів, що ведуться в контрольованій телефонній лінії.

Інший напрямок цієї ж (першої) групи приладів — для проведення спеціальних перевірок при періодичних вимірах. У таких випадках імовірність правильного виявлення стає залежною як від метрологічних характеристик приладу, так і від мистецтва оператора. Періодичній перевірці можуть піддаватися відсіки, шахти, люки чи траси, розподільні щити, де встановлення постійних приладів контролю з різних причин неможливе.

Для того, щоб полегшити виявлення грубих підключень навіть некваліфікованим користувачем, у першій групі приладів розроблені пристрої, які відображають відхилення

напруги від установлених значень. Найбільш прості з них не мають індикації значень напруги чи струму і дозволяють тільки контролювати відхилення напруги від заданого, подаючи сигнал при несанкціонованому підключенні. Значення заданої напруги встановлюється вручну, за допомогою елементів налаштування. Звільняючи користувача від процедури ведення журналу вимірів, такі прилади на практиці можуть знайти тільки «грубі» вторгнення, подібні до зняття трубки на паралельному телефоні, і не вирішують ані задачі виявлення сучасних ПНЗІ, ані задачі їхнього придушення.

Структурні схеми подібних пристроїв наведені на рис. 5.4. Пристрій, вказаний на рис. 5.4, а, дозволяє уловити момент зменшення напруги в лінії. Він може бути налаштований як на напругу у лінії за умови, що МТТ покладена, так і на напругу в лінії при знятій МТТ. Пристрій, показаний на рис. 5.4, б, має у своєму складі шунт і дозволяє уловити момент, коли струм, що протікає через ТА при розмові, стає менше норми.

Асортимент і конструктивне виконання приладів для контролю і проведення вимірів параметрів лінії при пошуку пристроїв несанкціонованого доступу досить різноманітні. Усі пристрої критичні до заміни типу ТА.

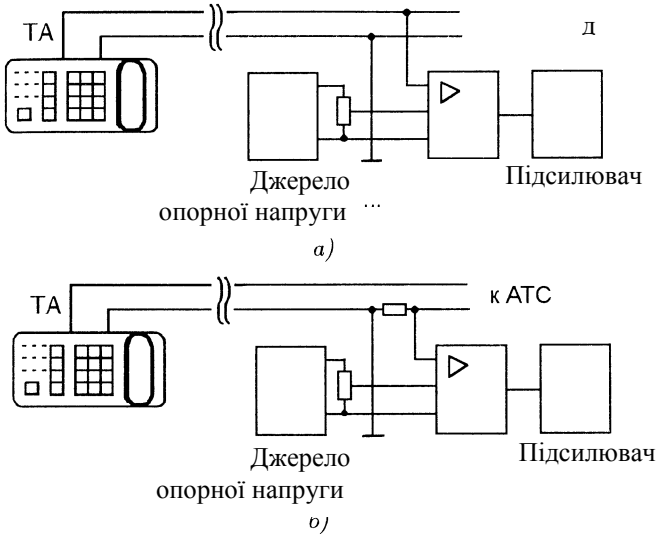


Рис. 5.4**.** Пристрій контролю телефонної лінії: *а* — напруги; *б* — струму

Наступний клас приладів призначений для вимірів і реєстрації показань у журналі. Наявні моделі приладів найчастіше дозволяють вимірювати тільки напругу в телефонній лінії при покладеній і знятій МТТ. Практично такі прилади дозволяють вирішувати задачу виявлення лише частково, а обов'язковою умовою вірогідності результатів, одержуваних з їхньою допомогою, є використання при вимірах того самого ТА. Недотримання цієї вимоги приведе до додаткових погрішностей, обумовлених значним розкидом параметрів різних ТА.

Виявлення ланцюгів живлення пристроїв несанкціонованого підключення до телефонних ліній і мереж електропостачання, включених послідовно з опором не менш 5 Ом, пристроїв, включених паралельно з опором не більш 1,5 МОм, може проводитися на екрані ЕПТ за зображенням сигналу, що зондує лінію.

Завдяки наочності зображення оператор легко може виявляти пристрої, що володіють підвищеною вхідною ємністю чи мають нелінійні елементи в ланцюгах живлення - діоди, тиристорні чи транзисторні ключі.

Вимірник неоднорідностей лінії

Принцип роботи вимірника [13]. Визначення неоднорідностей лінії можливе методом виміру КС у широкому діапазоні частот, методом виміру перехідних характеристик, методом імпульсної рефлектометрії.

Методи виміру КС і перехідних характеристик дозволяють оцінити сумарний ефект впливу неоднорідностей лінії на її характеристики, однак при наявності декількох неоднорідностей цими методами практично неможливо визначити розташування і характер кожної неоднорідності.

Метод імпульсної рефлектометрії (рефлектометрії у часовій області) дозволяє визначати місце розташування кожної неоднорідності, оцінювати її характер і чисельне значення. Сутність методу полягає в одержанні інформації про неоднорідність характеру імпульсного сигналу, відбитого від неї. Метод імпульсної рефлектометрії може реалізуватися зондуванням коротким відео імпульсом (мікросекундна імпульсна рефлектометрія) чи одиничним перепадом напруги (нано-пікосекундна імпульсна рефлектометрія).

Відстань до неоднорідності Lx визначається за часом запізнювання tз відбитого сигналу щодо фронту зондувального імпульсу

$$Lx = 0{,}5\ V\ tз = 0{,}5\ ctз / \gamma ,$$

де V — швидкість поширення електромагнітної хвилі (ЕМХ) у лінії; с — швидкість поширення ЕМХ у вільному просторі;

γ = с/V — коефіцієнт укорочення ЕМХ у лінії.

Відсутність відбитого сигналу свідчить про точне узгодження лінії за хвильовим опором. Характер і значення неоднорідності визначаються за формою відбитого сигналу в загальному випадку за відомим виразом

$$Г = (рх - ро)/(рх + ро) = Uотр/Uзонд,$$

де Г — коефіцієнт відбиття; рх — хвильовий опір лінії в місці неоднорідності; ро — хвильовий опір лінії; Uотр, Uзонд — амплітуди відбитого і зондувального сигналів відповідно.

В основу роботи вимірника покладений метод імпульсної рефлектометрії, заснований на зондуванні досліджуваної системи імпульсним сигналом із широким спектром (одиничним перепадом напруги) і спостереженні відбиття від неоднорідностей лінії за допомогою стробоскопічного методу індикації, тобто вимірі миттєвих значень повторюваних сигналів, що надходять на вхід пристрою, за допомогою коротких імпульсів напруги — строб імпульсів. Строб імпульси зрушуються у часі відносно сигналу при кожнім повторенні і, таким чином, послідовно зчитують його по крапках.

Основними вузлами вимірника є (рис. 5.5): задаючий генератор (ЗГ), генератор зондувальних імпульсів (ГЗІ), генератор горизонтального відхилення (ГГВ), підсилювачі горизонтального (ПГВ) і вертикального (ПВВ) відхилення, диференціальний пристрій (ДП), електронно-променева трубка (ЕПТ). Також у схему вимірника входять стробоскопічний перетворювач (змішувач), часовий калібратор, блоки живлення приладу і ЕПТ, регулювальні елементи для зручності роботи з приладом.

ЗГ керує роботою всієї схеми вимірника і може працювати в двох режимах: виміру і калібрування. У режимі виміру тактові імпульси генеруються мультивібратором, що задає. У режимі калібрування тактові імпульси надходять від часового калібратора. Імпульсами ЗГ запускаються ГЗІ і ГГВ. Пилкоподібні імпульси ГГВ, посилені ПГВ, надходять на горизонтально відхиляють пластини ЕПТ.

Зондувальні імпульси (ЗІ) від ГЗІ надходять через ДП в досліджувану лінію і через ДП (ослаблені) на ПВВ вертикально відхиляють пластини ЕПТ.

Відбиті неоднорідностями лінії імпульси (ВІ) надходять на вхід ДП, підсилюються і подаються на ПВВ та вертикально відхиляють пластини ЕПТ.

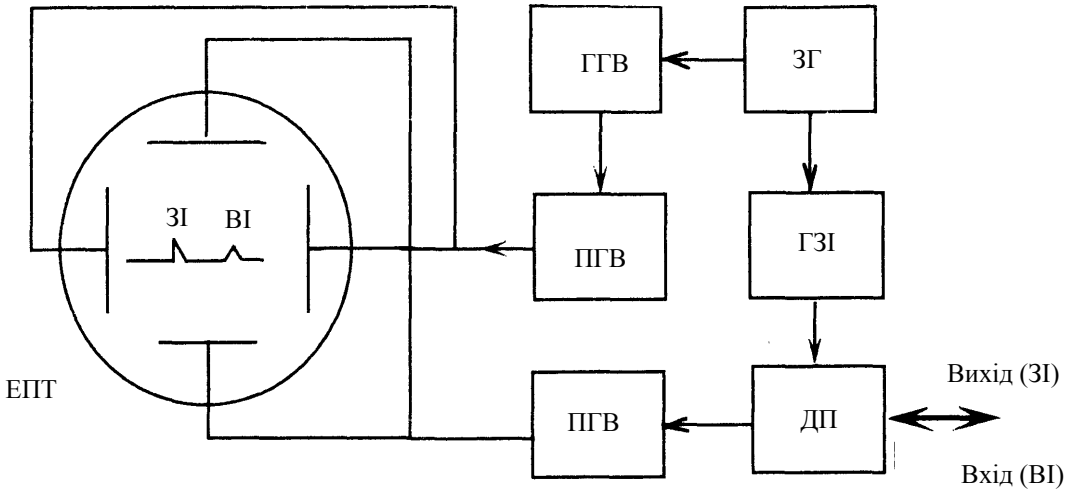


Рис. 5.5. Структурна схема роботи вимірника неоднорідностей лінії

Проведення вимірів. За допомогою вимірника (наприклад, типу Р5-11) можна проводити наступні виміри:

– визначення характеру неоднорідності;

- визначення значення неоднорідності (R, C L);
- визначення відстані до неоднорідності (ушкодження);
- визначення часової затримки;
- вимір коефіцієнта укорочення;
- вимір хвильового опору;
- вимір відстані до першої великої неоднорідності.

Визначення характеру неоднорідності. За виглядом рефлектограми можна визначити характер неоднорідності (рис. 5.7).

Визначення активних опорів (погані контакти, погана ізоляція, додаткове навантаження, стороннє підключення).

Плоска вершина зондувального перепаду сполучається з верхньою чи нижньою горизонтальною рискою шкали ЕПТ (нижньою — при збільшенні хвильового опору, верхньою — при зменшенні хвильового опору). Значення неоднорідності відраховується за номограмою (додається до опису приладу).

Визначення реактивності типу ємності шунтування і послідовної індуктивності (кабельні дефекти, допуски гнізд, помилки розмірів конструкції). Ці рефлектограми зображені на рис. 5.7.

Значення ємнісної неоднорідності визначається відповідно до виразу

$$C = 2U_o\, t\, \phi / \rho_o = 2\, K\, n\, t\, \phi / 100\, \rho_o,$$

а значення індуктивної неоднорідності визначається відповідно до виразу

$$L = 2U_o\, \rho_o\, t\, \phi = 2K\, n\, \rho_o\, t\, \phi / 100,$$

де К — встановлене значення ручки «Коеф. отраж. %.»;

п — значення відліків вертикальної шкали.

Визначення реактивностей типу послідовної ємності і паралельної індуктивності (помилки елементів конструкції високочастотних пристроїв, наприклад). На рис. 5.8 наведені рефлектограми ліній, що містять зазначені неоднорідності.

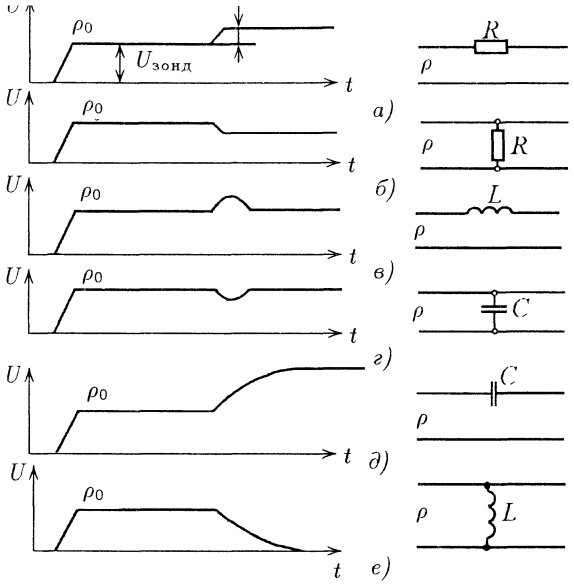


Рис. 5.6. Рефлектограми найпростіших неоднорідностей: *а, б* — погані контакти, погана ізоляція, послідовне чи паралельне навантаження; *в, г* — кабельні дефекти, допуски гнізд, помилки розмірів конструкції; *д, е* — випадкові обриви, короткі замикання чи помилки елементів конструкції високочастотних вузлів

Оцінка неоднорідностей за значенням відбитого сигналу неможлива, однак малі неоднорідності такого виду, хоча і з меншою точністю, але можуть бути оцінені за тривалістю наростання відбитого сигналу to за виразами:

$$to \approx 0{,}8\, t\,ф + 7\, рос\, In(0{,}1\, t\,ф / 2\, рос);$$

$$to \approx 0{,}8\, t\,ф + 7\{L / ро)\, in(0{,}1\, t\,ф\ ро /2L),$$

де t ф — тривалість фронту зондувального сигналу.

Значення індуктивності може бути також оцінене за тривалістю інтервалу часу Δ_t, укладеного між моментами, що відповідають значенням напруги U == 1, U = 0,5, вимірюваним на спаді осцилограми:

$$L = ро\, \Delta_t\ /1{,}386.$$

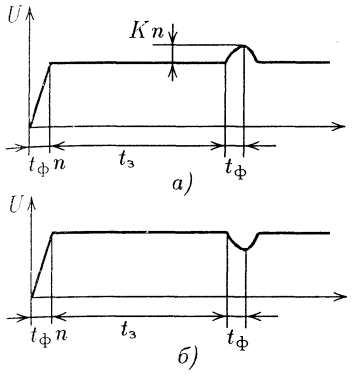


Рис. 5.7. Рефлектограми реактивних неоднорідностей: *а* — лінії з послідовною індуктивністю; *б* — лінії з паралельною ємністю

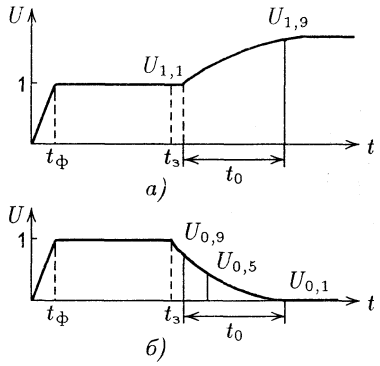


Рис. 5.8. Рефлектограми неоднорідностей: *а* — лінії з послідовною ємністю; *б* — лінії з паралельною індуктивністю

Доцільно згадати про особливості низькочастотного детектора провідних комунікацій «Візир», принцип дії якого аналогічний вищезгаданому (Вимірювач неоднорідностей лінії), а саме: у лінію подається зондувальний синусоїдальний сигнал, і відбувається реєстрація вищих гармонік струму, що виникають у напівпровідникових елементах підключеного до лінії засобу прослуховування.

5.2.3. Інші різновиди аналізаторів телефонних ліній

Аналізатор телефонних ліній SEL SP-18/T «Багер-01» забезпечує виявлення будь-яких гальванічних підключень до телефонної лінії пристроїв, які підслуховують , від місця установки до АТС поза залежністю від реактивних неоднорідностей лінії, неякісних контактів («ручних скруток») і витоків струму. Аналізатор працює в сторожовому режимі, постійно здійснюється контроль не лінійності імпедансу телефонної лінії при розімкнутому і замкнутому шлейфах, наявності напруги ВЧ - нав’язування в телефонній лінії, наявності аудіо сигналу в лінії через мікрофонний ефект дзвінкового ланцюга телефонного апарата і паралельного підключення до лінії під час телефонних переговорів.

Принцип дії аналізатора аналогічний вищезгаданому SEL SP-18/T.

Аналізатор телефонної лінії сімейства «Схил» («Схил-3», «Схил-4») призначений для виявлення несанкціонованого підключення до телефонної лінії пристроїв, що підслуховують; забезпечує світлову індикацію несанкціонованих підключень, захист переговорів, що ведуться в приміщенні, від витоку за рахунок мікрофонного ефекту. Стандартним рішенням для цих пристроїв є оформлення його в корпусі телефонної розетки.

Універсальний телефонний аналізатор TS-12 — високочутливий і точний — призначений для тестування звичайних і електронних телефонних систем. Тестує і виявляє всі сигнали, навіть ті, котрі виходять від лампочки чи дзвоника виклику. Застосовується для 50-жильної кабельної системи, що звичайно використовується разом з 5-канальними установками. Дозволяє проводити такі тестування, як перевірка напруги при знятій і покладеній трубці, прослуховування лінії, коливання тону, тестування імпульсу високої напруги і різних видів прослуховувань. Усе це може бути виконане за одну хвилину.

Телефонний аналізатор ТА17-с використовує ряд електронних тестів для встановлення спроб втручання в телефонну мережу. Тест високої напруги виявляє високовольтні містки, діодні містки, ємнісні пристрої зв'язку, важільно-перемикальні захисні механізми. Омметр із широким діапазоном виявляє пристрої, підключені через опір. Без яких-небудь додаткових пристроїв цей аналізатор перевіряє всі типи телефонних апаратів і систем, включаючи одиночні лінії, п’ятилінійні клавішні апарати, селектори і телефони «без рук». Застосовується техніка звукового зондування, але якщо трубку на досліджуваній лінії піднімуть, звук автоматично припиниться і виникне гучний сигнал тривоги.

Телефонний перевірочний пристрій ТПУ-5ВМ призначений для перевірки телефонних ліній міських і відомчих АТС на «чистоту». Пристрій дозволяє визначити наявність у телефонних лініях (крім спарених) послідовно і паралельно підключених пристроїв знімання інформації. Крім того, до складу комплекту входить покажчик телефонного наведення УП-5. Пристрій ТПУ-5ВМ дозволяє знайти:

- послідовно підключені радіо передавальні пристрої (РПП) із власним опором від 100 Ом і вище;
- паралельно підключені РПП з живленням від незайнятої лінії і струмом споживання від 0,5 мА і вище;
- паралельно підключені комбіновані РПП;
- паралельно підключені високо омні пристрої з власним опором до 20 МОм, такі як пристрої запису телефонних розмов, РПП з власним джерелом «телефонне вухо», пасивні мікрофони і т.п.;
- наявність у телефонних проводах високочастотного сигналу (так називаної «ВЧ накачки»), використовуваного для перехоплення акустичної інформації з телефонного апарата в режимі покладеної трубки; параметри сигналу, що виявляється: різниця напруги сигналу від 100 мВ і вище, частота сигналу 20... 5000 кГц.

Універсальний перевірочний пристрій провідних ліній ULAN (УЛАН УП-7)

.Рис. 5.8 Універсальний перевірочний пристрій провідних ліній ULAN

Прилад "ULAN" призначений для перевірки різних провідних комунікацій, включаючи електричну мережу 220 В, телефонні лінії, будь-які пари проводів і т.п. Прилад здатний не тільки провести відповідні виміри, але й ідентифікувати виявлені пристрої. Прилад "ULAN" може працювати як у ручному, так і в автоматичному режимах. В автономному режимі оператор задає деяку програму вимірів у вигляді набору обраних параметрів. Прилад здійснює їхній автоматичний контроль, накопичуючи інформацію в блоці пам'яті. Надалі її можна передати в персональний комп'ютер для аналізу й обробки за допомогою відповідного з'єднувача (USB).

Прилад "ulan" дозволяє виявити наступні види негласного підключення:

- У телефонних лініях (без відключення від АТС):
- послідовне підключення з еквівалентним опором більше 30 Ом;
- паралельне підключення в режимі "очікування виклику" зі струмами споживання більше 0,1 ма;
- паралельне підключення в режимі "знята трубка" зі струмами споживання більше 0,1 ма;
- високочастотні сигнали в лінії в діапазоні 0.02 - 30 Мгц при симетричному ("ВЧ - підкачування") і несиметричному ("ВЧ -нав'язування") підключенні з ефективною напругою більше 10 мв;
- низькочастотні сигнали в діапазоні 20 - 20000 Гц із ефективною напругою більше 10 мв

У знеструмлених лініях:

- паралельне підключення з активним опором більше 100 Мом;
- послідовне підключення з активним опором більше 1 Ом;
- паралельне підключення через конденсатор з постійної часу більше 1 мс;
- наявність елементів з вираженою нелінійностю від 5 % і вище в діапазоні напруги 0 -

100 В;

- наявність реактивних елементів з ємністю більше 10 % від власної ємності лінії й
- індуктивністю більше 1 Гн

У лініях електромережі 220 В:

- "сторожові пристрої" зі струмом споживання більше 0.1 ма.
- Точність виміру зазначених вище параметрів - не гірше 10 %

Крім зазначеного, прилад "ULAN" дозволяє:

- зробити вимір напруги постійного й змінного струмів у лініях, що перевіряються,
- прослухати аудіо сигнали в зазначеній лінії з використанням головних телефонів,
- простежити трасу прокладки цієї лінії в будівельних конструкціях.

Склад комплекту:

- Аналізатор - основний блок
- Комплект сполучний кабелів, адаптерів і з'єднувачів
- Головні телефони
- Інструкція для експлуатації

Покажчик провідних ліній "УП-7"

Варто також згадати про принципи дії аналізатора LBD-50, в основу роботи якого покладений метод нелінійної локації.

До переваг застосування аналізаторів телефонних ліній варто віднести те, що з'являється можливість відстежити зміни параметрів лінії і вчасно вжити заходів для проведення операції по огляду й очищенню лінії від можливих підключень.

До недоліків аналізаторів телефонних ліній варто віднести:

- відсутність чітких критеріїв оцінки несанкціонованого підключення (параметри телефонної лінії можуть змінюватися в часі в залежності від завантаженості АТС, коливань напруги в енергомережі);
- висока імовірність помилкових спрацьовувань;
- неможливість визначити усі види підключень;
- істотне зниження імовірності визначення факту підключення, якщо телефонна лінія заздалегідь не перевірена на «чистоту».

5.3. Індикатори поля

Найпростішими засобами вивчення радіозакладок є індикатори або детектори поля. Вони є не чим іншим, як приймачем з дуже низькою чутливістю, тому вони виявляють випромінювання радіозакладних пристроїв на дуже малій відстані (до 0.4 м), чим і

забезпечується селекція нелегальних випромінювань на фоні потужних сигналів. Важливою перевагою детекторів є здатність знаходити передавальні пристрої незалежно від виду модуляції. Основний принцип пошуку складається з виявлення абсолютного максимуму рівня випромінювання в приміщенні. Найкращі індикатори поля мають частотоміри, акустичні динаміки, режим прослуховування та подвійну індикацію рівня сигналу.

Так як індикатори повинні реагувати на рівень електромагнітних випромінювань, то в них застосовують амплітудні детектори, які дають додатковий ефект, який дозволяє прослуховувати сигнали від радіомікрофонів з амплітудною модуляцією і частково з частотною (за рахунок паразитної амплітудної модуляції).

Наведемо приклади сучасних індикаторів (детекторів) поля.

Детектор поля ST 007

Призначення: Виявлення й визначення місця розташування радіовипромінювань спеціальних технічних засобів (РСТС).

До таких засобів, насамперед, відносять:

- радіомікрофони;
- телефонні радіоретранслятори;
- радіо стетоскопи;
- сховані відеокамери з передачею інформації за допомогою радіоканалу;
- технічні засоби систем просторового високочастотного опромінення;
- радіомаяки систем спостереження за переміщенням об'єктів;
- не санкціоновано включені радіостанції й радіотелефони;

Принцип дії ST 007 заснований на широкосмуговому детектуванні електричного поля. Дає можливість виявлення РСТС із будь-якими видами модуляції. Має два основних режими роботи:

Пошуковий режим:

Роздільна індикація безперервного й імпульсного виду сигналів.

Індикація частоти прийнятого сигналу.

Індикація виявлення сигналів стандарту GSM і DECT.

Передача частоти радіосигналу на скануючий приймач.

Високочастотний фільтр.

Видалення фону.

Режим моніторингу:

Годинники реального часу.

Установка розкладу роботи.

Протокол подій (9 банків по 999).

Перегляд, сортування й графічний аналіз подій на IBM PC.

Використання режиму моніторингу дає можливість виявити РСТС із накопиченням і передачею інформації в імпульсному режимі.

Загальне.

Інформація відображається на графічному ЖК дисплеї з регульованим підсвічуванням.

Керування приладом виконується за допомогою клавіатури з шістьома кнопками.

Акустичний контроль здійснюється за допомогою головних телефонів або через вбудований звуковий випромінювач.

Живлення здійснюється від однієї батареї типу ААА або від блоку живлення.

Розширений інтерфейс настроювання й керування.

Вибір російської або англійської мови.

Додаткові можливості

Перепрограмування пристрою.

Для заміни програмного забезпечення (нові версії, додаткові можливості) користувачеві досить підключити ST007 до свого комп'ютера й із сайту виробника, в автоматичному режимі замінити програмне забезпечення.

Віддалений контроль.

Застосування додаткового комплекту: "віддалена антена – приймач передавач" користувач одержує можливість дистанційного контролю електромагнітної обстановки. Кількість одночасно працюючих комплектів з одним ST007 - до десяти.

Можливість підключення додаткових пристроїв індикації тривоги.

Вібровипромінювач, світлова й звукова сигналізація.

Основні технічні характеристики	
Основний блок.	
Діапазон частот, МГц	50-2500
Частота зрізу ВЧ- фільтра, МГц	400
Чутливість по входу, мв 100-1200 МГц 1200-2000 МГц	 < 0.2 < 0.45
Чутливість частотоміра, мв	< 15
Погрішність виміру частоти, %	±0.1
Динамічний діапазон індикатора, дБ	60
Напруга живлення, В: Від внутрішнього джерела живлення (батарея типу ААА) Від блоку живлення	 1.5 4
Споживаний струм, ма	80
Габарити (без антени), мм	85x53x19

Вага (без батареї), кг	0.1
Комплект віддаленої антени.	
Робоча частота, МГц	916.5/433.92
Випромінювана потужність приймача передавача, мвт	1
Габарити приймача передавача, мм	58x31x31
Габарити віддаленої антени, мм	85x53x19
Комплектність поставки	
Найменування	Кількість, шт.
1. Основний блок	1
2. Телескопічна антена	1
3. Блок живлення	1
4. Головні телефони	1
5. Сполучний кабель	1
6. Батарея типу ААА	1
7. Технічний опис і інструкція для експлуатації	1
8. Приймач передавач (поставляється додатково)	1
9. Віддалена антена (поставляється додатково)	до 10

Рис. 4.12 Детектор поля RFC-61

Детектор поля RFC-61

Детектор поля для виявлення радіопередавачів і "жучків" у приміщеннях або автомобілі. Має широкий діапазон частот (1 Мгц - 3 Ггц). Показує відносний рівень сигналу (5 секцій). Є ручка настроювання чутливості. Живиться від вбудованих акумуляторів, які забезпечують безперервний час роботи протягом 8 годин.

	RFC-61	RFC-51, RFC-52
Діапазон частот	1МГц-3ГГц	30МГц - 300МГц
Модуляція		FM
девіація		< 100 кГц

Чутливість		< -53 дБ на 500 МГц
Вага	230 м	280 м
Розмір	100х68х31 мм	
Опір	50 Ом BNC	
Корпус	Алюмінієвий із чорним анодируванням	
Батарея	Внутрішня 5хАА 600 мАч	
Живлення	9В, 300ма	

Приймач ближньої зони "СКОРПІОН 2"

Рис. 4.13 Приймач ближньої зони "СКОРПІОН 2

В 1998 році була завершена розробка приймача "Скорпіон", що зайняв гідне місце серед портативних пошукових технічних засобів. Висока оцінка, дана фахівцями приладу, підтвердила актуальність його створення. Аналіз роботи "Скорпіона" і вимог споживачів, пропонованих до роботи такого роду пристроїв, послужив поштовхом до логічного розвитку концепції й появі приймача "Скорпіон-2". "Скорпіон 2" має більше високу чутливість по всьому діапазоні частот. Поліпшення схемо технічного рішення привело до підвищення надійності і якості роботи приладу, що дозволяє йому зберігати працездатність в умовах сильних електромагнітних полів.

Прилад виконує наступні основні функції:

- Швидкого сканування у всьому діапазоні.
- Радіо тестеру на частоті, установленої оператором. Цей режим призначений для перевірки працездатності радіоприймачів, вимірників частоти й індикаторів радіовипромінювань (поля), радіопеленгаторів, систем радіомоніторингу.
- Частотоміра.
- Локалізації джерел випромінювання в ближній зоні.

Діапазон прийнятих частот, МГц	30 – 2000
Чутливість, мкв: - у діапазоні 30 – 1000 МГц - у діапазоні 1,0 – 2,0 ГГц	 не більше 25 не більше 500
Смуга пропущення на проміжній частоті, кгц	200
Час перегляду діапазону частот до 2000 МГц при відсутності сигналу, сек.	не більше 10
Точність виміру й установки частоти, кгц	не більше 10
Діапазон виміру рівня вхідного сигналу, дБ	не менш 50
Кількість каналів прийому, що виключають, шт.	4 850

Кількість виявлених сигналів, що запам'ятовують, шт.	256
Потужність генератора сигналу без модуляції в діапазоні частот до 1,0 ГГц, мвт	не більше 8
Габаритні розміри приладу, мм	не більше 300х130х60
Маса приладу, кг	не більше 2
Живлення приладу здійснюється: - через адаптер від мережі змінного струму напругою, В 220+/-22 частотою,50 Гц - акумуляторної батареї напругою,8-10 В	
Споживана потужність приладу, Вт	не більше 3
Час безперервної роботи, годин	не менш 6
Прилад при експлуатації повинен бути стійкий до кліматичних впливів: - температура навколишнього середовища, ° С - вологість повітря, %	0 - +45 не більше 80
Прилад при транспортуванні повинен бути стійкий до кліматичних впливів при температурі, ° С	-40 - +50
Прилад у транспортному впакуванні повинен бути стійкий до механічних впливів	
Час наробітку на відмову, годин	не менш 2500
Термін служби приладу, років	не менш 5

Портативний індикатор поля (ППП)

Призначений для виявлення "радіожучков" і випромінювання слабко екранованих СВЧ - печей, а також навмисного СВЧ - випромінювання в приміщенні, що викликає серцево-судинні й онкологічні захворювання.

Технічні характеристики:

- Діапазон частот: 300 Мгц - 16 Ггц
- Живлення: 9 В ("Крона")

Індикатор поля електричної мережі

Індикатор поля електричної мережі призначений для виявлення низькочастотних джерел електромагнітних випромінювань, у тому числі й радіо-закладок, що використають для передачі інформації в мережі 220 В.

Індикатор зовсім безпечний для людини, нічого не випромінює в навколишній простір і не вимагає заміни джерел живлення.

Конструктивне виконання виробу

Індикатор складається із блоку індикації зі шнуром живлення. На верхній панелі блоку індикації розміщений світло діодний індикатор рівня. На передню панель виведений регулятор чутливості індикатора.

Принцип використання виробу

Шнур живлення індикатора включається в розетку електричної мережі. Ручку чутливості обертають у праву сторону доти, поки не займеться 2-3 світло діода індикатора. Далі для порівняння індикатор підключають в іншу розетку й порівнюють показання, щоб визначити джерело випромінювання. У будь-якій розетці з радіо закладкою рівень сигналу буде в кілька разів вище, ніж у сусідній розетці, що відстоїть усього на 5-6 метрів. Для точного визначення джерела випромінювання необхідно по черзі відключати різні прилади, що живляться від електричної мережі. Якщо показання світлодіодного індикатора не досягають 2-3 запалених світлодіодов при гранично правому положенні ручки чутливості, то це свідчить про відсутність джерел електромагнітних випромінювань у даній розетці (подовжувачі) по електричній мережі 220 В.

Діапазон частот сигналів	5 кгц-30 МГц
Рівень вхідних сигналів	0,1-15В
Діапазон регулювання рівня вхідних сигналів	22 дБ
Напруга живлення	220В, 50Гц

Пристрій виявлення відеокамер "Алмаз"

Рис. 4.14 Пристрій виявлення відеокамер "Алмаз"

- Виявлення мікро відеокамер.
- Пошук загублених дорогоцінних каменів при огранці.

Пристрій "Алмаз" працює в оптичному діапазоні, тому ніякі електронні перешкоди або екранування не є перешкодою до виявлення.

"Алмаз" виявляє всі типи камер:

- відеокамери
- пінхоли ("шпигунські" камери)
- цифрові камери
- камери з автоматичним фокусуванням

"Алмаз" дозволить миттєво виявити камери, сховані в стінах і стелях, в елементах інтер'єра, навіть якщо вони перебувають у виключеному стані

Технічні характеристики:

- Вихідна потужність лазера 5-10 мвт
- Джерело живлення елемент живлення напругою 3 В.
- Час безперервної роботи від батарейки до 30 годин
- габарити 50х50х100 мм

Годинний індикатор поля (ГІП)

Рис. 4.15 Годинниковий індикатор поля (ГІП)

Годинниковий індикатор поля замаскований під звичайні годинники. На бічній панелі вимикач ON-OFF забезпечує включення індикатора поля. На задній стінці годинника є ручка установки часу (чорна) і регулятор чутливості індикатора поля (жовта або біла ручка). Для перевірки наявності джерел радіовипромінювання в калькуляторах, ручках і т.д. необхідно помахати ними поблизу годинника. Якщо при цьому індикатор не буде спалахувати, то це в більшості випадків свідчить про відсутність у них радіопередавача. Батарея годинникового механізму працює незалежно від індикатора поля. Індикатор поля живиться від акумуляторної батареї. Зарядка акумуляторної батареї виконується спеціальним зарядним пристроєм протягом 3-4 годин. Гніздо для підключення зарядного пристрою знаходиться на нижній панелі корпуса.

Годинниковий індикатор поля забезпечує:

- індикацію трансляції розмови із приміщення через засоби мобільного зв'язку відвідувачів,
- індикацію активізації свого мобільного телефону для підслуховування розмов у приміщенні,
- індикацію роботи передавачів сучасних відеокамер СВЧ діапазону
- індикацію радіо опромінення потужним джерелом СВЧ радіосигналу, що викликає розлад здоров'я персоналу приміщення

Діапазон частот	60 МГц- 9,5 ГГц
Напруга годинникової батареї	1,5 В
Напруга живлення акумуляторної батареї	3,6 В

Струм споживання індикатора поля в пасивному режимі	0,5 ма
Струм споживання індикатора поля в активному режимі	38 ма
Ємність акумуляторної батареї	300 ма/ч
Струм заряду зарядного пристрою	90-100 ма

Індикатор поля Protect 1205

Рис. 4.16 Індикатор поля Protect 1205

Індикатор поля Protect 1205 призначений для рішення наступних завдань:

- Пошук активних передавачів за допомогою радіоканалу. Кімнатні, такі що носять на тілі, телефонні й автомобільні передавачі можуть бути знайдені детектором Protect 1205.
- Визначення працюючих на передачу мобільних телефонів.
- Визначення наявності шкідливих випромінювань від пристроїв придушення мобільних телефонів або диктофонів.
- Визначення наявності шкідливих випромінювань побутової техніки.

Детектор поля Protect 1205:

- Діапазон частот 50-2400 MHz
- Заводське настроювання для роботи в міських умовах
- Конструктивне виконання у вигляді кулькової ручки. Не привертає увагу. Може носитися в нагрудній кишені сорочки або піджака. Дуже зручний для проведення перевірки під час ведення ділової бесіди, за обідом або в чужому офісі.
- Світлова індикація рівня випромінювання
- Додатковий індикатор високого рівня випромінювання
- Індикатор цифрових передавачів
- Живлення від батареї AAA

ОРГАНИ КЕРУВАННЯ

1. Індикатор високого рівня випромінювання Індикатор включається, коли рівень поля такий, що світяться 4 розподіли шкали потужності випромінювання. Індикатор призначений для схованої сигналізації про високий рівень випромінювання. Цей індикатор корисний, якщо детектор носиться в кишені. Звичайно "High Power"

включається в безпосередній близькості від "жучка" або включеного мобільного телефону. Середня відстань до включеного мобільного телефону становить 1-3 метра.

2. Антена. Служить для прийому електромагнітних хвиль. Для захисту від статичної електрики виконана усередині пластикового ковпачка. Для пошуку необхідно направляти антену на обстежуваний об'єкт.
3. Індикатор цифрової передачі даних. Індикатор світиться, якщо виявлено цифрову передачу даних. Це звичайно випромінювання стандарту GSM/DECT, але можуть бути й "жучки" з нестандартною передачею даних.
4. Індикатор рівня випромінювання. Відображає поточний рівень електромагнітного випромінювання й допомагає визначити місця розташування передавача. Для визначення місця розташування передавача необхідно переміщати детектор в обстежуваній зоні й стежити за показаннями індикатора. Звичайно на індикаторі не світитися жоден сегмент, але, іноді, у випадку наявності поруч потужних легальних джерел випромінювання (ретранслятори мобільного зв'язку й т.п.) або масивних металевих предметів може світитися один або два сегменти індикатора.
5. Гніздо для вставки батареї. Для заміни батареї обертайте це кільце проти годинній стрілки. Використайте тільки батареї LR03 (AAA). Найбільш тривалою робота детектора буде при використанні алкалайнових батарей.
6. Ручка включення/вимикання детектора. Для включення приладу натисніть на ручку й обертайте її по годинній стрілці. Повинні збігтися маркери на детекторі й ручці включення. Для вимикання приладу обертайте ручку проти годинної стрілки.

– Частотний діапазон 50 - 2400 Мгц
– Джерело живлення 1 x AAA / LR3 / R3
– Споживаний струм 50 м
– Час роботи від однієї батареї 8 годин

Індикатор поле-частотомір SEL SP-71 "ОБЕРІГ"

Індикатор поля-частотомір "Оберіг" призначений для миттєвого виявлення будь-яких джерел радіовипромінювання: радіомікрофонів, у тому числі таких що носять, радіостанцій, а також працюючих стільникових телефонів стандарту GSM і DECT.

– малогабаритність;
– відсутність зовнішньої антени;
– реалізовано алгоритм адаптивного цифрового фільтра для зниження ймовірності помилкових спрацьовувань;
– наявність безшумної індикації (вібраційний дзвінок);
– камуфляж (конструктивно виконаний у корпусі пейджера)

Серед пошукового обладнання індикатори електромагнітного поля займають одне з провідних місць. Індикатори поля при своїй відносній простоті, невисокій ціні, малих габаритах позволяють виявляти джерела практично будь яких радіосигналів, в тому числі складних—широкосмугових, зі скачками частоти, псевдо шумових та інших.

У табл 5.16 наведені основні характеристики індикаторів поля.

Індикатор поля BLOODHOUND дозволяє фіксувати наявність місцевих радіовипромінювань у приміщеннях, автомобілях і т.д., локалізувати з похибкою до 10...15 см місце розташування джерел малопотужних випромінювань. Комплект містить детектор радіовипромінювань і тестовий транслятор (імітатор передавача).

Технічні характеристики: дальність виявлення до 8 м, живлення 9 В, модуляція FM.

Таблиця 5.16

Основні характеристики індикаторів поля

Модель	Діапазон частот, МГц	Акусти - чна зав'язка	Індикація	Примітки
D006	50...1000	є	Світлодіодна шкала; звукова з можливістю вимикання	Сертифікат Гостехкомісії РФ
D008	50... 1500	є	Світлодіодна шкала; звукова	Сполучений із приймачем для перевірки провідних комунікацій (до 500 В; 0,05...7 МГц)
PT022	10...1000	є	Стрілочний індикатор; звукова	Вбудовані смугові і режекторні фільтри
PT025	10...1000	є	РК- дисплей, звукова	Аналог PT022 4- убудовані фільтри
RM-10	80...8000	немає	Світлова, звукова з можливістю вимикання	Потайливого носіння (портмоне)
R-finder	20...1300	немає	Світлова, звукова	Мініатюрний
PIF-2	30...2500	немає	Стрілочний індикатор; звукова	Вбудовані режекторні фільтри, таймер
Сканер-2	30...2500	є	Стрілочний індикатор; звукова	Вбудовані смугові і режекторні фільтри
ИПФ-6	30...2500	є	Світлова, звукова з можливістю вимикання	Аналог «Сканер-2» + частотомір

ДИ-04	20...1000	є	Світлова, звукова з можливістю вимикання	Режими: черговий і пошуковий. Тестовий звуковий генератор
ДИ-К	60...1000	Немає	Світлова	Закамуфльований у настільні годинник
ИЭП	60...1500	Немає	Світлова, звукова з можливістю вимикання	Мініатюрний
BLOOD-HOUND	20...800	є	Світлова, звукова	Закамуфльований у валізу

5.4. Скануючі приймачі

Радіоприймальні пристрої є більш складними та надійними засобами виявлення радіозакладок ніж індикатори поля та частотоміри. Але вони повинні задовольняти таким умовам:

- мати можливість настройки на частоту роботи радіомікрофонів;
- мати можливість виділяти потрібний сигнал за характерними ознаками на фоні завад;
- мати можливість де модулювати різні види сигналів.

Для вирішення першої задачі треба пам‘ятати, що радіомікрофони працюють в діапазоні від 20 до 1500 МГц. Отже, приймач повинен перекривати весь цей частотний діапазон.

Для вирішення другої задачі приймач повинен мати смугу пропускання ($\Delta f_{\text{і}}$), яка приблизно дорівнює ширині спектру сигналу та мати добру вибірковість сигналу.

Для вирішення третьої задачі треба пам‘ятати, що рідіозакладки можуть мати амплітудну модуляцію (AM), вузько смугову (NFM) та широкосмугову (WFM) частотну модуляцію, амплітудну модуляцію з однією смугою (SSB) з режимом прийому верхньої (USB) та нижньої бокової смуги (LSB) а також модуляцію для передачі телеграфних сигналів (CW). Наприклад скануючий приймач AR-5000.

Скануючий приймач AR-5000.

Стаціонарний скануючий приймач японської фірми AOR Ltd. AR-5000 одержав високу оцінку фахівців завдяки ряду унікальних характеристик: широкій смузі робочих частот, високої швидкості сканування (CyberScan), набору смуг пропускання, які перемикаються, як по 2-й так і по 3-й ПЧ,а також по звуковій частоті, автоматичної конфігурації вхідних перед селекторних кіл, включаючи функцію підключення попереднього підсилювача й атенюатора. У середині 2003 року випущена нова модифікація приймача AOR AR5000A, основні відмінності - розширений діапазон 0.01-3000 Мгц, збільшений обсяг пам'яті, поліпшена робота з магнітофоном.

Рис. 4.17 Скануючий приймач AR-5000

- Широкий діапазон: 0.01 - 3000 Мгц зі збереженням високої чутливості у всьому діапазоні.
- Малі габарити й вага для даного типу пристроїв(217x100x260 мм, 3,5 кг).
- Висока стабільність частоти, (температурна нестабільність ТСХО: $\pm 1{,}5*10^{-6}$ у діапазоні температур *0°C...+ 50°C*; старіння: $\pm 1*10^{-6}$/за рік).
- Програмувальний крок перебудови від 1 Гц до 1 Мгц, для всіх режимів.
- Функція автоматичного підстроювання частоти (AFC), AR5000 підбудовується на частоту прийнятого сигналу.
- Великий дисплей відображає багато різної інформації (частота, режим, АРП й т.д.) символьно-цифрові коментарі (які також можуть бути збережені в пам'яті для ідентифікації даних).
- Аналоговий індикатор дозволяє стежити за відносною величиною сигналу.
- Автоматично або примусово включення попереднього підсилювача або атенюатора.
- Зручність настроювання. Передбачено кілька методів уведення частоти: із клавіатури, за допомогою 2-х ручок настроювання.
- Види модуляції: AM, FM, SSB (USB, LSB), CW
- Номінальні смуги пропускання приймача: 500 Гц (опція); 3 кГц; 6 кГц; 15 кГц, 30 кГц; 110 кГц; 220 кГц.
- Режим автоматичної установки виду модуляції й кроку перебудови частоти по робочому діапазону.
- Повне відновлення несучої в режимі SSB, що поліпшує якість прийому.
- Потрійне перетворення частоти Fпч = 622 Мгц; 10,7 Мгц; 455 кГц..
- Типи сканування й перегляду: програмувальне, діапазонне, по каналах пам'яті, по видах сигналу (голос, тон, CTCSS, DTMF) по групах каналів пам'яті, пріоритетне, з автоматичним записом частот. Час затримки регулюється. Система "пошуку голосу" дозволяє пропускати шумові сигнали та без модуляції.
- 2000 чарунок пам'яті в 40 банках. Кожній чарунці пам'яті й банку пам'яті можна

привласнити ім'я - коментар довжиною до 8 символів. 20 банків перегляду з автоматичним записуванням частот

- RS232 порт для зв'язку з комп'ютером. Вихід-BNC-вихід проміжної(Рознімання: частоти IF = 10,7 Мгц і BNC - вхід опорної частоти STDin=10 Мгц. ACC1 і ACC2-рознімання. Два антенних гнізда, які перемикаються Тип-N-типу й Тип-PL-типу, гнізда для навушників і зовнішнього гучномовця, гніздо "MUTE" при використанні AR5000 з передавачем.
- Живлення AR-5000 від джерела напругою 12-16 В, струм 1 А (входить у комплект).
- Вихідна звукова потужність - 1,7 Вт на навантаженні 8 Ом.

Аксесуари

- DA3000 – диско конусна антена 25 Мгц - 2000 Мгц.
- MA500 - компактна VHF/UHF антена на магнітній підставі.
- CR5000 - кабель для зовнішнього магнітофона.
- CT5000 - CTCSS - модуль, який вбудовується.
- SDU5500 - панорамний індикатор спектра
- DS8000 - аналоговий демаскуватор мовних сигналів.
- Фільтри Коллинза:

  MF6 (AM/FM 5,5 кгц/3 дБ; 11 кгц/60 дБ);

  MF2,5 (SSB 2,5 кгц/3 дБ; 5,2 кгц/60 дБ);

  MF500 (CW 500 Гц/3 дБ; 2 кгц/60 дБ).

Технічні характеристики AR5000A

Діапазон частот (МГц)	0.01...3000				
Види модуляції	SSB (USB, LSB), AM , CW, FM				
Чутливість (мкв) (AM при 10дБ S/N, SSB, CW, FM при 12дБ SINAD)	Діапазон	AM 6 кГц	SSB/CW 3 кГц	FM 15 кГц	FM 220 кГц
	10 - 40 кГц	63	17,7	-	-
	40 - 100 кГц	4,46	1,25	-	-
	100 кГц - 2 МГц	2,23	0,40	-	-
	2 МГц - 40 МГц	1,25	0,40	0,56	1,58
	40 - 1000 МГц	0,63	0,3	0,4	1,28
	1000 -3000 МГц	0,63	0,3	0,36	0,89
Швидкість сканування	45 каналів або кроків перебудови частоти в секунду				
Напруга живлення/струм споживання	12 - 16 В / 1 А (типове)				

АКОР-1 Автоматизований комплекс виявлення радіовипромінювань

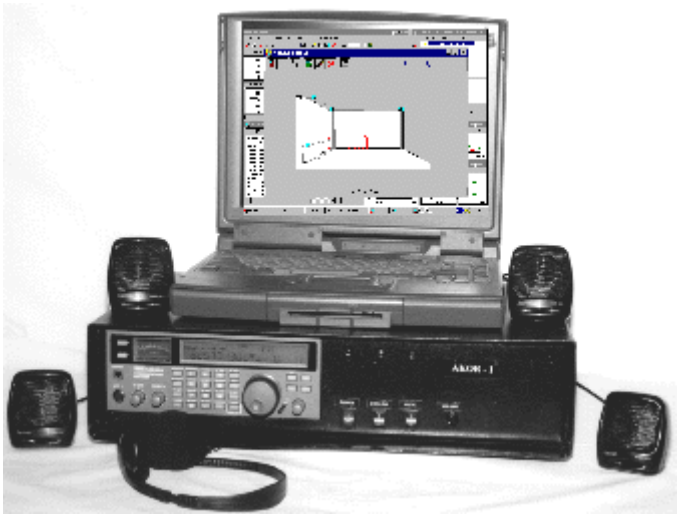


Рис. 4.18 Комплекс АКОР-1

Комплекс АКОР-1 є професійною багатофункціональною системою, призначеної для:

- перевірки приміщення, електромережі, телефонних ліній і інших комунікацій на наявність пристроїв негласного знімання мовної інформації;
- контролю робочого місця керівника, окремих кабінетів або всього офісу від появи пристроїв знімання, що використають дистанційне включення або короткочасну роботу, а також внесених на час проведення наради, переговорів і ін. закритих заходів;
- виявлення каналів витоку інформації від засобів оргтехніки, зв'язку й іншої апаратури по електромагнітному полю.

Завдяки впровадженню оптимальних методів виявлення й аналізу сигналів (швидке свіпування по діапазону, просторова селекція сигналів, кореляційна обробка по тест-сигналу або звуковому фону, аналіз сигналів на гармоніки, звукове зондування, ведення по контрольованих об'єктах архівів даних по сигналах) комплекс забезпечує:

- гарантоване виявлення будь-яких засобів знімання інформації, що використають у т.ч. закриті види модуляції (інверсія спектра, дельта модуляція, сигнал схожий на шум, цифрова передача) і стрибкоподібна зміна частоти;
- автоматичну роботу без її демаскування й без помилкових спрацьовувань на сторонні сигнали;
- підключення генератора автоматичного придушення пристроїв знімання інформації;
- використання в стаціонарному й мобільному варіантах.

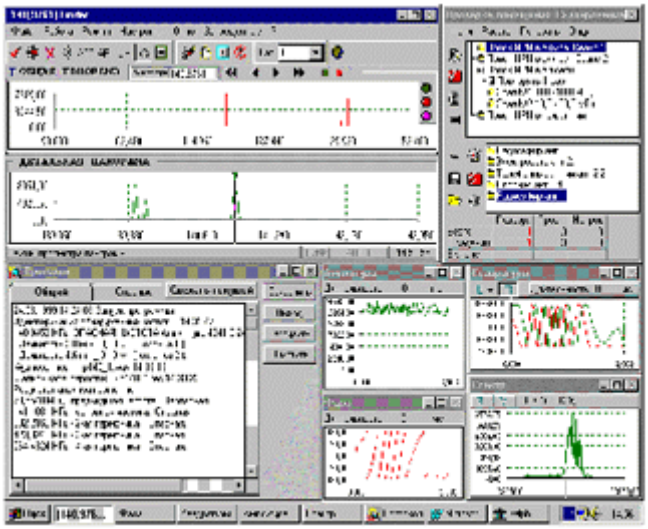


Рис. 4.19 Аналіз сигналів на АКОР-1

Склад базового варіанта комплексу:

- приймально - аналізуючий пристрій, що складається із РПП AR.5000 - для мобільного варіанта або AR.8000- для портативного варіанта (допускається поставка Замовником), швидкодіючого блоку панорамного огляду. блоків 4-х канальних ВЧ- і НЧ - комутаторів і НЧ - підсилювача. генератора тест-сигналу, блоку живлення; широкосмугова антена (2 шт.). звукові датчики (4 шт.); мережний адаптер, комплект монтажних кабелів
- спеціальне програмне забезпечення;
- технічний опис і інструкція для експлуатації;
- стаціонарна або портативна ПЕОМ не гірше Pentium-200/16/2.1 (допускається поставка Замовником);
- акумуляторна батарея ємністю 4 А/годин й зарядний пристрій.

Технічні характеристики		
Діапазон робочих частот (для AR.5000), МГц	0.01 - 2600	Можливе розширення діапазону
Швидкість аналізу частотного діапазону, МГц/сек..	50	
Чутливість в автоматичному режимі, мкВ	1 - 3	
Дальність дії в автоматичному режимі, м	50	Для випромінювача потужністю 50 мкВт
Точність визначення місця розташування в автоматичному режимі, м	±0.1	
Середній час виявлення: при первинній перевірці приміщення не більше, хв	5	

при контролі приміщення не більше, сек..	20 - 30	
Маса (без урахування ПЕОМ): - мобільний варіант, кг - портативний варіант, кг	 9 5	без акумулятора
Габарити (без урахування ПЕОМ): - мобільний варіант, мм - портативний варіант, мм	 460x335x120 420x230x55	
Електроживлення, В	220±12	

Професійна моніторингова програма "Філін-98"

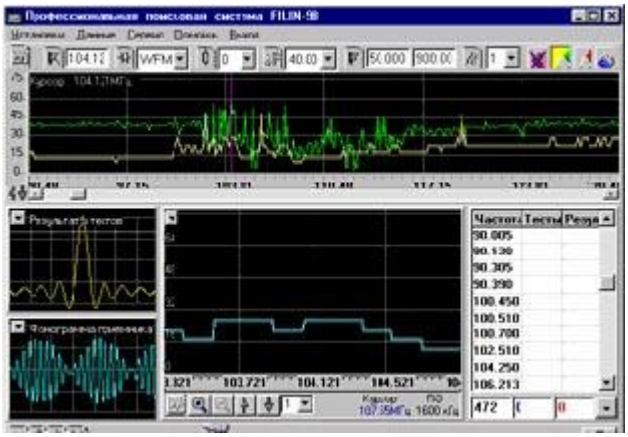


Рис. 4.19 Програма "Філін-98"

Програма призначена для створення на її основі програмно-апаратних комплексів пошуку й локалізації засобів несанкціонованого знімання акустичної інформації.

До складу комплексу входять апаратні засоби, що безпосередньо здійснюють пошук засобів несанкціонованого випромінювання й керуюча програма ФІЛІН-98. Як апаратні засоби може використатися будь-який скануючий радіоприймач із широкої номенклатури радіоприймальних засобів фірм ICOM і AOR Co. Ltd, а також радіоприймачі WiNRADi. Крім того, як апаратні засоби можуть використатися аналізатори спектра (типу ESA-L1500, серії 859... фірми Hewlett Packard) або спеціально розроблені пристрої швидкого панорамного аналізу (аналоги аналізатора спектра). У другому випадку швидкість і якість пошуку істотно зростають. Керування апаратними засобами, знімання, зберігання, обробка й подання даних, керування всіма режимами роботи комплексу здійснюються керуючою програмою ФІЛІН-98.

Програма ФІЛІН-98 призначена для функціонування в операційних системах Windows 95, Windows 98. Вимоги до комп'ютера: ПЕОМ із установленою операційною системою Windows-95/98, сумісної з Windows звуковою картою (бажано Creative Sound Blaster 16, ESS1869, ESS1879, інші типи - необхідна консультація) і комплектом акустичних колонок. У програмі реалізована більшість із відомих у сьогодення алгоритмів виявлення радіозакладок, які використовуються у комплексах OSCOR 5000, АРК-Д1, АРК-Д3, RS-1000 і інших, що забезпечує високу ймовірність виявлення засобів несанкціонованого знімання інформації при низькому рівні хибної тривоги. Важливою особливістю програми є реалізація концепції єдиного робочого екрана, що містить у собі всю необхідну інформацію, що позбавляє користувача від необхідності відкривати ієрархічну систему вікон і підвищує ефективність роботи. Для ідентифікації радіозакладок у програмі використаються різні типи тестів:

активний, пасивний, параметричний і тест на наявність гармонік. Якщо є спеціалізовані апаратури швидкого панорамного аналізу, то стають доступні ще два тести, реалізованих на базі цих апаратур - зовнішній активний і зовнішній пасивний. Результат виконання кожного з тестів несе в собі досить повну інформацію про наявність або відсутність рідіозакладки. Комплексне використання тестів дозволяє домогтися набагато більшої ймовірності виявлення при меншій імовірності хибної тривоги. Програма може без участі оператора здійснювати всі необхідні для оптимального рішення завдань установки параметрів використовуваних апаратур і функції керування аж до подання кінцевих результатів, залишаючи для користувача тільки функцію первісного визначення конфігурації комплексу. Таким чином, навіть не дуже кваліфікований оператор може одержувати надійні й достовірні результати. Все це дає можливість стверджувати, що програмою повністю реалізується основний принцип автоматичної роботи устаткування : "включив - одержав результат".

З іншого боку, програма має гнучкий, інформативний інтерфейс, що відображає процес роботи комплексу, характеристики сигналів, проміжні результати їхнього аналізу й дозволяє кваліфікованому операторові при бажанні самому проводити детальний аналіз прийнятих сигналів по їх спектральним складовим, осцилограмам, кореляційним функціям і іншим характеристикам. Дана особливість програми дозволяє використати її й для рішення широкого кола прикладних завдань радіомоніторингу. У число таких завдань входить накопичення даних про радіоелектронну обстановку й виявлення нових сигналів; контроль частот радіоелектронних засобів або систем радіозв'язку з різними параметрами випромінюваного сигналу (видом модуляції, шириною спектра, рівнем у точці прийому й ін.); оцінка електромагнітної сумісності радіоелектронних засобів, завантаження частотних діапазонів і інтенсивності використання фіксованих частот; аналіз індивідуальних особливостей спектра окремого сигналу; контроль виконання обмежень на використання радіоелектронних засобів, дотримання правил радіообміну; виявлення інформативних електромагнітних випромінювань, що виникають при роботі обчислювальної техніки, засобів зв'язку, оргтехніки; оцінка ефективності використання технічних засобів захисту інформації й ін. Програма створювалася на заміну СПО "Sedif Scout".

Індикатор сторонніх електричних сигналів ПСЧ-5

Індикатор сторонніх електричних сигналів ПСЧ-5 виконує наступні функції:

- дослідження електричних сигналів у провідних системах, силових і слабкострумових мережах;

– виявлення акустичних і вібраційних каналів витоку мовної інформації і пристроїв, що підслухують інформацію в ІЧ діапазоні.

У комплект постачання входять: пошуковий пристрій, контрольний пристрій, який озвучує , виносний мікрофон, виносний вібродатчик, виносний ІЧ-детектор, головні телефони, кабель для силових мереж, кабель для слабкострумових ліній, щупи електричні, елементи живлення.

Багатофункціональний пошуковий прилад «Піранья»

Рис. 4. 20 Пошуковий прилад «Піранья»

Багатофункціональний пошуковий прилад «Піранья» може працювати в наступних режимах: високочастотний детектор-частотомір; скануючий аналізатор провідних ліній; детектор ІЧ-випромінювань; детектор низькочастотних магнітних полів; вібро акустичний приймач; акустичний приймач; провідний акустичний приймач. До його складу входять: основний блок керування, обробки та індикації, антени телескопічна та ВЧ, адаптер скануючого аналізатора, провідних ліній, насадки типу «голка», «Крокодил» та «220», кабель , магнітний датчик, інфрачервоний датчик, акустичний датчик, вібро акустичний датчик, перехідник, головні телефони та елемент живлення.

Прилад призначений для вирішення таких задач:

1. Виявлення факту роботи і локалізації розташування радіо випромінюючих спеціальних технічних засобів, які створюють потенційно небезпечні, з погляду витоку інформації, радіовипромінювання. Такі як:

– радіомікрофони;

– телефонні радіоретранслятори.

- радіо стетоскопи;

- сховані відеокамери з радіоканалом передачі інформації;
- технічні засоби систем просторового високочастотного опромінення в радіодіапазоні;
- технічні засоби передачі зображення з монітора ПЕОМ по радіоканалу;
- радіомаяки систем спостереження за переміщенням об'єктів (людей, транспортних засобів, вантажів і т.п.);
- не санкціоновано включені радіостанції, радіотелефони й телефони з радіо подовжувачем;
- технічні засоби обробки інформації, робота яких супроводжується виникненням побічних електромагнітних випромінювань (елементи фізичної архітектури ПЕОМ, факси, ксерокси, деякі типи телефонних апаратів і т.п.).

2. Виявлення й локалізація місця розташування спеціальних технічних засобів, що працюють із випромінюванням в інфрачервоному діапазоні. До таких засобів, у першу чергу, відносять:

- заставні пристрої добування акустичної інформації із приміщень із її наступною передачею по каналу в інфрачервоному діапазоні;
- технічні засоби систем просторового опромінення в інфрачервоному діапазоні.

3. Виявлення й локалізація місця розташування спеціальних технічних засобів, що використають для добування й передачі інформації провідні лінії різного призначення, а також технічних засобів обробки інформації, що створюють наведення інформативних сигналів на поруч розташовані провідні лінії або стік цих сигналів у лінії мережі електроживлення. Такими засобами можуть бути:

- заставні пристрої, що використають для передачі перехопленої інформації лінії мережі змінного струму 220В і здатні працювати на частотах до 15Мгц;
- ПЕОМ і інші технічні засоби виготовлення, розмноження й передачі інформації;
- технічні засоби систем лінійного високочастотного нав'язування, що працюють на частотах понад 150кгц;
- заставні пристрої, що використають для передачі перехопленої інформації абонентські телефонні лінії, лінії систем пожежної й охоронної сигналізація з несучою частотою понад 20кгц.

4. Виявлення й локалізація місця розташування джерел електромагнітних полів з перевагою (наявністю) магнітної складового поля, трас прокладки схованої (непозначеної) електропроводки. потенційно придатної для установки заставних пристроїв, а також дослідження технічних засобів, що обробляють мовну інформацію. До числа таких джерел і технічних засобів прийнято відносити:

- вихідні трансформатори підсилювачів звукової частоти;
- динамічні гучномовці акустичних систем;

- електродвигуни магнітофонів і диктофонів;

5. Виявлення найбільш уразливих місць, з погляду виникнення віброакустичних каналів витоку інформації, а також оцінка ефективності систем віброакустичного захисту приміщень.

6. Виявлення найбільш уразливих місць, з погляду виникнення каналів витоку акустичної інформації, а також оцінка ефективності звукоізоляції приміщень.

Опис режимів роботи приладу.

Кожний з режимів роботи приладу характеризується набором тільки йому властивих властивостей і основних, попереднє закладених, можливостей. Нижче приводиться їхній короткий опис.

Режим високочастотного детектора-частотоміра

У цьому режимі прилад забезпечує прийом радіосигналів у діапазоні від 30 до 2500 Мгц у ближній зоні (у межах об'єкта спец робіт), їх детектування й вивід для слухового контролю й аналізу у вигляді тональних посилок, що чергуються, (щигликів), або у вигляді явних фонограм при їхньому прослуховуванні як на убудований гучномовець, так і на головні телефони.

У кожний конкретний момент часу на фоні реальної завадової обстановки приймається й детектується найбільш потужний із всіх радіосигналів у робочому діапазоні. Його рівень, щодо встановленого порога детектора, відображається на двострочному індикаторі з 40-сегментною шкалою у верхній частині рідкокристалічного дисплея.

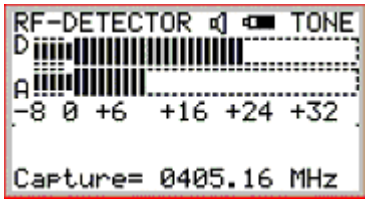


Рис. 4.21 Двохсмуговий індикатор приладу «Піранья»

Розходження у використанні двох шкал полягає в наступному: верхня шкала індукує усереднені значення про детектованого сигналу, а нижня його пікові значення. Відповідно, у верхньому рядку будуть переважати сигнали з постійною несучою частотою (без модуляції, частотно модульовані), а в нижній близькі до імпульсних видів сигналів (наприклад сигнали з амплітудною й імпульсною модуляцією). Наявність індикації на двох шкалах говорить про змішаний вид сигналу на вході детектора (наприклад, телевізійний сигнал).

У випадку впевненого прийому сигналу зі свідомо відомими параметрами індукується напис ідентифікації сигналу під цифровою шкалою рівня сигналу.

Можлива індикація виявлення сигналів наступних стандартів: GSM (напис "GSM"), DECT (напис "DECT").

Залежно від умов і цілей проведення контрольно-пошукових робіт є можливість вибору й установки необхідного (найбільш раціонального) порога детектора.

Одночасно здійснюється вимір поточних значень частоти прийнятого радіосигналу й визначення найбільш стійкого її значення (для сигналів з постійною несучою частотою). І ті, і інші значення в явному виді відображаються на екрані дисплея.

Для якісної оцінки ступеня мінливості частоти прийнятого радіосигналу використається спеціальна обчислювальна процедура, результати якої відображаються на екрані дисплея у вигляді тонкої горизонтальної лінії яка динамічно змінює довжину безпосередньо над цифровими символами поточних значень частоти прийнятого сигналу (залежність довжини лінії й стабільності частоти - обернено пропорційна, тобто чим вище мінливість частоти радіосигналу, тим коротше довжина лінії як індукується)

Технічні характеристики	
Діапазон робочих частот, МГц	30-2500
Чутливість, мв	<2 (200МГц-1000МГц)
	4 (1000МГц-1600МГц)
	8 (1600МГц-2000МГц)
Динамічний діапазон, дБ	60
Чутливість частотоміру, мв	<15 (100МГц-1200МГц)
Точність виміру частоти, МГц	± 0,1

Порядок керування приладом у режимі високочастотного детектора-частотоміра.

Підключити телескопічну антену, використовуючи перехідник, або високочастотну антену до гнізда "RF ANT". Включити живлення приладу.

Установка "нульового" порога детектора здійснюється при включенні автоматично. Якщо буде потреба, натисканням кнопок " " або " " установити поріг детектора вручну, керуючись показаннями додаткової шкали "min - - -|- - -max". Якщо буде потрібно, натисканням кнопки " " повернутися до автоматичної установки порога.

Візуально по кількості повністю пофарбованих елементів індикаторів рівня сигналу й "на слух" по частоті щигликів в убудованому гучномовці або головних телефонах оцінити рівень прийнятого сигналу.

При необхідності натисканням кнопки "SET" і встановити потрібні границі динамічного діапазону: (-8..16)дб; (-8..32)дб; (-8..48)дб.

Натиснути кнопку "RUN/STOP" і зупинити (при необхідності) динамічні виміри рівня й частоти радіосигналу. Повторним натисканням цієї кнопки відновити динамічні виміри.

Натиснути кнопку "ENTER" (переклад звукової індикації в режим "AUD"), прослухати наявність і зміст потенційно небезпечних модульованих радіовипромінювань.

Натисканнями кнопок "+" і "-" установити необхідну гучність виведеного або на убудований гучномовець, або на головні телефони звукового сигналу (тонального або демодульованого).

Натиснути кнопку "OSC" і перейти (при необхідності) до осцилографічного контролю параметрів сигналу.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра демодульованого сигналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Режим скануючого аналізатора провідних ліній

У цьому режимі прилад забезпечує прийом і відображення параметрів сигналів у провідних лініях різного призначення (електричної мережі, телефонної мережі, обчислювальних мереж, пожежної й охоронної сигналізації й т.п.) як знеструмлених, так і тих що перебувають під напругою (постійною або змінною) до 600В.

Підключення приладу ST 031 "Піранья" до аналізованої лінії виконується через універсальний адаптер з комплектом насадок типу "220", "Крокодил" і "Голка". Крім того, адаптер оснащений пристроєм ослаблення сигналів по входу, що включається при необхідності спеціальним перемикачем на корпусі адаптера, а також двома світло діодами для індикації наявності в провідній лінії змінної або постійної напруги.

Прийом сигналів здійснюється шляхом автоматичного або ручного сканування в частотному діапазоні до 15Мгц. Крок перебудови фіксований і становить 5кгц і 1кгц при автоматичному й ручному скануванні, відповідно.

Для адаптації настроювання приладу до умов і завдань контрольно-пошукових робіт передбачена можливість вибору напрямку й швидкості автосканування, а так само два варіанти установки необхідних границь діапазону перебудови (завдання початкової й кінцевої частоти або завдання центральної частоти перебудови й ширини діапазону).

Класифікація сигналів у контрольованих провідних лініях здійснюється на основі аналізу автоматично виведеної на екран дисплея панорами (діаграми), що відображає частотні складові спектра прийнятого сигналу і його рівень на кожній з них. При здійсненні ручного сканування (точного настроювання) додатково забезпечується можливість безпосереднього слухового контролю прийнятого сигналу шляхом виводу його на убудований гучномовець або головні телефони.

Технічні характеристики	
Діапазон сканування, МГц	0,01-15
Чутливість, при с/ш 10 дБ, мв	<0,5
Крок сканування, кГц	5(1)
Швидкість сканування, кГц	50-1500
Смуга пропущення, кГц	10
Вибірковість по сусідньому каналі, дБ	30
Режим детектування	АМ, ЧМ
Допустима напруга в мережі, В	600

Порядок керування приладом у режимі скануючого аналізатора провідних ліній.

Підключити мережний адаптер до гнізда "PROBES", а його щупи до провідної лінії (лінії електромережі з напругою до 600В.

Включити живлення приладу.

Дочекатися 2-3-х кратного "пробігу" діапазону сканування підрядковим маркером в границях , що встановлюються автоматично, 0.0-10.450MHz.

Установити необхідні (найбільш раціональні) границі частотного діапазону сканування.

Натиснути кнопку "SET", потім кнопку "4". Натисканням кнопок із цифровим маркуванням набрати число, що відповідає нижній границі діапазону.

Натиснути кнопку "ENTER" і підтвердити завершення установки значення нижньої границі.

Натисканням кнопок із цифровим маркуванням набрати число, що відповідає верхній границі діапазону.

Натиснути кнопку "ENTER" для підтвердження установки верхньої границі діапазону.

При помилці в процесі набору значень частот нижньої й (або) верхньої границь діапазону сканування натиснути кнопку " " і скинути набране число.

Натиснути кнопку " " або " " і вибрати потрібний напрямок і швидкість сканування.

Нажати кнопку "SET", потім кнопку "3" до появи на екрані в четвертому рядку напису "3 - > THRESHOLD level".

Натиснути кнопку "ENTER" і повернути на екран зображення панорами.

Натисканням кнопок " " і " " установити найбільш зручна межа індикації вимірника рівня сигналу (напис під горизонтальною віссю "level threshold = XX%").

Натиснути кнопку "RUN/STOP" і зупинити автосканування в необхідній точці частотної осі. Натисканням кнопок " " або " " провести точне ручне настроювання на частоту, що цікавить. Прослухати демодульований сигнал.

Натиснути кнопку "ENTER (AM/FM)" і вибрати вид демодуляції ("на слух", по якості його відтворення).

Натиснути кнопку "RUN/STOP" і повернутися до автосканування.

Включити систему автоматичної зупинки сканування на найбільш виражені (по амплітуді) частотних складові панорами.

Натиснути кнопку "SET", потім кнопкою "3" установити в четвертому рядку меню напис "3 - > Ї SQUELCH level".

Натиснути кнопку "ENTER".

Кнопками " " і " " вибрати бажаний рівень автоматичної зупинки автосканування (по положенню короткої горизонтальної риски в правій частині екрана). Після зупинки сканування кнопками " " і " " зробити уточнення настроювання по ознаці якості демодульованого сигналу. Для продовження сканування нажати кнопку "RUN/STOP".

Включити (при необхідності) режим вирахування спектрів.

Натиснути кнопку "SET", потім кнопку "2" і встановити напис "2 - > Difference ON D2-1".

Натиснути кнопку "ENTER" для початку процедури вирахування спектрів.

Вийти з режиму вирахування спектрів.

Натиснути кнопку "SET", потім кнопкою "2" і встановити напис "Difference OFF".

Натиснути кнопку "ENTER".

Записати (при необхідності) зображення панорами в енергонезалежну пам'ять.

Натиснути кнопку "SAVE", потім кнопку "ENTER".

Викликати з пам'яті зображення, що цікавить, панорами.

Натиснути кнопку "LOAD".

Натиснути кнопку "RUN/STOP" і повернути на екран динамічно відображувану панораму.

Стерти (видалити) з пам'яті зображення якої-небудь панорами.

Натиснути кнопку "LOAD", потім "SAVE" і "ENTER".

Натиснути кнопку "OSC" і перейти (при необхідності) до осцилографічного контролю параметрів сигналу.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра сигналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Режим детектора інфрачервоних випромінювань

У цьому режимі прилад забезпечує, з використанням виносного датчика, прийом випромінювань джерел інфрачервоного діапазону в ближній зоні (у межах конкретного приміщення на об'єкті спеціальних робіт), їх детектування й вивід для слухового контролю й аналізу у вигляді або тональних посилках, що чергуються, (щигликів), або у вигляді явних фонограм при їхньому прослуховуванні як на убудований гучномовець, так і на головні телефони.

У кожний конкретний момент часу на фоні реальної завадової обстановки приймається й детектується найбільш потужний із всіх сигналів у робочому діапазоні.

Його рівень, щодо встановленого порога детектора приладу, відображається на індикаторі рідкокристалічного дисплея з 21-сигментной шкалою. При цьому, залежно від умов і цілей проведення контрольно-пошукових робіт, передбачена можливість вибору й установки необхідного (найбільш раціонального) порога детектора приладу.

У сукупності цим забезпечується можливість оперативної попередньої класифікації сигналів і їхніх джерел.

Технічні характеристики	
Діапазон частот, кГц	770-100
Гранична чутливість, Вт/Гц^2	10(-13);
Кут поля зору, град.	30
Смуга частот, МГц	5

Порядок керування приладом у режимі детектора інфрачервоних випромінювань.

Підключити інфрачервоний датчик до сполучного кабелю, а сам кабель - до рознімання "PROBES".

Включити живлення приладу.

Установка "нульового" порога детектора здійснюється при включенні автоматично. Якщо буде потреба, натисканням кнопок " " або " " і встановити поріг детектора вручну, керуючись показаннями додаткової шкали "min - - -|- - -max". Якщо буде потрібно, натисканням кнопки " " повернутися до автоматичної установки порога.

Візуально по кількості повністю пофарбованих елементів 21-сегментної шкали й "на слух" по частоті щигликів в убудованому гучномовці або головних телефонах оцінити рівень прийнятого інфрачервоного випромінювання.

Натиснути кнопку "RUN/STOP" і зупинити (при необхідності) динамічні виміри рівня інфрачервоного випромінювання. Повторним натисканням цієї кнопки відновити динамічні виміри.

Натиснути кнопку "ENTER" (переклад звукової індикації в режим "AUD"), прослухати наявність і зміст потенційно небезпечних модульованих інфрачервоних радіовипромінювань.

Натиснути кнопку "MUTE" і наступними натисканнями кнопок "+" і "-" установити необхідну гучність виведеного або на убудований гучномовець, або на головні телефони звукового сигналу (тонального або демодульованого).

Натиснути кнопку "OSC" і перейти (при необхідності) до осцилографічного контролю параметрів демодульованого сигналу.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра демодульованого сигналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Режим детектора низькочастотних магнітних полів

У цьому режимі прилад забезпечує прийом на зовнішню магнітну антену й відображення параметрів сигналів від джерел низькочастотних електромагнітних полів з переважної, (наявної) магнітної складового поля в діапазоні від 300 до 5000Гц.

Класифікація сигналів і їхніх джерел здійснюється на основі аналізу автоматично виведеної не екран дисплея осцилограми, що відображає форму прийнятого сигналу й поточне значення його амплітуди. Підвищення вірогідності класифікації сигналів і їхніх джерел забезпечується можливістю одночасного з аналізом зображення на екрані дисплея, прослуховування "фонової" обстановки з використанням убудованого гучномовця або головних телефонів.

Для роботи в умовах складної завадової обстановки передбачений так званий диференціальний режим антени, що вводять у дію перемикачем на її корпусі.

Технічні характеристики	
Діапазон частот, кГц	0. 3-10
Гранична чутливість, А/(м х Гц^2)	10(-5)

Порядок керування приладом у режимі детектора низькочастотних магнітних полів.

Підключити зовнішню магнітну антену до сполучного кабелю, а сам кабель - до рознімання "PROBES".

Включити живлення приладу. Осцилографічний контроль параметрів прийнятого по магнітному полю сигналу включається автоматично.

Візуально по амплітуді й характеру сигналу на осцилограмі й "на слух" по його тональності в убудованому гучномовці або головних телефонах оцінити рівень магнітного

поля й присутність фона електромережі 220Vx50Hz або її гармонік. При необхідності (у випадку високого рівня фону електромережі) включити диференціальний режим антени перемикачем на її корпусі (положення "до білої крапки").

Нажати кнопку "RUN/STOP" і зупинити (при необхідності) динамічні виміри. Повторним натисканням цієї кнопки відновити вивід на екран динамічне змінення осцилограми.

Натиснути кнопку "MUTE" і наступними натисканнями кнопок "+" і "-" установити необхідну гучність сигналу, виведеного або на убудований гучномовець, або на головні телефони.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра прийнятого сигналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Режим віброакустичного приймача

У цьому режимі прилад забезпечує прийом від зовнішнього віброакустичного датчика й відображення параметрів низькочастотних сигналів у діапазоні від 300 до 6000Гц.

Стан віброакустичного захисту приміщень оцінюється як кількісно, так і якісно.

Кількісна оцінка стану захисту здійснюється на основі аналізу автоматично виведеної на екран дисплея осцилограми, що відображає форму прийнятого сигналу й поточне значення його амплітуди.

Якісна оцінка стану захисту заснована на безпосереднім прослуховуванні прийнятого низькочастотного сигналу й аналізі його гучності й тембрових характеристик. Для цього використається або убудований гучномовець, або головні телефони.

Технічні характеристики	
Чутливість, В х сек^2/м	1
Власний шум у смузі 300Гц-3000Гц, мкв	50

Порядок керування приладом у режимі віброакустичного приймача.

Підключити зовнішній віброакустичний датчик до рознімання "PROBES".

Включити живлення приладу.

Осцилографічний контроль параметрів прийнятого по віброакустичному каналу сигналу включається автоматично.

Візуально по амплітуді й характеру сигналу на осцилограмі й "на слух" по його розбірливості і якості в убудованому гучномовці або головних телефонах оцінити рівень і темброві характеристики перетвореного звукового сигналу.

Натиснути кнопку "RUN/STOP" і зупинити (при необхідності) динамічні виміри. Повторним натисканням цієї кнопки відновити вивід на екран динамічне змінення осцилограми.

Натиснути кнопку "MUTE" і наступними натисканнями кнопок "+" і "-" установити необхідну гучність сигналу, виведеного або на убудований гучномовець, або на головні телефони.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра сигналу, прийнятого по віброакустичному каналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Режим акустичного приймача

У цьому режимі прилад забезпечує прийом на зовнішній мікрофон і відображення параметрів акустичних сигналів у діапазоні від 300 до 6000Гц.

Стан звукоізоляції приміщень і наявність у них уразливих, з погляду витоку інформації, місць визначається як кількісно, так і на якісно.

Кількісно оцінка стану звукоізоляції приміщень і виявлення можливих каналів витоку інформації здійснюються на основі аналізу автоматично виведеної на екран дисплея осцилограми, що відбиває форму прийнятого сигналу й поточне значення його амплітуди.

Якісна оцінка заснована на безпосереднім прослуховуванні прийнятого акустичного сигналу й аналізі його гучності й тембрових характеристик. Для цього використається або убудований гучномовець, або головні телефони.

Технічні характеристики	
Чутливість, мв/Па	>=5
Діапазон частот, Гц	300-6000

Порядок керування приладом у режимі акустичного приймача.

Підключити мікрофон до рознімання "PROBES".

Включити живлення приладу.

Осцилографічний контроль параметрів прийнятого акустичного сигналу включається автоматично.

Візуально по амплітуді й характеру сигналу на осцилограмі й "на слух" по його розбірливості і якості в убудованому гучномовці або головних телефонах оцінити рівень і темброві характеристики перетвореного звукового сигналу.

Натиснути кнопку "RUN/STOP" і зупинити (при необхідності) динамічні виміри. Повторним натисканням цієї кнопки відновити вивід на екран динамічне змінення осцилограми.

Натиснути кнопку "MUTE" і наступними натисканнями кнопок "+" і "-" установити необхідну гучність сигналу, виведеного або на убудований гучномовець, або на головні телефони.

Натиснути кнопку "SA" і перейти (при необхідності) до аналізу спектра сигналу, прийнятого по акустичному каналу.

У випадку збоїв у роботі натиснути кнопку "RESET" і здійснити знову запуск приладу.

Порядок керування підсвічуванням екрана рідкокристалічного дисплея.

Включити живлення приладу в будь-якому необхідному режимі роботи.

Натиснути кнопку "HELP", потім кнопку "MUTE".

Кнопками "+" і "-" установити необхідну яскравість підсвічування екрана дисплея. Натисканням кнопки "HELP" зняти із кнопок "+" і "-" функції керування яскравістю підсвічування й повернути на екран дисплея "картинку", що відповідає вихідної індикації активізованого режиму.

Універсальний пошуковий прилад D 008

Рис. 4. 22 Універсальний пошуковий прилад D 008

Універсальний пошуковий прилад D 008 призначений для оперативного виявлення пристроїв промислового шпигунства.

Даний прилад є кінцевим елементом пошуку подібних пристроїв і дозволяє в конкретній обстановці виявити й локалізувати потай установлені ПУ.

D 008 включає два канали виявлення:

- радіодетектор (РД), призначений для пошуку радіо передавальних пристроїв.

- аналізатор провідних ліній (АПЛ), призначений для пошуку ПУ, що використають для передачі інформації провідні лінії (380/220В, телефонні, сигналізації)

Атенюатор дозволяє проводити виміру в умовах складної електромагнітної обстановки, властивим великим промисловим центрам, за рахунок ослаблення вхідного сигналу. Даний режим корисний і для локалізації потужних ПУ.

Активна антена полегшує виявлення ПУ із частотою передачі вище 400 Мгц.

Наявність системи акустичного зворотного зв'язку (АЗЗ) дозволяє виключити помилкові спрацьовування детектора на локальні електромагнітні поля й ідентифікувати ті що знаходяться в приміщенні ПУ за характерним звуковим сигналом

Технічні характеристики	
Живлення, В	9
Споживаний струм, ма: - черговий режим РД - черговий режим АПЛ - робочий режим	 20 30 до 100
Габарити, мм	148x68x24
Діапазон частот РД, МГц	50 - 1500
Чутливість по входу,мв: - F=100 МГц - F=400 МГц - F=800 МГц - F=1400 МГц	 2 2 1,5 6
Ослаблення атенюатора, дБ	20
Діапазон частот активної антени, МГц	400-1500
Посилення активної антени не менш, дБ	7
Динамічний діапазон індикатора, дБ	20
Смуга пропущення, кГц	200
Вид модуляції	АМ, ЧМ
Максимальна вхідна напруга адаптера, В	500

Універсальний прилад для виявлення засобів негласного знімання інформації

СРМ-700

Рис. 4. 23 Прилад СРМ-700

Застосовується для виявлення й локалізації засобів негласного знімання конфіденційної інформації, що використають для передачі інформації радіоканал (інфрачервоний, акустичний канал - при наявності додаткових зондів) або провідні лінії, включаючи телефонні й силові (до 300 В).

Являє собою широкосмуговий високочутливий приймач. Застосування додаткових зондів дозволяє використати прилад для рішення самого широкого кола завдань по виявленню різних пристроїв, що підслуховують, і пристроїв дистанційного керування. Чутливий підсилювач на додатковому вході дозволяє контролювати будь-який електронний пристрій і провідні лінії на витік інформації й наявність сигналів.

Функція "моніторингу" дозволяє використати прилад у стаціонарному режимі для безперервного цілодобового контролю приміщення на появу нового пристрою, що підслуховує.

Для реєстрації сигналів, що надходять із зондів, може використатися будь-який магнітофон, що має вхід дистанційного керування (Remote).

Технічні характеристики

РЧ-зонд	
Діапазон частот	
номінальне значення 20 дБ	номінальне значення 20 дБ
Чутливість	62 дБ щодо рівня 1 мвт

Максимальний рівень вхідного сигналу	+15 дБ відносно 1 мвт; 50В постійної напруги
ОНЧ-зонд	
Діапазон частот	15 кгц ... 1 МГц
номінальне значення 20 дБ	номінальне значення 20 дБ
Чутливість	38 дБ щодо рівня 1 мвт
Максимальний рівень вхідного сигналу	+15 дБ відносно 1 мвт; 300 В постійної напруги
Напруга пробою	1500 В при 60 Гц
Звуковий підсилювач	
Вхід	50 кОм симетричний
Діапазон вхідних сигналів	1,7 мкв ... 10 В (135 дБ)
Вихід на навушники	розмах сигналу 5 В, 220 Ом
Вихід на магнітофон	розмах сигналу 25 мв із АРП
Дисплей	18-сегментний рідкокристаличний
Монітор	
Діапазон настроювання граничної чутливості	18 сегментів
Сигнал тривоги	звуковий 2,8 кГц або світлодіод, що мигає із частотою 2 Гц
Вихід дистанційного керування пристроєм замикаючий контакт	300 ма, 25 В
Мережний адаптер/зарядний пристрій	
Вхід	95... 130 В або 200 ... 275 В змінної напруги 50...60 Гц
Вихід	12 В постійної напруги, 500 ма

Живлення	Alkaline-батареї, мережний адаптер або NiCd акумулятор
Час зарядки NiCd акумулятора	8...10 годин
Час зарядки NiCd акумулятора	8...10 годин
Час зарядки NiCd акумулятора	8...10 годин

Таблиця 5.18

Основні характеристики багато функціональних пошукових приладів

Модель	Види модуляції	Діапазон частот, МГц	Живлення, В	Додаткові можливості
ПСЧ-5	AM/FM AF	0,020...10; (0,2...7)×10^{-3}	6	Чутливість: 30; 50 мкВ
«Піранья»	—	Аналізатора: 0,01...15; частотоміра: 30...2500; детектора магнітного поля: (0,3...5)×10^{-3}; віброакустичного приймача: (0,3...5) ×10^{-3}; акустичного приймача: (0,3...6) ×10^{-3}	—	ST031 дозволяє обробляти низькочастотні сигнали, що надходять, у режимі осцилографа чи спек-троаналізатора з індикацією чисельних параметрів
OSCOR-500	NFM, WFM,FM	0,01...3000	12, 110, 220	Доповнення OTL-5000 методом трьохточечної просторової локації дозволяє локалізувати місцезнаходження радіомікрофонів
СМР-500	AM	2×10^{-4}...3000	12; 220	Індикація: візуальна і звукова

Перехід приладу в кожній з режимів здійснюється автоматично при підключенні відповідного перетворювача, що входить у комплект. Прилад керується за допомогою шестнадцятикнопочної плівкової клавіатури.

Прилад дозволяє обробляти низькочастотні сигнали, що надходять, у режимі осцилографа або спектроаналізатора з індикацією чисельних параметрів.

Широкодіапазонний спектральний корелятор OSCOR-500 призначений для виявлення технічних засобів несанкціонованого одержання інформації, реалізує принцип порівняння сигналів, прийнятих у будь-якому діапазоні частот, з акустичною інформацією приміщення або з еталонним акустичним сигналом і обчислення кореляційної функції для оцінки ступеня погрози При цьому отримана інформація може бути виведена на вбудований друкувальний пристрій (плотер) і записана в пам'ять для подальшого аналізу користувачем (рис. 5.14).

Автоматичний режим дозволяє проводити перевірку будь-якого набору попередньо запрограмованих під діапазонів, що найбільш ефективно у випадках безупинного контролю протягом тривалого часу, або для попередньої оцінки електромагнітної обстановки.

Ручний режим передбачає можливість детального аналізу будь-якого зареєстрованого сигналу.

Модифікація OSCOR-500video дозволяє виявляти наявність систем відеоспостереження, що працюють по радіоканалу, і переглядати зображення на вбудованих моніторах у системах PAL, SECAM, NTSC.

Модифікація De Luxe-1 містить у собі OSCOR-500video, доповнений OTL-500, різними адаптерами для підключення до провідних комунікацій і диктофонів для реєстрації звукової інформації.

OSCOR-500 дозволяє для зменшення часу сканування запам'ятовувати в звичайному варіанті 7000 відомих частот («дружніх сигналів»), а для роботи в складній електромагнітній обстановці (умови великого промислового міста) передбачене функціональне доповнення OEM-5000, що дозволяє запам'ятати до 28672 відомих частот.

Універсальний пошуковий прилад CMP-700 призначений для оперативного виявлення і визначення місцезнаходження електронних пристроїв знімання інформації. Висока чутливість і автоматичне регулювання посилення, а також наявність входів і комплектація різноманітними датчиками-зондами перетворює прилад у багатофункціональний пристрій. Передбачено можливість використання CMP-700 у стаціонарному варіанті для контролю приміщень чи ліній зв'язку (рис. 5.15).

Аксесуари: інфрачервоний зонд, електромагнітний зонд, зонд-I стетоскоп, телефонний адаптер, адаптер для запису, адаптер до прикурника 12 В, кадмієво-нікелеві акумулятори, інфрачервоний тестовий передавач, мережний тестовий передавач, тестовий радіопередавач.

Багатофункціональний модуль захисту телефонної лінії SEL SP-17/D є технічним засобом активного захисту інформації і забезпечує мікропроцесорний контроль підключень до телефонної лінії (від абонента до АТС) з інформуванням користувача і гарантовано придушує підслуховування з використанням телефонних передавачів будь-якого типу і

потужності, пристроїв знімання інформації безконтактного типу (індуктивних і ємнісних) і заснованих на мікрофонному ефекті і ВЧ - нав'язуванні, засобів магнітного запису і паралельних телефонних апаратів.

Відмінні риси: повна автоматизація виявлення і придушення пристроїв, що підслуховують (для реалізації цих особливостей використовується вбудований мікропроцесор).

Допускається дистанційне керування модулем тональним сигналом DTMF з телефону, що захищається.

«Сторожовий режим» — постійний контроль підключення до телефонної лінії пристроїв, що підслухують, з оповіщенням про це користувача звуковим (у тому числі у слухавку) і світловим сигналами [3].

Прилад комплексного захисту телефонних переговорів KZOT-06 призначений для виявлення і придушення (блокування) роботи пристроїв несанкціонованого знімання інформації з телефонних ліній. Факт прослуховування телефонної розмови визначається за допомогою системи цифрового сканування. Пристрій містить у собі блок придушення, що під час його активації цілком виводить пристрої знімання інформації з робочого стану. Спеціальна схема не дозволяє прослухувати телефонну розмову паралельно включеним ТА. KZOT-06 має спеціальний фільтр від ВЧ- нав'язування.

Технічні характеристики: напруга живлення 9 В, струм споживання не більше 40 мА, режим індикації світловий, габаритні розміри 120х120х30 мм.

5.6 Випалювачі телефонних заставних пристроїв

Випалювачі телефонних закладних пристроїв призначені для запобігання прослуховування абонентських телефонних ліній пристроями несанкціонованого доступу, встановленими в телефонні лінії паралельним чи послідовним способом, шляхом їхнього електричного знищення (рис. 5.16). У табл. 5.19 наведені основні характеристики випалювачів телефонних закладних пристроїв [13].

Таблиця 5.19

Основні характеристики випалювачів телефонних закладних пристроїв

Модель	Час безупинної роботи, с, у режимі		Живлення, В	Напруга на виході, В	Габаритні розміри, мм	Виконання і додаткові можливості
	Автоматичному	Ручному				
BUG-ROASTER	600	-	220	1500	60x155x198	Зачищення в зоні до 200 м
«Кобра»	600	20	220	≥1600	65x170x185	Пропалювання паралельно і послідовно підключених пристроїв
КС-1300	1440	-	220	≥1500	170x180x170	Знищення пристроїв, що використовують радіоканал-
ПТЛ-1500	600	-	220	≥1500	65x170x185	-

5.7. Виявлювачі та придушувачі диктофонів і ВЧ електронних пристроїв

У сучасній практиці ділового спілкування дуже часто застосовуються малогабаритні диктофони — зручні у використанні й ефективні. Якість запису мови сучасними диктофонами дозволяє з високою імовірністю визначати співрозмовника за його голосом і, тим більше, зміст розмови при відтворенні.

Наведена на рис. 5.17 структурна схема не залежить від типу носія запису. В даний час на ринку з'явилися моделі, що використовують у якості носія магнітооптичні диски і мікросхеми пам'яті, але канал попередньої обробки сигналу залишається без зміни.

Мовний сигнал при розмові характеризується зміною рівня звукового тиску від 30 до 50 дБ, причому рівень приголосних звуків на 20 дБ нижче, ніж рівень голосних. З урахуванням можливого переміщення осіб, що розмовляють, рівень сигналів, що реєструються у фіксованій точці, змінюється більш ніж на 50 дБ. Тому виникає потреба у вирівнянні потужностей цих сигналів.

Слухові відчуття голосності майже пропорційні логарифму інтенсивності впливу, вухо практично не уловлює зміни рівня сигналу в межах 1 дБ. Слух має слабку чутливість до точності передачі фазових співвідношень окремих складових сигналів.

Постійна часу слуху складає в середньому при наростанні 20...30 мс. при спаді — 100...200 мс.

Спектральні і кореляційні характеристики мовного сигналу плавно змінюються в часі і залежать від типу звуків які вимовляються.

Рис. 5.17. Структурна схема сучасного пристрою звукозапису

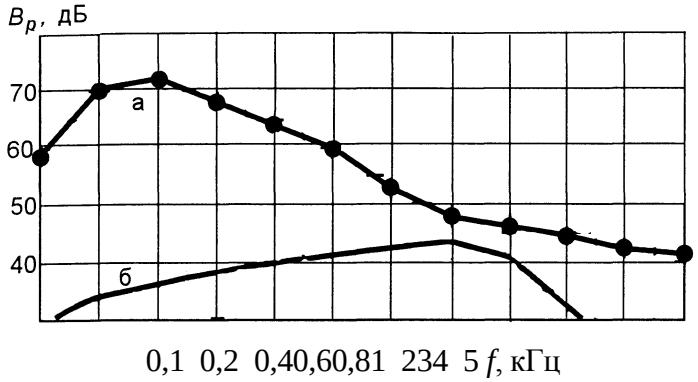


Рис. 5.18. Амплітудно-частотні характеристики: а — російської мови; б — чутливості мікрофона

Вокалізовані звуки, до яких відносяться голосні і частина приголосних (А, О, У, В), відрізняються значною нерівномірністю спектральної щільності потужності і концентрацією енергії в низькочастотній області, отже, високою кореляцією між прилеглими відліками сигналу. Невокалізовані звуки (З, Ж, Ш), навпаки, характеризуються більш рівномірним розподілом енергії за спектром і, відповідно, меншою кореляцією між відліками.

Усереднена крива спектру російської мови для чоловічих і жіночих голосів показана на рис. 5.18. верхньою лінією.

У будь-якому пристрої звукозапису акустичні коливання викликають коливання мембрани мікрофона, що формують електричний сигнал, амплітуда якого знаходиться в межах 0,05...10 мкВ. Нижня лінія на рис. 5.18. ілюструє амплітудно-частотну характеристику чутливості мікрофонів, застосовуваних при записі мови.

Для ефективного узгодження мікрофона і попереднього підсилювача, особливо при використанні виносного мікрофона, сигнал проходить через мікрофонний підсилювач (підсилювач струму), розташовуваний часто в одному корпусі з мікрофоном, і далі — через попередній підсилювач з регульованим коефіцієнтом підсилення. Його призначення полягає в тому, щоб стискати динамічний діапазон сигналів мікрофона до значення біля 30 дб, що доступний для запису на магнітну стрічку без істотних спотворень та забезпечити однаковий рівень сигналів у визначеній смузі частот[13].

Наявність системи АРП дозволяє досить якісно записувати мову співрозмовників, що знаходяться на відстані від десятків сантиметрів до десятка метрів від мікрофона. Система

АРП спрацьовує не миттєво - при збільшенні голосності розмови час зниження чутливості складає 1...3 с, а час підвищення чутливості 3...5 с. Завдяки наявності таких постійних часу забезпечується запис з мінімальним рівнем нелінійних спотворень мовного сигналу, тому що викиди його інтенсивності не встигають знизити коефіцієнт підсилення.

Розглянемо найбільш використовувані на сьогодні моделі переносних і стаціонарних виявлювачів диктофонів і ВЧ електронних пристроїв (рис. 5.19). Технічні характеристики розглянутих пристроїв зведені в табл. 5.20.

Таблиця 5.20

Основні характеристики виявлювачів диктофонів

Модель	Дальність виявлення диктофонів, м	Індикація	Габаритні розміри, мм; маса, кг	Додаткові можливості
RM-100	0,4...2	Світлова, беззвучна вібрація	60x100x22; 0,2	Виявляє будь-які диктофони зі стрічкопротягувальним механізмом і деякі види диктофонів із флеш-пам'яттю. Регулювання Чутливості ручне
TRD-800	-	Світлова, беззвучна вібрація	222x89; 0,17	Виявляє ВЧ- передавачі, магнітофони, відео/аудіо камери
PTRD-016	0,5..4,2	За радіоканалом на спеціальний приймач	датчика: 230x18x18; основного блока: 180x170x25	Підвищена завадостійкість. Базова модель приладу складається з основного блока та чотирьох датчиків. Чутливість датчиків 10^{-11} Тл. Споживана потужність 0,6 Вт
PTRD-018	0,5... 1,5	Світлова	550x350x165; 9,5...13,5	Виявляє ПЗП, визначає його місцезнаходження та час роботи з виводом поточної інформації на РК- дисплей або через інтерфейс RS-232 на екран монітора

Прочерк означає відсутність даних.

На додаток до даних табл. 5.20. варто згадати про принцип дії системи для виявлення диктофонів PTRD-018, що заснований на реєстрації електромагнітних полів, створюваних працюючим мотором ПЗП, послідовним опитуванням кожного каналу (датчика), і про такі технічні характеристики, як:

- час виявлення ПЗП — 20...30 с;
- кількість каналів (у залежності від варіанта постачання) — 4, 8, 16;
- швидкість відображення стану — 1,25 с;
- швидкість опитування одного каналу — 2...30 с,

- живлення — 220 В, 50 Гц;
- потужність споживання — не більш 8 Вт;

При протидії несанкціонованого звукозапису технічна задача полягає в тім, щоб забезпечити незастосовність результатів запису в тих цілях, з якими вона проводилася. При цьому часто не обов'язково руйнувати запис цілком, тому що зміст переговорів, відомий стороні співрозмовника, досить лише спотворити голоси, що говорять.

Фізичні принципи протидії несанкціонованого запису мови можна зрозуміти, проаналізувавши канали проникнення перешкод у тракти пристроїв запису мови, а це:

а) через мікрофон у мовній смузі частот;

6) через мікрофон у інфра- і ультразвуковій смугах частот;

в) наведення електромагнітного поля крізь корпус.

Найбільш простим і очевидним способом постановки перешкоди запису варто вважати акустичні перешкоди в тій же смузі частот, що й мова, і бажано з близькими кореляційними властивостями. На практиці це означає, що переговори, з погляду безпеки від запису, зручно вести там, де грає голосна музика, транслюється передача чи працює монітор (у ресторані, на вертольоті). При цьому через особливості слуху людина в стані селектувати голос співрозмовника, а мікрофон буде насамперед сприймати найбільш голосні звуки, викликаючи спрацьовування системи АРП і зниження коефіцієнта підсилення до значення, при якому шуми і перешкоди задавлять сигнал при наступному відтворенні. Цей спосіб особливо ефективний за умови, що співрозмовник не в змозі вплинути на вибір місця переговорів і підготуватися до них заздалегідь.

Іншим, можливим на перший погляд, способом протидії є постановка перешкоди, не сприйманої людським вухом у інфра- і ультразвуковий смугах частот. Однак унаслідок характеристик мікрофонів і підсилювачів сучасних диктофонів, що забезпечують спад сигналів у цих частинах спектра більш, ніж на 80 дБ, сформувати непомітно для співрозмовника такі коливання, потужності яких вистачило б для створення перешкоди, не представляються можливим, тому такі способи не одержали поширення.

Найбільш ефективним на сьогодні способом протидії несанкціонованого запису звуку є постановка перешкоди у виді імпульсного електромагнітного випромінювання. Переваги такого виду перешкод очевидна: скритність для оточуючих — випромінювання не сприймається людиною; ефективність впливу — перешкода щодо невеликої потужності в стані забезпечити повне придушення корисного сигналу; складність протидії — способи захисту апаратури досить громіздкі [13].

Практично відразу з початком появи імпульсних радіолокаційних систем, у яких частота посилок знаходилася в межах 0,2...1 кГц, персонал станцій і жителі міст стали

відзначати перешкоди для радіоприймальної і звуковідтворюючої апаратури, викликані роботою РЛС. Радіочастотна енергія великого рівня наводиться в монтажі, а потім детектується на найближчому нелінійному елементі. Граничні значення щільності потужності, при яких виявляється ефект випадкового детектування сигналів, що наводяться, у ланцюгах звукової частоти, 4-10...+20дБ відносно 1 мВт/м2, чи 1...10 мкВт/см2 [13].

Таблиця 5.21

Мінімальні значення енергії ушкодження для різних груп елементів

Групи елементів	Мінімальна енергія, мДж
Інтегральні аналогові мікросхеми	0,08...0,1
Інтегральні цифрові мікросхеми	0,012...0,5
Малопотужні транзистори	0,01
Потужні транзистори	0,02...0,1
Перемикаючі діоди	0,7...1

Механізм впливу цієї перешкоди на звукозаписну апаратуру полягає в тім, що імпульси електромагнітного випромінювання, частота повторення яких знаходиться в смузі частот мовного сигналу, наводять високочастотні струми на поверхні плат апарата запису звуку і детектуються на будь-якій нелінійності — у підсилювачах, стабілізаторах живлення, детекторі системи АРП. У результаті ці явища призводять до того, що система АРП знижує посилення сигналу мікрофона, а при збільшенні рівня детектованої перешкоди може зовсім припинити запис сигналу з мікрофона.

Спеціальні експерименти показали, що електромагнітне випромінювання великої потужності в стані викликати навіть необоротні зміни в структурі приладів (табл. 5.21.).

Відносно невелика енергія ушкодження інтегральних мікросхем і напівпровідникових приладів обумовлена малими розмірами напівпровідникових структур, а також особливими властивостями p-n-переходів. Ушкодження більшості напівпровідникових приладів безпосередньо зв'язані з тепловими процесами.

Для запобігання запису зовсім не обов'язково руйнувати диктофон співрозмовника. На практиці повне придушення звукового сигналу забезпечується вже при середній щільності потоку потужності в зоні друкованої плати диктофона, що перевищує 50 мкВт/см2. Для того щоб створити таку середню щільність потоку потужності на відстані 1,5 м від ізотропної антени, варто випромінювати потужність близько 14 Вт.

Частотний діапазон, у якому можуть працювати постановники перешкод, обмежений знизу, насамперед, габаритними розмірами передавальних антен і починається від 300 МГц. Відомо, що з ростом частоти габаритні розміри антен знижуються, з'являється можливість створення вузькоспрямованих випромінювачів, однак фактором, що обмежує верхню частоту системи постановки перешкод, є частотний діапазон детектуючих властивостей

елементів схеми апарата запису звуку. Для найбільш масових кремнієвих напівпровідникових структур верхня частота близько 450...500 МГц, а на більш високих частотах варто використовувати велику пікову потужність випромінювання при тій же середній щільності потоку потужності. Крім того, на частотах нижче 1000 МГц велика частина випромінюваної енергії НВЧ проходить через тіло. Поглинання складає менш 40 %, що дає можливість здійснювати придушення навіть через людське тіло. Реально працюючі зразки приладів володіють, крім того, спрямованою антеною з коефіцієнтом підсилення 3...5, що дозволяє обходитися набагато меншою середньою потужністю випромінювання 2...3 Вт. При цьому прилад стає переносним з гарантованою автономністю не менш 30 хв.

Рис. 5.20. Структурна схема імпульсного пристрою постановки перешкод

Якщо звукозаписний апарат оснащений металевим екраном, то щільність потоку потужності, що досягає друкованої плати, стає менше. Для збереження високих характеристик придушення навіть для металевих диктофонів використовують стаціонарні придушувачі, що працюють у діапазоні сантиметрових хвиль з піковими потужностями до 2 кВт. При цьому, завдяки дифракції на швах корпусів диктофонів, потужність сигналу, що проходить у корпус і детектованого елементами схеми, достатня для повного придушення сигналу мікрофона. На рис. 5.20. приведена структурна схема пристрою постановки перешкод.

Таблиця 5.22

Основні характеристики придушувачів диктофонів

Модель	Дальність придушення диктофонів, м, у корпусі		Споживана потужність, Вт	Час безупинної роботи, год	Габаритні розміри, мм; маса, кг	Додаткові можливості
	Металевому	Пластмасовому				
«Буран-3»	1,3	2,5	40	0,5	-	Поставляється в стаціонарному варіанті чи в кейсі
ППД-02	4	6	60	1,5	550х450х х110; 7	Обладнаний пультом дистанційного керування

R-2000	2	-	50	1	460x350x x120; 7	Протидія пристроям, що підслухують, забиваючи їхній мікрофон
«Шумо-трон-2»	1.5		100	від мережі: 4; від акуму-лятора: 1	500x400x x120; 11	Спотворює звук до невпізнанності
«Бастіон-1Д»	З виносним мікрофоном: 8; з неекранованим мікрофоном: 8; з екранованим мікрофоном: 4		-	1	10	Змонтовано в аташе-кейсі
«Рамзес-дубль»	1 антена: 2; 2 антени: 1,3		-	1	8	Провідне дистанційне керування. Зона придушення для кожної антени: кульовий сектор з кутом 30°

Прочерк означає відсутність даних.

У табл. 5.22. наведені технічні характеристики придушувачів диктофонів. На додаток до табл. 5.22. доцільно згадати про особливості принципу дії цих пристроїв. Наприклад, ППД «Буран-З» впливає на звукозаписну апаратуру вузькоспрямованим площинно-поляризованим випромінюванням. Площина поляризації хвилі випромінювання збігається з площиною максимального габариту приладу. Ефект від роботи приладу полягає у впливі імпульсного випромінювання на нелінійні елементи схем диктофонів. Шум, який генерується приладом, записується на магнітну стрічку.

Ефективність дії системи заснована на нанесенні тимчасового чи непоправного збитку елементній базі (мікросхемам, транзисторам, будь-яким магнітним носіям, мікрофонам і ін.) працюючих електронних приладів (спеціальних і побутових, у тому числі підключених до комунікацій мережі 220 В, 50 Гц, телефонної мережі й ін.).

Нанесення збитку відбувається в результаті наведення в елементній базі імпульсних струмів і напруг, що виникають під дією імпульсних НВЧ коливань, які генеруються приладом.

Безпечна для здоров'я тривалість проведення щоденних переговорів при роботі з одним пристроєм, що створює середню щільність потоку потужності в зоні диктофона, рівну 50 мкВт/см^2, складає не більш 4 год у день.

5.8 Системи віброакустичного зашумлення

Системи віброакустичного зашумлення призначені для запобігання прослуховування приміщення створенням шумової смуги звукових частот. У табл. 5.23. приведені основні характеристики систем віброакустичного захисту [13].

Крім даних, приведених у табл. 5.23., генератор віброакустичного шуму ANG-2000 . характеризується наступними параметрами: межі регулювання вихідної напруги — 0...14 В на навантаженні 6 Ом, мінімальний опір навантаження — 1 Ом, опір одного випромінювача — 6 Ом.

Варто згадати про відмінні риси деяких систем, приведених у табл. 5.23.

Для **чотирьохканальної системи віброакустичнго шуму SEL SP-51/A** - це наявність керованих мікропроцесором двох незалежних формувачів цифрового шуму з 40-хвилинною тривалістю його кореляції, що виключає можливість очищення апаратно-програмними методами, у тому числі, систем з опорним каналом [13].

Технічні характеристики вібраційного випромінювача SP-51/AV:

- виконання герметичне;
- тип електромагнітний;
- габаритні розміри 51х22 мм.

Віброакустичний шумогенератор SI-3001 може формувати сигнал шумової перешкоди з автоматичним регулюванням рівня, що залежить від голосності переговорів у приміщенні, що захищається.

Іншою особливістю приладу є генерація мовноподібної перешкоди, що ефективно ускладнює відновлення й обробку інформації навіть у тому випадку, якщо рівень перешкоди не перевищує рівень мовного сигналу перехопленої інформації. Підключення джерела мовноподібної перешкоди (зовнішнього диктофона з попередньо записаною мовою) до приладу здійснюється через лінійний вхід. Це дозволяє зменшити рівень шумового сигналу, який підводиться до випромінювача (у порівнянні із шумовою перешкодою), що, у свою чергу, приводить до зменшення паразитного шуму в приміщенні.

Пристрій може працювати в одному з трьох режимів: «I», «2». Режим відповідає відключенню шумової перешкоди, дозволяє формувати на виходах каналів мовноподібну перешкоду. Режим «I» відповідає формуванню шумової перешкоди на виходах каналів. Режим «2» відповідає формуванню шумової перешкоди з автоматично регульованим рівнем, що залежить від гучності переговорів у приміщенні, що захищається.

У режимах «I» і «2» крім шумової перешкоди можливе формування комбінованої перешкоди, що є сумішшю шумової перешкоди з регульованим рівнем і мовноподібної перешкоди, яка подається на лінійний вхід приладу [3].

Особливістю **системи віброакустичного зашумлення VAG-6/6** є використання віброперетворювачів на основі п’єзокераміки, що володіють високою ефективністю при формуванні необхідного рівня вібраційних перешкод.

Трохи докладніше про **генератор віброакустичного шуму «Соната-Ав».** Він призначений для захисту приміщень від витоку інформації по акустичних і віброканалах, зокрема, цілеспрямовано розроблений для сеансового блокування пристроїв, що підслуховують, які неможливо виявити і(чи) знищити. Правильно встановлений і відрегульований генератор дозволяє нейтралізувати такі види підслуховування, як:

- безпосереднє підслуховування в умовах поганої звукоізоляції в приміщенні;
- застосування радіо- і провідних мікрофонів, встановлених у порожнинах стін, у надстельовому просторі, вентиляційних коробах і т.п.;
- застосування стетоскопів, установлених на стінах (стелях, підлогах), трубах водо-, тепло- і газопостачання і т.п.;
- застосування лазерних і мікрохвильових систем знімання аудіоінформації з вікон і елементів інтер'єра.

Таблиця 5.23

Основні характеристики систем віброакустичного зашумлення

Модель, марка	Диапазон частот, кГц	Число датчиків, що перемикаються, шт.		Радіус дії вібродатчиків, м	Живлення, В	Сертифікати. Додаткові функції
		Вібраційних	акустичних			
ANG-2000, REI	0,25... 5	незалежно від типу 18		-	Від адаптера мережі	Має рутливе регулювання та світлодіодну індикацію рівня шуму
SP-51/A	0,1...11	типа SP-51/AV: 2...8		не менш 20	220 чи 12	Захист від перевантаження Програмування параметрів роботи системи
VAG-6/6	-	6	6	-	-	Віброперетворювачі (на основі п’єзокераміки) високоефективні при формуванні потрібного рівня вібраційних завад
SI-3001	0,25...5	до 36	до 72	не менш 20	-	Можливе формування шумової завади, що подається на лінійний вхід прилада
«Барон»	0,15...15			-	220	Можливість беспровідного дистанційного вмикання комплекса

VNG-006DM	0,2...6,3	типа КВП-26...12		Стеновых 4±1; оконных 1,5±0,5	220	Позволяет «зашумлять» вентиляційні Канали та дверні тамбури
ФОН-В	0,25...5	Типа Фон-В1: 1; типа Фон-В2: 2		не більш 5	-	Сертифікат Гостехкомісії Росії для об'єктів 2 категорії
Шорох-1 Шорох-2	0,2...5	КВП-7: 16	КВП-2: 24	стеновых 6±1; оконных 1,5±0,5	-	Сертифікат Гостехкомісії Росії для об'єктів 1 категорії

Віброакустична загороджувальна завада, що створюється генератором «Соната-АВ», синтезована таким чином, щоб забезпечити максимальне маскування мовних сигналів при мінімальному рівні шуму, що заважає переговорам. Прилад має два виходa з незалежним програмуванням вигляду завади (вібро- або аудіо-) та регулюванням її рівня. Також передбачений вхід віддаленого провідного керування.

Віброзашумлення елементів приміщення, що захищається, забезпечується за допомогою вібро- та аудіовипромінювачів, що підключаються до відповідних виходів генератора. Вібровипромінювачі використовуються для зашумлення огороджувальних конструкцій (стін, стелі, підлоги, вікон, дверей, труб тепло-, водо- і газопостачання). Аудіовипромінювачі використовуються для зашумлення простору над стелею, вентиляційних каналів, дверних тамбурів та ін.

Оптимальна кількість вібро- та аудіовипромінювачів для кожного приміщення визначається такими факторами, як його конструкція, матеріали огороджувальних поверхонь, розташування приміщення, рівень шумового фону і т.ін. Крім того, досить істотними можуть бути обмеження, обумовлені жорсткими вимогами до збереження дизайна приміщення.

Для попередньої оцінки необхідної кількості вібровипромінювачів ВИ-45 потрібно виходити з наступних норм:

стіни — один випромінювач на кожні 3...5 м периметра для капітальної стіни за умови розташування випрмінювачів на рівні половини висоти приміщення;

стеля, підлога —один випромінювач на кожні 15...25 м^2;

вікна — один випромінювач на вікно (при розташуванні на віконний переплет);

двері — один випромінювач на дверь (при розташуванні над дверним проємом);

труби систем водо-, тепло- и газопостачання — один на кожну вертикаль (окрему трубу) вида комунікацій.

Необхідна кількість аудіовипромінювачів АИ-45 может бути визначена виходячи з наступних норм:

один — на кожний вентиляційний канал або дверний тамбур;

один — на кожні 8...12 м^2 простору над стелею або інших пустот.

Кількість вібровипромінювачів — по одному на кожне скло.

Основні технічні характеристики генератора віброакустичного шуму «Соната-АВ»

Число незалежних каналів 2

Максимальна кількість одночасно увімкнутих:

- вибровипромінювачів великої потужності (ВВ-45) 12 (6-4-6)
- аудіовипромінювачів (АВ-45) 16 (8+8)
- вибровипромінювачів малої потужності (ПВ-45) 24 (12+12)

Смуга частот вібро- та аудіозавади гарантованої інтенсивності 0,3...5 кГц

Перевищення вібро- та аудіозавади над рівнем мовного сигнала в каналі витоку інформації не менш 10 дБ

Наявність входа ДУ (інтерфейс) Є (НР-контакт)

Электроживлення 220/50 В/Гц

Умови експлуатації:

- температура навколишнього середовища 5...40 °С
- відносна вологість повітря 70% (при 25 ° С)

Тривалість неперервної роботи – без обмежень

Примітки.

1) Умови проведення вимірів: цегляна стіна товщиною 40 см; відстань від вібровипромінювача до вимірювального вібродатчика – 2 м; відстань від джерела мовного сигнала до вібродатчика – 1 м; вібровипромінювач та джерело мови розташовані з одного боку стіни, а вібродатчик – з протилежного.

2) Умови проведення вимірів: дерев’яна дверь товщиною 5 см у цегляній стіні; відстань від джерела мовного сигнала до вібродатчика – 1 м; аудіовипромінювач і мікрофон розташовані з протилежних боків двері (аудіовипромінювач знаходитьсь біля двері, а мікрофон – на відстані 1 м від неї).

Портативний пристрій для захисту телефонних каналів від несанкціонованого прослуховування "ЩИТ" ("REDOUT")

Рис. 4.27 пристрій "ЩИТ" ("REDOUT")

Пристрій призначений для захисту від прослуховування конфіденційної інформації, переданої по телефонному каналі. Для цього пристрій генерує в телефонну лінію потужний мово-схожий шумовий сигнал, що надійно маскує корисну мову. На відміну від більшості інших систем цього призначення РЕДУТ установлюється тільки на одному кінці телефонного каналу (наприклад, в офісі). Абонент, що передає конфіденційну інформацію, може користуватися будь-яким телефонним апаратом, не обладнаним якою-небудь системою захисту (наприклад, таксофоном). Принцип дії пристрою РЕДУТ заснований на тім, що йому відомий той шумовий сигнал, що він видає в телефонну лінію, і тому його можна видалити із суміші мова/шум, виділивши корисний сигнал. За межами пристрою в телефонній лінії присутня тільки суміш сигналів. Оскільки шумовий сигнал формується випадковим чином, видалити його неможливо навіть використовуючи інший екземпляр пристрою РЕДУТ. Пристрій має два режими роботи: нормальний і захищений. У нормальному режимі РЕДУТ не робить ніякого впливу на роботу телефонної лінії. Для включення захищеного режиму досить натиснути кнопку ON на передній панелі. Після цього абонент на іншому кінці лінії може передавати конфіденційну інформацію, що почує лише його співрозмовник. У захищеному режимі передача інформації відбувається в симплексному режимі: власник пристрою РЕДУТ може тільки слухати, а його співрозмовник, що користується звичайним апаратом - тільки говорити. Для відновлення дуплексного зв'язку необхідно виключити кнопку ON.

Технічні характеристики: Амплітуда шумового сигналу 1.6 V; Амплітуда корисного сигналу 0.8 V; Вихідний опір генератора шуму 660 Om; Період повторення квазівипадкового шумового сигналу - не менш 60 годин; Живлення 85-260 V, 50-440 Hz; Споживана потужність 20 W.

Генератор шуму ANG-2200

Рис. 4.28 Генератор шуму ANG-2200

DNG-2000 призначений для захисту від пристроїв, що підслухують, які не реєструються звичайними методами й створення вібро-акустичних перешкод з метою захисту від провідних і радіо- мікрофонів, вмонтованих у стіну, а також лазерних і мікрохвильових систем, що використають відбиття від вікон. Прилад захищає периметр приміщення шляхом наведення на конструкції білого нефільтруємого шуму. Ступінь захисту DNG-2000 вище ніж систем з гучномовцями. Вібровипромінювачі DNG-2000 здійснюють спрямоване покриття площі усередині периметра й мають набагато кращі характеристики, роблячи при цьому менше шуму в заданій області. Хоча усередині захищеної області може бути чутний деякий шум, підвищувати голос не прийдеться.

Спектр шуму, виробленого DNG-2000, має форму, що рівномірно покриває діапазон голосових частот. Кожний випромінювач має пристосування для кріплення на стіни, стелі, вікна й т.д. DNG-2000 має 2 незалежних виходи, до кожного з яких можуть бути підключені вібраційні або акустичні випромінювачі. Кожний канал має незалежний блок живлення. Крім того, генератор має додатковий вхід і індикатор рівня "ЗВОРОТНИЙ ЗВ'ЯЗОК", що дозволяє здійснювати калібрування рівня шуму. Для цього до генератора підключається спеціальний мікрофон (DNG-MIC) або вібродатчик (DNG-STET). Вони дозволяють виміряти реальний рівень шуму, що наводиться на поверхню

Рис. 4.29 Віброгенератори TRN-2000 та OMS-2000

- Вібровипромінювач TRN-2000. Використається для поширення звукових коливань у стінах, стелі, вікнах, перегородках і витяжках (ліворуч унизу).

- Акустичний випромінювач OMS-2000, використовується для зашумления приміщення зсередини (праворуч).

Технічні характеристики	
Діапазон частот	250 Гц- 5 кгц
Мінімальне навантаження	3 Ом
Електроживлення	220В
Габарити	
основного блоку	4.4 x 15 x 25.4 см
вібродатчика TRN-2000	10,2 x 3,8 см
акустодатчик OMS-2000	12,7 x 14,6 см
Вага	
основного блоку	2,2 кг
вибродатчка TRN-2000	907 г

Генератор шуму ANG-2000

Рис. 4.29 Віброгенератор ANG-2000

ANG-2000 спроектований для захисту від провідних мікрофонів, стетоскопів, мережних передавачів, лазерних/ІЧ віконних стетоскопів. Система звукового маскування зашумляє периметр приміщення й не заважає розмові усередині. Діапазон частот ANG-2000 збігається з діапазоном людської мови, завдяки чому прилад має максимальну ефективність.

Система зашумления складається з основного модуля (ANG-2000), а також наступних додаткових елементів:

- Вібровипромінювач TRN-2000. Використається для поширення звукових коливань у стінах, стелі, вікнах, перегородках і витяжках (ліворуч унизу).
- Акустичний випромінювач OMS-2000, використовується для зашумления приміщення зсередини (праворуч

Рис. 4.31 TRN-2000 та OMS-2000

Акустичний генератор білого шуму WNG-023

Призначений для захисту переговорів від прослуховування з використанням технічних засобів промислового шпигунства. Принцип дії моделі заснований на генерації так званого "білого шуму" в акустичному діапазоні частот, що унеможливлює прослуховування розмови після його передачі будь-якими типами передавальних систем. WNG-023 може використатися тільки в замкнутому просторі - у кімнаті, у салоні автомобіля й т.д.

Рис. 4.32 Акустичний генератор білого шуму WNG-023

Технічні характеристики	
Живлення	220 В/9 В
Споживаний струм	130 ма
Діапазон частот	100 – 12000 Гц
Вихідна потужність	1 Вт
Габарити	111x70x22 мм

ЛУНА" ПРИСТРІЙ АКУСТИЧНОГО ЗАХИСТУ

Рис. 4.33 Пристрій "Луна-2ДУ"

Виріб призначений для захисту конфіденційних переговорів шляхом формування спеціальної акустичної шумосхожої шумової перешкоди.

Виріб забезпечує захист конфіденційних переговорів від прослуховування всіма відомими способами добування акустичної інформації в приміщеннях.

Захист переговорів і приміщення від прослуховування здійснюється шляхом формування спеціальних шумових мовосхожих сигналів, що маскують.

Шумові сигнали, що маскують, формуються з мовних шляхом їхнього спеціального перетворення й багаторазового повторення.

Основними особливостями виробу є:

- відсутність шумових сигналів у паузах розмови;

- залежність рівня шумових сигналів від гучності розмови;

- зменшення впливу що заважає та дратує людину, у порівнянні з білим або "пофарбованим" шумом (енергетичний виграш 8-10дБ у порівнянні з білим шумом і 6-8дБ із пофарбованим);

- рішення завдань, покладених на системи віброзахсту; - неможливість відновлення інформації сучасними методами, внаслідок збігу спектра й динаміки сигналу й перешкоди.

Електроживлення виробу здійснюється від мережі 220В.

Базовий комплект: 2 активні акустичні колонки з убудованим блоком обробки мовних сигналів, настільний мікрофон на підставці.

Комплект "Луна-2ДУ": використається для більших приміщень. Виріб являє собою два базових комплекти "Луна" із загальним каналом дистанційного керування, причому комплект N1 є провідної (номер нанесений на задній стінці активної колонки).

ПРИСТРІЙ АКУСТИЧНОГО ЗАХИСТУ "ЛУНА - КЕЙС"

Рис. 4.34 Пристрій "Луна - кейс"

Виріб призначений для захисту конфіденційних переговорів шляхом формування спеціальної акустичної мовосхожої шумової перешкоди.

Виріб є автономним пристроєм захисту інформації, виконаному в кейсі. Він забезпечує захист конфіденційних переговорів від прослуховування всіма відомими способами добування акустичної інформації в приміщеннях, на вулиці або в автомобілі.

Захист переговорів і приміщення від прослуховування здійснюється шляхом формування спеціальних шумових мовосхожих сигналів, що маскують.

Шумові сигнали, що маскують, формуються з мовних шляхом їхнього спеціального перетворення й багаторазового повторення.

Основними особливостями виробу є:

- відсутність шумових сигналів у паузах розмови;
- залежність рівня шумових сигналів від гучності розмови;
- зменшення впливу на людину що заважає й дратує (у порівнянні з білим шумом) ;
- рішення завдань, покладених на системи віброзахисту;
- неможливість відновлення інформації сучасними методами, внаслідок збігу спектра й динаміки сигналу й перешкоди.

Електроживлення виробу здійснюється від убудованих акумуляторів.

Тривалість безперервної роботи від одного комплекту акумуляторів не менш 3 годин.

Комплекс "Переговірна кімната" SR-4

Комплекс «Переговірна кімната» призначений для проведення закритих нарад у мобільному режимі. Комплекс забезпечує захист від всіх типів пристроїв, що підслухують. Головною відмінною рисою є мобільність, що дозволяє захищати переговори як у своїх приміщеннях так і в чужих переговірних кімнатах, обладнаних засобами зняття мовної інформації. Мобільність комплексу забезпечується відсутністю проводового зв'язка (наявністю закритих радіоканалів) між учасниками наради, автономним акумуляторним

живленням всіх абонентських комплектів, базового блоку, генераторів акустичних перешкод і самоорганізацією мереж, що дозволяє не займатися частотним плануванням.

Комплекс складається із чотирьох абонентських комплектів, базового блоку, зарядного пристрою й двох генераторів шумових перешкод.

Основні технічні характеристики

довжина хвилі радіозв'язку	15 см
швидкість передачі інформації	1115 кбіт/с
час для організації прямого й зворотного каналів	10 мс
вихідна середня потужність портативного пристрою	4..6 мвт
Вихідна середня потужність базового пристрою	30..40 мвт
радіус ведення переговорів	4..10 м
ємність акумуляторної батареї портативного пристрою	550 мАч
ємність акумуляторної батареї базового пристрою	1600 мАч
Ємність акумуляторної батареї генератора шуму	1600 мАч
струм споживання портативного пристрою	23 ма
струм споживання базового пристрою	240 ма
струм споживання генератора шуму	200 ма

Принцип дії комплексу полягає в наступному:

Учасники переговорів надягають переговірну гарнітуру, підключену до передавача абонентського комплекту. Передавачі підтримують метод множинного радіодоступу з динамічним вибором радіоканалу. Це дозволяє вести якісний радіозв'язок без втручання учасників переговорів. Цифровий широкополосный режим роботи передавачів і наявність секретного ключа аутоідентифікації роблять практично неможливим перехоплення й розшифровку інформації в даній системі зв'язку.

До базового блоку підключені дві колонки генераторів шумових перешкод. Шум формується тільки в тому випадку, якщо хтось із учасників переговорів говорить у мікрофон. Шумовий сигнал завади придушує всі типи акустичних пристроїв, що підслухують. У той же час переговірна гарнітура зменшує рівень шуму настільки, що можна без ускладнень розібрати суть бесіди.

Підготовка до роботи.

Попередньо необхідно зарядити базовий пристрій, портативні пристрої й генератори шуму. Для цього потрібно підключити штекер блоку живлення до гнізда для зарядки одного

із пристроїв. Після підключення нажати кнопку запуску на блоці живлення. При цьому займеться зелений індикатор на передній панелі блоку живлення. По закінченні заряду зелений індикатор згасне й займеться червоний. Далі можна відключити заряджений пристрій і підключити наступне. Одночасно від одного блоку живлення можна заряджати два пристрої.

Порядок включення.

Включити базовий блок. Потім включити по черзі всі портативні пристрої. При цьому кожний портативний пристрій згенерує характерний короткий звуковий сигнал, що свідчить про встановлення каналу зв'язку з базовим пристроєм.

Багатофункціональний генератор шуму Гром-Зи-4

Рис. 4.35 генератор шуму Гром-Зи-4

Призначення:

Для захисту переговорів від витоку інформації по телефонній лінії й електричній мережі. Прилад захищає ділянку лінії від телефонного апарата до автоматичної телефонної станції, а також блокує пристрої, що використають електричну мережу приміщення як канал витоку інформації. Принцип дії приладу заснований на маскуванні спектра мови широкосмуговим шумом.

Прилад запобігає прослуховування телефонного апарата пристроями, що працюють за принципом високочастотного нав'язування, а також реагуючими на підняття трубки телефонного апарата.

Генератор може працювати в автоматичному й неавтоматичному режимах. В автоматичному режимі контролює напругу лінії й включає захист при піднятті трубки телефонного апарата й зниженні напруги лінії у випадку підключення до неї паралельного телефону або пристрою, що підслухує.

Тіхничні характеристики

- Максимальне значення напруги, генерируемого приладом по телефонній лінії в діапазоні частот 6...40 кгц: не менш 3 В .

- Відношення напруги перешкод, які генеруються приладом по лінії, до напруги перешкод по клемах телефонного апарата: не менш 40 дб.
- Діапазон регулювання струму лінії: не менш 10 ма.
- Поріг включення приладу в автоматичному режимі: 55 + 3В.
- Напруга перешкод, яка генерується приладом по електромережі відносно 1 мкв:
  - у діапазоні частот 0,1...1 МГц: не менш 60 дБ;
  - у діапазоні частот 1...5 МГц: не менш 30 дБ.
- Час безперервної роботи приладу: 8 годин.
- Живлення: мережа 220 В, 50 Гц.
- Споживана потужність: 10 Вт.
- Маса: 1,5 кг.

Генератор шуму Волна-4Р

Пристрій призначений для активного захисту ПЕОМ від витоків оброблюваної інформації, викликаних високочастотними випромінюваннями, а також по ланцюгах електроживлення й заземлення.

Технічні характеристики:

- Потужність, споживана від мережі - 20 Вт.
- Потужність, яка комутується на зовнішнє навантаження - 300 Вт
- Розміри: 70 X 170 X 230 мм. Маса: 1500 г.

Мобільний генератор шуму MNG-300 Skeller

Рис. 4.36 Мобільний генератор шуму MNG-300 Skeller

Захищає від засобів знімання информації (мікрофони, радіомікрофони, цифрові й плівкові диктофони, стетоскопи), випромінюючи «білий» звуковий шум який не фільтрується. Завдяки використанню цифрових технологій генератор випромінює шум у такому діапазоні, що точно відповідає вхідному діапазону диктофонів і мікрофонів (250-4500 Гц). Тому Skeller створює ефективну перешкоду й заважає розмові значно менше на відміну від інших виробів даного типу. Корпус приладу виконаний із міцного матеріалу, що відповідає military-стандартам і розміщується в пачку сигарет Parliament. Кришка сигаретної пачки відкриває динамік для роботи. Skeller має регулятор гучності й індикатор рівня шуму. Рівень шуму настроюється відповідно до вимогам щодо комфорту й ступеня захисту.

5.9 Нелінійні радіолокатори

Однією з найбільш складних задач у галузі захисту інформації є пошук закладних пристроїв, які не використовують радіоканал для передавання інформації, а какож радіозакладок, що знаходяться у пасивному стані. Для таких пристроїв скануючі (панарамні) радіоприймачі, аналізатори спектру або детектори поля не є ефективними.

В зв'язку з цим, ця проблема й привела до появи зовсім нового виду пошукового приладу, який отримав назву нелінійного радіолокатора. своєю назвою він зобов'язаний фізичному принципу, який закладений в нього для виявлення підслуховуючих пристроїв.

Справа в тому, що всі ці пристрої мають в своїй основі напівпровідникові елементи (діоди, транзистори, мікросхеми), для яких характериний нелінійний вид вольт-амперної характеристики. Наявність такого нелінійного зв'язку призводить до появи на виході напівпровідникового приладу великої кількості гармонік з частотами $f_n = n \cdot f_0$, де $n = 1,2,3...$, а f_0 – частота зондуючого сигнала, який діє на вході напівпровідникового приладу.

Таким чином, нелінійний локатор – це пристрій, який реалізує такий принцип: випромінює електромагнітну хвилю з частотою f_0, а приймає перевипромінені сигналина частотах f_n. Якщо такі сигнали будуть виявлені, то в зоні дії локатора є напівпровілникові елементи, та їх необхідно перевірити на можливу належність до закладних пристроїв.

Таким чином, нелінійний локатор виявляє тільки електронну апаратуру та, на відмінність від класичного лінійного радіолокатора, «не бачить» відбиття від оточуючих предметів, тобто має високу вибірковість.

Джерелом завад для його роботи можуть слугувати контакти зі слабкими прижимами, для яких характерна наявність проміжного окисного шару. В рідких випадках небажаний ефект можуть дати паяні та зварні з'єднання.

Причина виникнення вказаних завад пов'язана з тим, що слабкі металічні контакти, як правило, являють собою квазілінійні елементи з нестійкими p-n переходами, які повэязані з наявністю окислів на поверхні металу.

Треба відзначити, що нелінійні локатори знайшли застосування і в «мирному» житті. Наприклад в системах контролю виносу речей з магазину «пошуку людей» у снігових завалах та зруйнованих будівлях, контроль багажу авіапасажирів та таке інше.

Серійний випуск локаторів розпочався у 1980 році в США (локатор Supercout), а в 1981 з'явився британський локатор Broom та радянський «Орхидея» (1982 рік).

Зараз на ринку представлена велика кількість нелінійних локаторів вартістю від 10 тис. грн. до 150 тис. грн.

До основних характеристик нелінійних локаторів відносять:

– значення робочих частот зондуючих сигналів;

– режим випромінювання та потужність передавача;

– форма, геометричні розміри та поляризація антени;

– точність визначення місця об’єкта перевипромінювання;

– чутливість радіоприймача;

– максимальна дальність дії;

– кількість гармонік, що аналізуються;

– розміри та вага.

Значення робочих чатот передавачів усіх типів локаторів знаходяться в межах від 400 до 1000 МГц (для приймачів ці показники відповідно вдвічі або втричі більші). Але, більшість пристрохв мають частоту близьку до 900 МГц.

Нажаль, більшість нелінійних радіолокаторів працюють на фіксованих частотах без можливості перестройки, а це погіршує їх екстплуатаційні характеристики. Взагалі, більш зручні в експлуатації локатори, які мають можливість перестройки в межах якогось діапазону. Наприклад, «Orion (MJE-400)» забезпечує автоматичний режим вибору робочої частоти в діапазоні 880÷1000 МГц. Її оптимальне значення визначається за найкращими умовами прийому для другої гармоніки частоти зондуючого сигналу.

Від робочої частоти залежить форма та геометричні розміри антени, важливою характеристикою яких є поляризація. Передавальні антени мають як правило, лінійну, а приймальні – колову поляризацію.

Точність визначення місця знаходження радіоелектронного пристроя складає декільки сантиметрів.

Режим роботи нелінійного локатора буває безперервним та імпульсним.

Потужність локаторів у безперервному режимі складає від 10 до 850 мВт і обмежена 3÷5 Вт, а в імпульсному режимі від 5 до 400 Вт з обмеженням в 400 Вт. Причина обмежень криється в тому, що локатори можуть створювати проблеми в плані електромагнітної сумісності із засобами зв’язку, навігації, телебачення, датчиками пожежної та охоронної сигналізації. крім того, зондуюче випромінювання меє негативний вплив на операторів, які експлуатують апаратуру.

Деякі сучасні нелінійні локатори мають можливість змінювати потужність зондуючого сигналу. Наприклад, локатор NJE-400 змінює потужність від 0.01 до 1 Вт.Чутливість приймачів сучасних нелінійних локаторів знаходиться в мажах $10^{-15} \div 10^{-11}$ Вт. У імпульсних вона дещо гірше. Більшість приймачів мають чутливість, яка регулюється в межах 30÷50 дБ.

Дальність дії більшості локаторів не перевищує 0.5 м.

Глибина виявлення об’єктів у маскуючому середовищі залежить від матеріалу, з якого виготовлені стіни та складає від декількох см до 0.5 м.

Кількість гармонік, які аналізуються одночасно є важливою характеристикою, яка характеризує переваги локаторів, що виявляють більше однієї гармоніки.

Сучасні нелінійні локатори мають невеликі розміри, вагу та дозволяють проацювати як від електромережі, так і від автономних джерел живлення.

Треба зазначити, що нелінійні локатори повністю не вирішують задачу виявлення закладок у приміщенні.

Питання для самоперевірки

1. Назвіть критерії за якими формується класифікатор засобів технічного захисту інформації.
2. Скільки класів засобів захисту інформкції вам відомо та охарактерезуйте їх.
3. Наведіть приклади (назву пристрою) типів пристроїв захисту інформації, які відносяться до четвертого, шостого та сьомого класу.
4. Які засоби захисту телефонних апаратів вам відомі?
5. Що таке аналізатор телефонних ліній?
6. Які марки аналізаторів ліній вам відомі?
7. Що таке індикатор поля?
8. В якому діапазоні працюють скануючі приймачі та яке їх призначення?
9. Що таке багатофункціональна пошукова система?
10. Які принципи покладено в основу роботи пристроїв визначення та придушення диктофонів?
11. За допомогою чого можна захиститись від прослуховування лазерними пристроями?
12. В чому різниця між лінійними та нелінійними радіолокаторами?

Розділ 6. Основи криптографії та шифрування.

6.1. Основні принципи криптографії

Одним з перших в історії документально – засвідченими прикладом шифрування є шифр Цезаря (I в. до н.е.), яким складався із заміни одних літер на відповідні їм інші літери у всьому тексті. Закон заміни був дуже простий. Під час шифрування повідомлення замість п'ятої літери латинського алфавіту ставилось друга, замість четвертої – перша, замість третьої – двадцять шоста і т.д. під час дешифрування зсув треба було роботи в прямому напрямку: замість першої літери брати четверту і т.д.

У сучасній термінології шифр Цезаря та його модифікації відносяться до одноалфавітних підстановок або одно алфавітних замін.

В протилежність розвитку криптографії стала поява криптоаналізу, який досить швидко знайшов слабкі місця у зазначених вище методах шифрування.

Значною модифікацією одноалфовітної заміни є шифр, який носить назву квадрату Полібія або тюремною азбукою. У ньому символи алфавіту розміщують в квадрат та замість букви в письмі записують пару чисел: номер строки та номер стовпця чарунки. У XVI сторіччя Д. Кардано винайшов новий тип шифра, заснований на дуже простій але надійній перестановці Літер повідомлення. Для шифрування Кардано запропонував використовувати квадрат з прорізаними в ньому декількаами чарунками. Чарунки прорізалися таким чином, щоб при повороті квадрата навколо свого центру на 90º , потім на 180º та 270º у отворах почергово з'являлись всі позиції первісного квадрата по одному разу При шифруванні квадрат покладають на аркуш для послання спочатку в первісному положенні та пишуть зліва направо зверху вниз першу порцію повідомлення Для дешифрування треба мати точну кожного того квадрата, яким користувався шифрувальник та повторити з нею ті самі повороти.

Цей пристрій досить зручний для зберігання та забезпечує гарну стійкість шифру. Так, маючи квадрат з прорізями розміром M*N для розшифровки треба перебрати варіанти. Наприклад, якщо N=6, то число переборів дорівнюватиме 262144.

Такі шифри, які не модифікують літери повідомлення, а тільки змінюють їх розташування, називають перестановочними.

Після Д.Кардано французьким дипломатом Віженером була запропонована модифікація шифру замін, яка одержала назву таблиця Віженера. Для шифрування за цією схемою потрібна таблиця з 26 латинських алфавітів, у кожному з яких за якимось законом змінено порядок букв та секретне слово-пароль, яке відоме тільки відправнику та одержувачу повідомлення. Такий шифр отримав назву багатоалфавітної заміни.

Подальшою модифікацією цього способу стало шифрування за книгою, коли відправник та одержувач повідомлення домовляються про однакову книгу одного й того ж видавництва. При шифруванні відправних вибирає в ній довільне місце та записує замість пароля який повторюється під первісним повідомленням у всю його довжину текст з книги, починаючи з того місця. Само кодування ведеться по тій же схемі, що й в схемі Віженера. Одержувач іншим каналам зв'язку отримає сторінки та слова в книжці. З якого почалася шифрування.

З XIX сторіччя криптографія перейшла на якісно інший рівень – почалася ера цифрової криптографії .

В 20-х роках XX сторіччя Г. Вернам запропонував автоматизувати шифрування телетайпних повідомлень за такою схемою. Інформація на телетайпі стрічці являє собою послідовність отворів та не пробитих ділянок , які відповідають "0" та "1". Вернам запропонував на передавальній стороні розмістити замкнену в кінце строчку з досить довгою послідовністю схожих "0" та "1", яка відіграє роль паролю . в момент передачі чергового імпульсу в канал зв'язку стрічка пароль, зсувається на одну позицію і з неї зчитується поточне двоічне значення. Якщо був зчитано "0", то первісний двоічний сигнал не змінювався, яка на стрічці паролі в цьому місці виявилась "1" то первісний сигнал інвертувався на приймальний стороні повинна бути присутня точно така ж стрічка і, притому у тому ж початковому положенні, що й у відправника.

Таким чином, тут вперше була застосована операція складання за модулем 2, яка стала базою у цифровій криптографії. Така операція має ще назву "виняткове ЧИ" і записується як " ˇ" або XOR (від англійського Exclusive OR). У відношенні складання за модулем 2 цікавий ще один факт – зворотний до нього, тобто відновлення. Операцією є окрім віднімання за модулем 2 ще й сама ця операція, тобто для яких X та Y виконується . І ця дуже зручна якість нерідко застосовується в різноманітних сучасних шифрах та схемах.

Іншим цікавим моментом виявилось те, що роблячи стрічку довжиною у довжину повідомлення можна зробити шифр абсолютно стійким.

Недоліком такої схеми є незручність зберігання великого паролю та його одноразовість.

6.2. Класифікація шифрів.

Першою принциповою ознакою, яка дозволяє провести класифікацію шифрів, є обсяг інформації, який невідомий третій стороні. Якщо зловмиснику повністю не відомий алгоритм виконаного над повідомленням перетворення. Шифр називають тайнописом. Тобто тайнопис є звичайним кодуванням інформації, або представленням її у іншому вигляді. При цьому третій стороні невідомий сам принцип кодування.

У свій час А.Кергофф висунув ідею про те, що розкриття самого алгоритму не повинно ні на крок наближати її до закритого повідомлення. Це повинно досягатися базуванням всього алгоритму шифрування на невеликому обсязі таємної інформації. Ця ідея лягла в основу всієї сучасної криптографії та отримала назву принцип Кергоффа.

У противагу тайнопису криптографією з ключем називають сьогодні алгоритми шифрування, в яких сам алгоритм перетворень широко відомий та доступний кожному, але шифрування виконується на основі невеликого обсягу інформації – ключа, який відомий тільки відправнику та одержувачу повідомлення. В сучасній криптографії розмір ключа складає від 56 до 4096 біт.

Всі криптоалгоритми з ключем поділяються на симетричні та асиметричні. У симетричних криптоалгоритмах ключі, які використовуються на передавальній та приймальній стороні повністю ідентичні. Такий ключ несе в собі всю інформацію щодо процесу утаємнення повідомлення і тому не повинен бути відомий нікому, окрім учасників переговорів. Тому тут часто застосовують термін таємний ключ. А самі системи називають шифрами на таємному ключі. Загальна схема процесу передачі повідомлення приведена на рис.6.1.

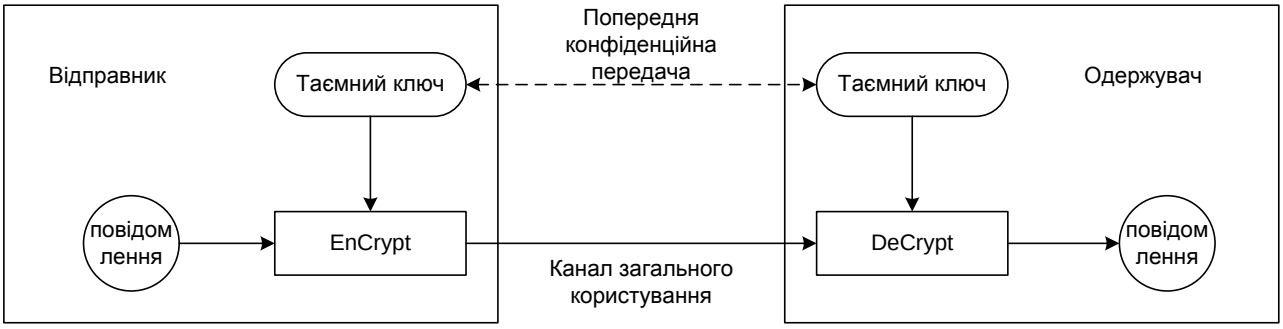


Рис. 6.1. Загальна схема процесу передачі повідомлення

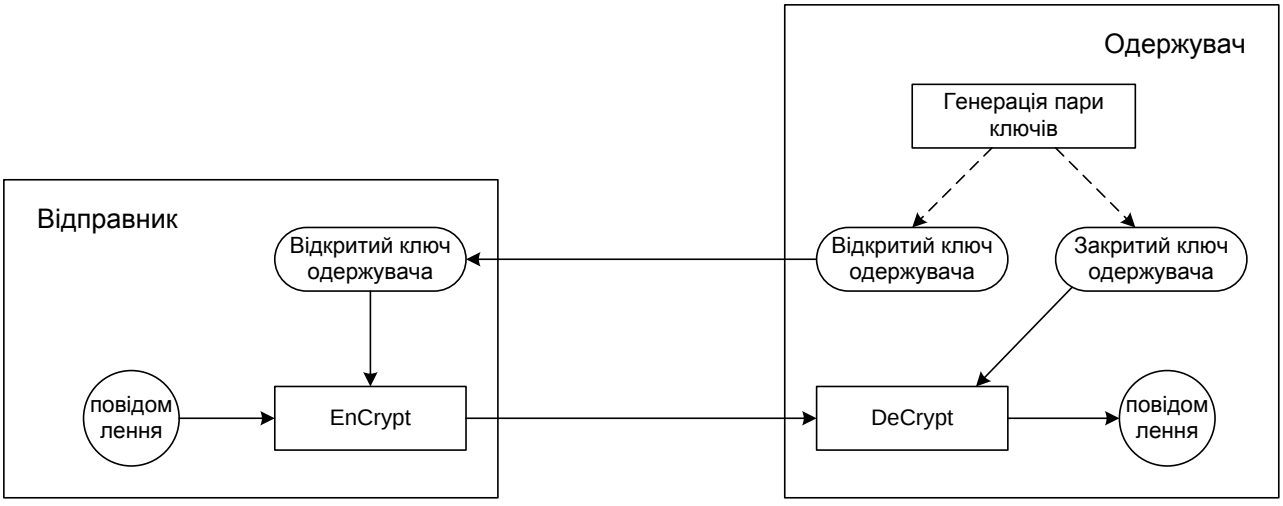


Рис. 6.2. Асиметричне шифрування

У асиметричному шифруванні (рис.6.2.) для шифрування повідомлення використовуються один ключ, а для дешифрування – інший. Таким чином, прочитати зашифрований текст можливо, тільки при наявності ключа дешифрування. Тому ключ шифрування може бути відомий всім користувачам мережі та носить назву відкритого ключа. А ключ дешифрування називають закритим. Самі ж асиметричні системи отримали назву шифру на відкритому ключі. Асиметричні шифри немає сенсу використовувати для захищеного зберігання документів. Їх призначення – захист повідомлень, електронна пошта, тощо.

Наступним критерієм класифікації шифрів є схема обробки ними потоку інформації.Згідно йому симетричні криптоалагоритми поділяються на: поточні та блочні шифри. Поточний шифр здатний обробляти інформацію побітно. Така схема дуже зручна в каналах послідовного зв'язку, де сам процес передачі інформації може обриватися в будь який момент а потім продовжуватся далі.

Така обробка інформації є досить повільною і тому, враховуючи можливості сучасних процесорів здійснювати паралельну обробку, застосовують інші принципи криптографічних перетворень, які носять назву блочних шифрів. Основним законом блочного шифрування є „або блок, або нічого". Тобто перетворення можуть здійснюватися тільки над інформацією строго визначеного обсягу. Розмір блоку на сьогоднішній день дорівнює 64, 128 або 256 бітам. Часткове шифрування (наприклад намагання обробити 177 біт) неможливе. Блочне шифрування отримало значно ширше розповсюдження завдяку розвитку обчислювальної техніки. Отже, якщо поточні шифри однаково часто реалізуються як програмно, так і апаратно, то блочні шифри в своїй більшості мають програмну реалізацію.

Теоретично можливо створення поточних асиметричних систем, але практичної цінності такі системи не будуть мати. Метою шифрування на відкритому ключі є конфіденційність деякого повідомлення, тому етап нагромадження в буфері та блочність тут має місце.

Загальна схема класифікації шифрів наведена на рис.6.3.

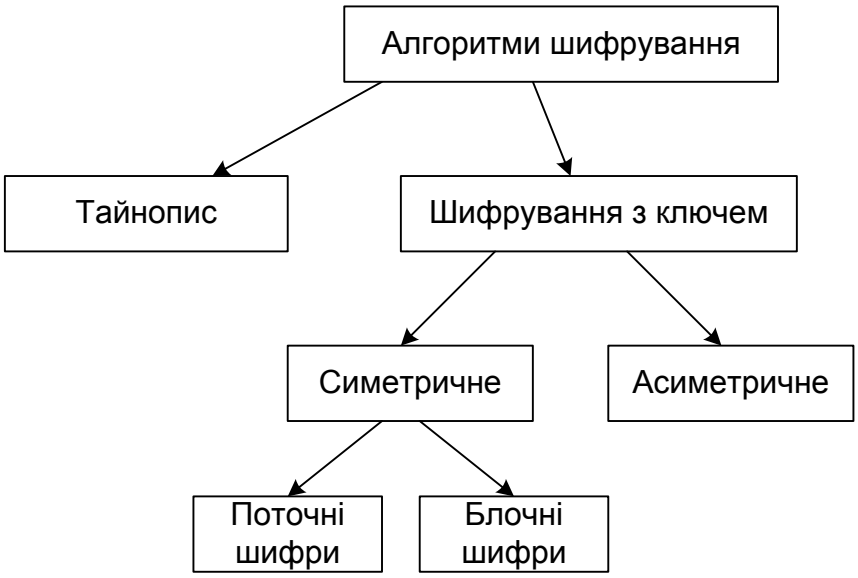


Рис. 6.3. Загальна схема класифікації шифрів

Як було зазначено вище, абсолютна стійкість шифру може бути досягнута тільки у випадку, коли розмір ключа дорівнює або перевищує розмір первісного повідомлення. Якщо ж розмір ключа менше за обсяг первісного повідомлення, тоді втрачається непередбаченість. Причина цього криється в надлишковості будь-якої національної мови. Будь яка людина може визначити з будь якого невеликого тексту, можливий (має зміст) чи ні він у рідній мові. Ключ вважається підібраним, якщо в результаті дешифрування в повідомленні визначилася частина, яка має сенс. Таким чином, будь-який шифр, довжина якого менше довжини повідомлення., яке передається, не є абсолютно стійким. Його можна завжди розкрити хоча б повним перебором всіх можливих ключів до появи фрази, яка має сенс. Тобто можна говорити тільки про практичну стійкість шифру.

Практично стійким називають шифр, до якого не можна застосувати будь які результативні методи атаки окрім повного перебору всіх можливих ключів.

Розглянемо основні види атак, яким повинен протистояти стійкий шифр.

Атака на основі шифротексту – це намагання зловмисника виявити або первісний текст, або ключ шифрування за допомогою досить великого обсягу зашифрованих даних.

Атака на основі відомого відкритого тексту – ситуація коли зловмисник знає і первісний і перетворений в процесі шифрування текст, та бажає дізнатися про ключ шифрування. Справа в тім, що зловмисник у 99% випадків знає яку-небудь додаткову інформацію про первісний текст. Тому стійкість шифрів до такої атаки, тобто невідтворність відносно ключа є такою ж важливою метою їх розробки, як і захист від першого типу атак.

Атака на основі вибраного відкритого тексту є модифікацією попередньої атаки у тому випадку, коли зловмисник знаходиться серед обслуговуючого персоналу системи та може нав’язати службі шифрування яку інформацію треба передати по криптоканалу.

Практично стійкий шифр повинен витримувати величезну кількість подібних намагань, не давши зловмиснику ніякої нової інформації про ключ шифрування.

Якщо протягом досить великого проміжку часу (десятки років) на якийсь шифр не знайдено жодного способу злому. То він вважається надійним шифром. Але, треба пам'ятати, що в будь який момент якийсь шифр може покинути сукупність надійних шифрів у зв'язку з відкриттям якоїсь нової математичної теореми або метода криптоаналіза. Наприклад, після доведення Д.Мессі та Е.Берлекампом теореми про те, що при перехваті $2 \times N$ біт шифруючої послідовності лінійного регістру зсуву завжди можна відновити його внутрішню структуру, лінійні регістри зсуву покинули клас надійних шифрів та застосовуються тільки як складові елементи більш складних криптоалгоритмів. До цих пір не існує теорії, яка дозволяє генерувати надійні на 100% практично стійкі шифри.

Отже. Будь який шифр можна відкрити простим перебором ключів. Все залежить від розміру ключа, який визначає кількість часу щоб перебрати всі варіанти. Так, якщо довжина ключа 32 біта (4 млрд. варіантів), то треба декілька днів (або тижнів) для його відкриття. Ключі довжиною 128 біт у сучасних надійних шифрах не можливо відкрити повним перебором на сучасних ЕОМ. Рекомендована довжина ключів для комерційних цілей 192 біта, а для державних 256 біт. Тобто зроблено запас на декілька десятків років, з урахуванням бурхливого розвитку сучасних ЕОМ.

6.3. Симетрична криптографія.

6.3.1. Поточні шифри.

Симетричні алгоритми почали розвиватися значно раніше асиметричних тому на цей час накопичилась значна кількість досліджень у цьому напрямку.

Характерною особливістю поточних шифрів є побітова обробка інформації. Тому шифрування та дешифрування в таких схемах може обриватися у довільний момент часу. Коли потік, що передається, а також відновлюватись у разі продовження передачі. Така обробка інформації може бути представлена у вигляді автомату, який на кожному своєму такті:

- генерує за якимось законом один біт шифруючої послідовності;
- якимось зворотнім перетворенням накладає на один біт відкритого потоку цей шифруючий біт та отримує зашифрований біт.

Пояснимо, чому шифруючи послідовність достатньо обмежити тільки одним бітом на біт первісного тексту. Справа в тім. Що в арифметиці за модулем 2. до яких відносяться будь які перетворення над бітами існує тільки дві оборотні операції: виняткове ЧИ (воно же додавання за модулем 2) та заперечення. Оборотною називають функцію, у якої, знаючи

результат та всі операнди, крім одного, можна відновити цей невідомий операнд Отже у процесі шифрування потоку можна застосовувати тільки оборотні операції .

Таким чином, як би багато не було створено шифруючих бітів на один біт первісного тексту, усі вони будуть накладатися на даний біт шляхом комбінації з операцій XOR та заперечення. Але заперечення можна вносити всередину операції XOR, тобто для будь яких a та b:

$NOT(a\ XOR\ b) = a\ XOR\ (NOT\ b)\ XOR\ b$.

Отже, якою б не була складною композиція з шифруючих біт та первісного, її завжди можна розділити, тобто представити у вигляді:

$p\ XOR\ F(g_1, g_2, g_3)$,

де p - первісний біт (від англ.. $plain$- відкритий), g - шифруючи біти, F - якась функція, яка містить в собі операції виняткове ЧИ та заперечення. Логічно зразу провести ці перетворення над проміжними бітами g_1 та отримати в результаті вся формула шифрування буде мати універсальний вигляд: $c = p\ XOR\ g$, де c - зашифрований біт (від англ. $ciphered$ - зашифрований).

Загальна схема шифрування поточним шифром наведена на рис.6.4.

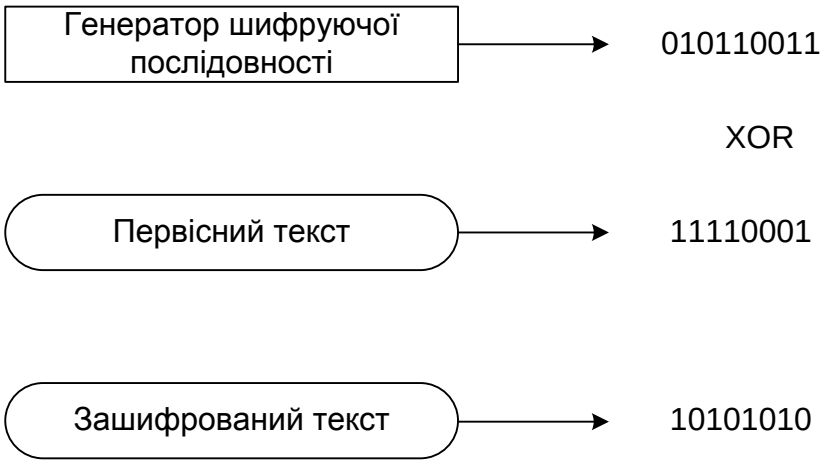


Рис. 6.4. Загальна схема шифрування поточним шифром.

Усі сучасні поточні шифри працюють за даною схемою. Біт шифрування, який з'являється на кожному новому кроку автомата, або цілий набір таких біт, прийнято позначати символом γ (гама), а самі поточні шифри отримали за це другу назву – шифри гамування. Ці шифри набагато швидкіші своїх найближчих конкурентів – блочних шифрів – у тому випадку, якщо поточне шифрування реалізується апаратно. У тому випадку, коли ці алгоритми реалізовано програмно, то їх швидкість мало відрізняється від блочних, а інколи й значно нижче.

Три основних компоненти, над якими обчислюється функція, яка породжує гаму, є:

- ключ;
- номер поточного кроку шифрування;
- найближчі від поточної позиції біти первісного і/або зашифрованого тексту.

Ключ є необхідною частиною гамую чого шифру. Якщо ключ і схема породження гами не є таємним. То поточний шифр перетворюється у звичайний перетворювач – кодер – скремблер (від англ. *scrumble* - перемішувати). Скремблери широко застосовуються у системах телекомунікацій для покращення статистичних характеристик сигналу, що передається. Частота появи „0” та „1” необхідна у багатьох системах синхронізації – за моментом зміни значення (фронту) сигналу з „0” на „1” або з „1” на „0” приймальна сторона коригує свої генератори синхроімпульсів. Часто у відношенні поточних шифрів за аналогією з подібними код ерами застосовується термін „скремблер”.

Залежність шифрую чого від номера поточної позиції, якщо така існує, частіше всього задається номером позиції до ключа чергового біта гами. Просто на кожному такті шифрування над матеріалом ключа та внутрішніми перемінними поточного шифру виконуються якісь однотипні перетворення, і за це кожний шифруючий біт фактично залежить від його положення (номеру) у загальному потоці гами.

Матриця залежності основних властивостей поточних шифрів від ідеології їх побудови наведена у табл.6.1.

Таблиця 6.1.

Властивості різних поточних шифрів.

	Гама залежить від біта первісного або зашифрованого тексту	Гама не залежить від біта первісного або зашифрованого тексту
Гама залежить від номера поточного тексту шифрування	(-) дешифратор втрачає синхронізацію при помилці „вставка/пропуск біта” в каналі зв’язку. (-) дешифратор розмножує помилки „спотвореного біта” в каналі зв’язку (+) схема стійка до атаки за відомим первісним текстом	(-) дешифратор втрачає синхронізацію при помилці „вставка/пропуск біта” в каналі зв’язку (+) дешифратор не розмножує помилки „спотворення біта” в каналі зв’язку (+) схема стійка до атак за відомим первісним текстом
Гама не залежить від номера поточного такту шифрування	(+) дешифратор не втрачає синхронізацію при помилці класу „вставка/пропуск біта” в каналі зв’язку (-) дешифратор розмножує помилки класу „спотворення біта” в каналі зв’язку (-) схема не стійка до атаки за відомим первісним текстом	

Таким чином, шифри, які залежать тільки від ключа та номера такту, шифрування (правий стовпець верхня строка в таблиці 6.1.) одержали найбільше розповсюдження у сучасній практиці.

Атаки на шифри гамування, не пов'язані з конкретною їх реалізацією, засновані у своїй більшості або на факті значного відхилення статистичних характеристик гами від дійсно випадкового потоку, або на повторному використанні деяких частин гами в процесі шифрування.

У першому випадку відхилення характеристик гами не може повноцінно приховати частотні характеристики первісного тексту, і з'являється можливість проведення різноманітних форм частотного та кореляційного криптоаналіза. У другому випадку повторне накладання на виняткове ЧИ тієї ж шифруючої послідовності g на новий первісний блок P_2 дозволяє зловмиснику на основі нехитрої формули:

$$(P_1 \; XOR \, g) \; XOR \, (P_2 \; XOR \, g) = P_1 \; XOR \, P_2$$

цілком позбутися від гамуючої послідовності. А це вже дає можливість при вдалому збігу обставин за допомогою спеціальних методів, включаючи підбір букв та статистичні дослідження, добути з $(P_1 \; XOR \, P_2)$ окремо P_1 та окремо P_2.

Ці методи криптоаналіза дозволяють сформувати два основних принципи шифрів гамування, які не залежать від їх конкретної структури:

- гама, яка породжується шифром, повинна мати дуже гарні стохастичні характеристики;
- період гами шифру повинен перевищувати довжину найбільшого з повідомлень, яке планується до пересилання за допомогою одного й того ж ключа.

Крім того, треба пам'ятати, що в каналах з можливостями модифікації даних шифри гамування повністю беззахисні перед фальсифікацією. У тому випадку, коли зловмисник знає побітне розташування даних у послідовності, що передається, інвертування будь-якого біта не можна бути розпізнано на приймальній стороні. Це приведе до інвертування відповідного біта в декодованому тексті повідомлення. Під час використання поточних шифрів у каналах такого роду необхідна ретельна реалізація системи підтвердження цілісності і повідомлення.

Найбільш простими схемами, які використовуються в якості базових при побудові інших, більш стійких поточних шифрів, є лінійні регістри зсуву – ЛРЗ (англ. *linear feedback shiftregisters – LFSR*). Їх побудова дуже проста: пристрій являє собою декілька $(20 \div 100)$ чарунок пам'яті, в кожній з яких може зберігатися один біт інформації. Сукупність біт, яка знаходиться в даний момент у ЛРЗ, називають його станом. Для виробітку чергового біту

шифруючої послідовності, тобто гами, ЛРЗ виконує один цикл перетворень, який носить назву такта, за таким алгоритмом:

- перший (скажемо, самий правий) біт із послідовності поступає на вхід ЛРЗ – це є черговий біт гами;
- вміст усіх проміжних чарунок пам'яті зсувається на одну позицію вправо;
- у пусту чарунку пам'яті, що з'явилася у результаті зсуву з лівого краю ЛРЗ, розміщують біт, який розраховується, як операція *XOR* над значеннями з чарунок ЛРЗ з заданими номерами.

Природно, напрямок зсуву не грає ніякої ролі, та можна було б сформулювати весь цей алгоритм зсувами „справа наліво". Схематично лінійний регістр зсуву зображено на рис.6.5.

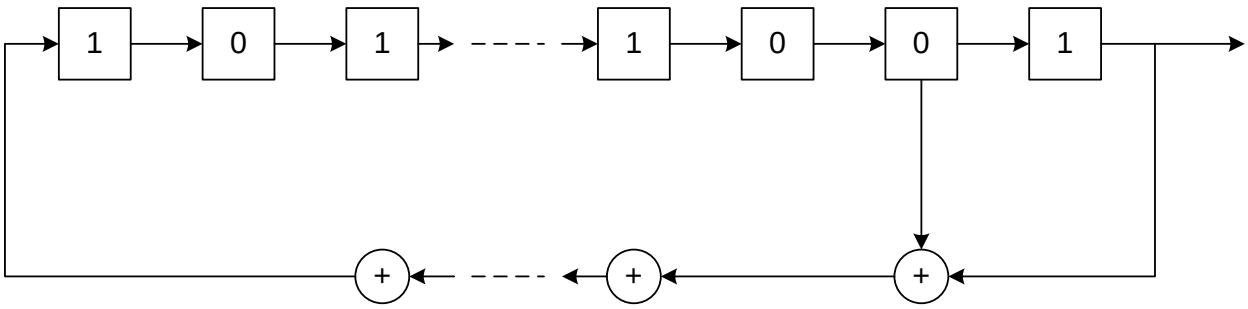


Рис. 6.5. Лінійний регістр зсуву

Кількість біт, які охоплені в ЛРЗ зворотнім зв'язком, називають його розрядністю. В разі використання в якості простого шифру перед початком процесу в чарунки пам'яті ЛРЗ розміщують побітно ключ. Як наслідок. Біт гами, який породжується на кожному такті, залежить від ключа і від номера даного такту в загальній процедурі шифрування. Приклад роботи ЛРЗ розрядності 3, з установкою ключа 011 показана на рис.6.6.

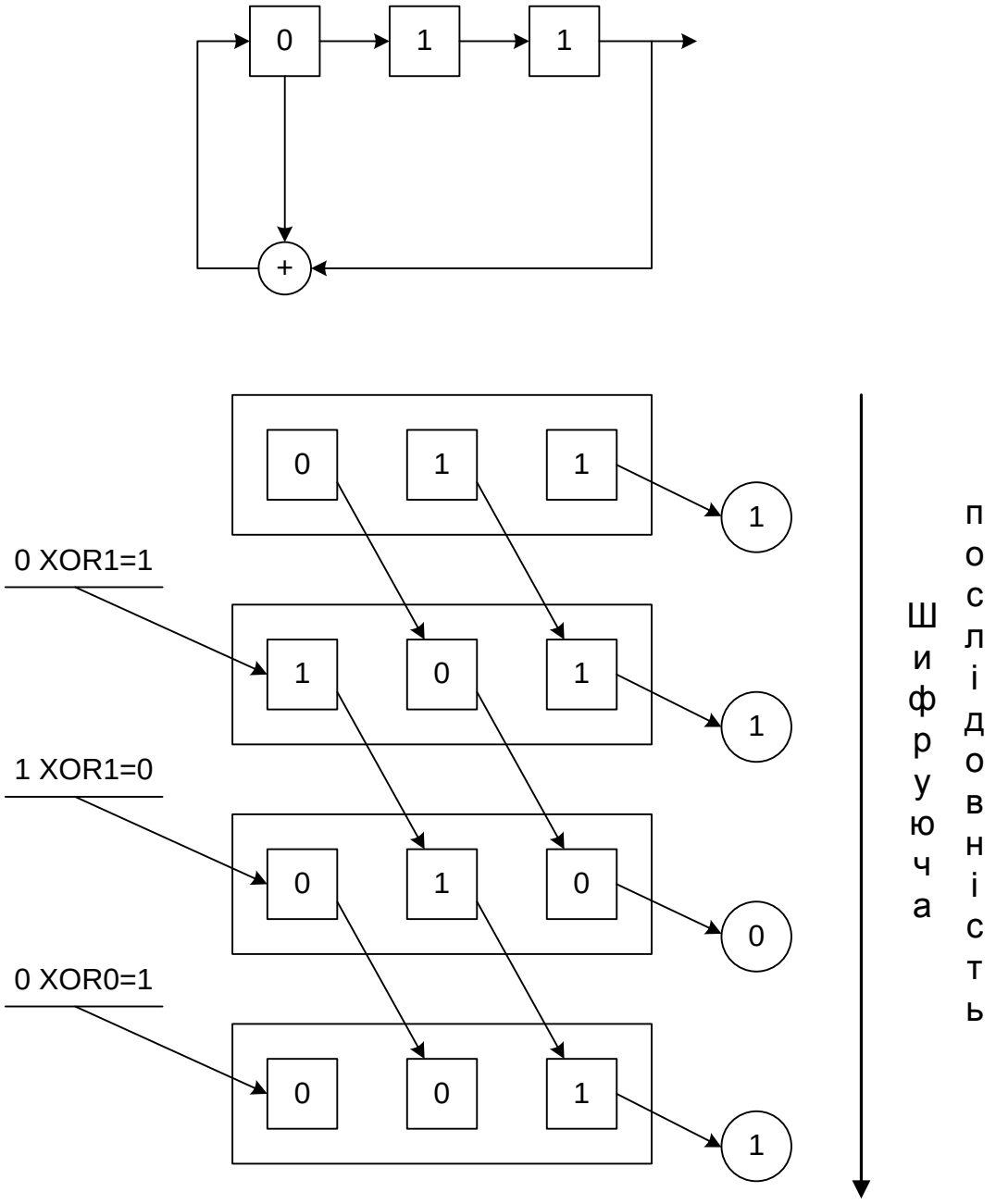


Рис. 6.6. Приклад роботи ЛРЗ розрядності 3 з установкою ключа 011

Якщо скремблер працює досить довго, обов'язково виникає його зациклювання – тому що кількість можливих варіантів стану ЛРЗ кінцеве і, як наслідок, після виконання визначеної кількості тактів в його чарунках створюється комбінація біт, яка вже була утворена до цього. З цього моменту кодуючи послідовність почне циклічно повторюватися з фіксованим періодом. Якщо представити множину станів ЛРЗ та переходів між ними у вигляді графа, то в залежності від номера чарунок, які породжують зворотній зв'язок, можуть створитися зовсім різні топології. Деякі з них наведені на рис.6.7.

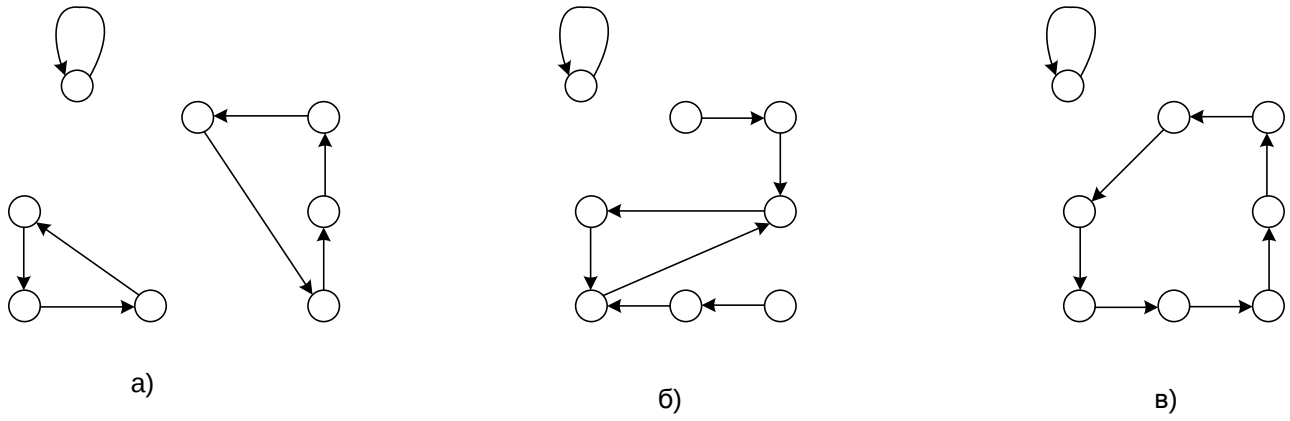


Рис. 6.7. Стани ЛРЗ та переходів між ними

Цикл „000” характерний для всіх графів внаслідок побудови ЛРЗ. На рис. 6.7.а бачимо окрім „нульового” циклу ще два цикли – 3^x та 4^x станів. На рис. 6.7.б ланцюг сходиться до циклу 3^x етапів і все ніколи звідти не виходить. І, нарешті, на рис. 6.7.в всі можливі стани, окрім нульового об’єднані в один замкнений цикл.

В вочевидь, що якраз у цьому випадку, коли всі 2^N-1 станів системи (де N - розрядність ЛРЗ), крім нульового, утворюють єдиний цикл, період повторення гами максимальний, а кореляція між довжиною циклу та початковим станом регістру (тобто ключем), яка привела до появи більш слабких ключів, відсутня.

Схеми з вибраними за даним законом зворотними зв’язками називають генераторами послідовностей найбільшої довжини. Існує велика кількість публікацій з рекомендаціями щодо таблиць номерів чарунок, від яких треба вибрати відводи зворотного зв’язку для одержання ПНД. В цілому проблема породження послідовностей найбільшої довжини на ЛРЗ тісно пов’язана з математичним поняттям неприводимих та примітивних поліномів над полем Галуа $GF(2)$.

Основною завадою до застосування ЛРЗ у якості безпосередньо шифрів є їхня нездатність протистояти атаці за відомим відкритим текстом. По-перше, коли зловмиснику відома структура зворотних зв’язків ЛРЗ розрядності N і хоча б N послідовних біт, породжених їм на будь-якому етапі шифрування (тобто стан регістру $(N-1)$ тактів назад), то всі наступні стани регістру можуть бути отримані самостійно. Таким чином, буде породжена вся наступна за цим моментом гама, та дешифровано весь текст. Більше того, відновлення біт гами можливо і в зворотному напрямку внаслідок побудови ЛРЗ. Це дозволяє зловмиснику записувати увесь шифротексту, який передається та одночасно виконувати спроби підібрати відповідний йому відкритий текст на основі набору високо вірогідних для даного контексту фраз або даних. Якщо в будь який момент часу відкритий текст довжиною N буде успішно підібрано, то і весь шифрований потік, який іде за ним, буде успішно

дешифровано. Паралельно, можливо на іншій ЕОМ, весь законспектований до точки взлому шифротексту буде прочитано в зворотному напрямку.

По-друге виявилось, що нестійкі до атаки на основі відкритого тексту й ЛРЗ з таємною структурою відводів зворотного зв'язку. Алгоритм, який запропонували Е. Берлекамп та Дж.Мессі, дозволяє на основі безперервної послідовності з $2 \times N$ біт збудувати ЛРЗ розрядності N, яка породжує таку послідовність. Таким чином, якщо навіть зловмиснику невідома структура ЛРЗ, то шляхом перебору спочатку з початкової позиції відомих слів або даних у відкритому тексті, а потім за розрядністю регістру зсуву (якщо вона невідома) можливо збудувати ЛРЗ, яка зашифрувала цей текст. При цьому відновлюється як структура ЛРЗ, так і поточні його стани, що дозволяє виконувати подальшу де шифровку як і у випадку з відомим видом зворотного зв'язку ЛРЗ. Для усунення цих недоліків були створені нелінійні поточні шифри.

Найбільш популярні на сьогоднішній день комбінуючи, фільтруючі та динамічні поточні шифри. Всі вони в якості базових елементів використовують лінійні регістри зсуву, при цьому тільки ті, які породжують послідовності найбільшої довжини. У всіх трьох методах основною метою ставиться одержання великого періоду породжуваної гами, високої не лінійності, стійкості до атак за відкритим текстом та кореляційним атакам.

Фільтруючі шифру мають найбільш просту структуру з нелінійних поточних шифрів. Їх будують на базі одного ЛРЗ шляхом створення від його чарунок додаткових відводів, ніяк не пов'язаних з відводами зворотного зв'язку. Значення, які отримують за цими відводами, зменшують на основі якоїсь нелінійної функції – фільтру (рис. 6.8.). Біт – результат цієї функції й подають на вихід схеми як черговий біт гами.

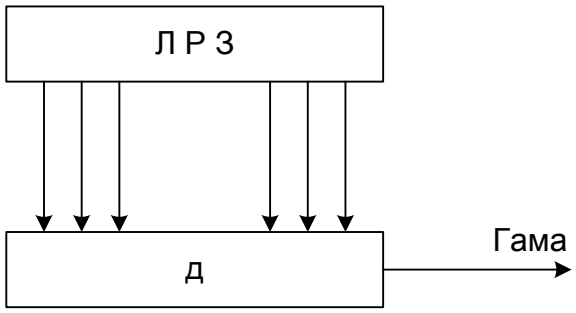


Рис. 6.8. Фільтр

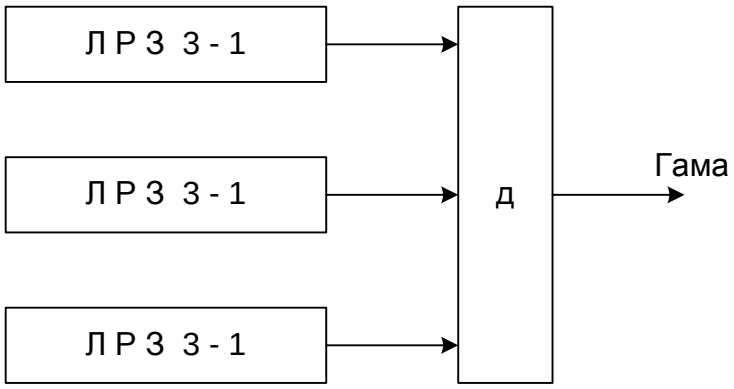


Рис. 6.9. Комбінація шифрів

Комбінуючи шифри будуються на основі декількох ЛРЗ, об'єднуючи нелінійною функцією біти, які породжуються кожним з ним на черговому кроці. (рис. 6.9.).

Однією з основних проблем комбінуючи шифрів є можливість витоку інформації з одного або декількох ЛРЗ у вихідну гаму. Так, у найпростішому випадку, наведеному на рис. 6.10., підсумкова шифруючи послідовність породжується за формулою $g = a \oplus (b \,\&\, c)$. Не дивлячись на те, що така гама є збалансованою, тобто вірогідність появи „0" та „1" у ній співпадають, у неї з неприпустимо великою вірогідністю проходить поток біт, який породжений першим ЛРЗ. Дійсно, вірогідність $P(g = b) = 4/8 = 1/2$, але $P(g = a) = 6/8$. Це дозволяє при досить великому обсязі інформації, яка перехвалена, чим це було раніше, проводити на перший ЛРЗ все ті ж атаки, що й на одиночний ЛРЗ. А отримавши всю необхідну інформацію по першому ЛРЗ, можна або безпосередньо скористатися нею для прочитання з „догадкою" відкритого тексту, або намаганням отримати більше інформації про другий та третій ЛРЗ.

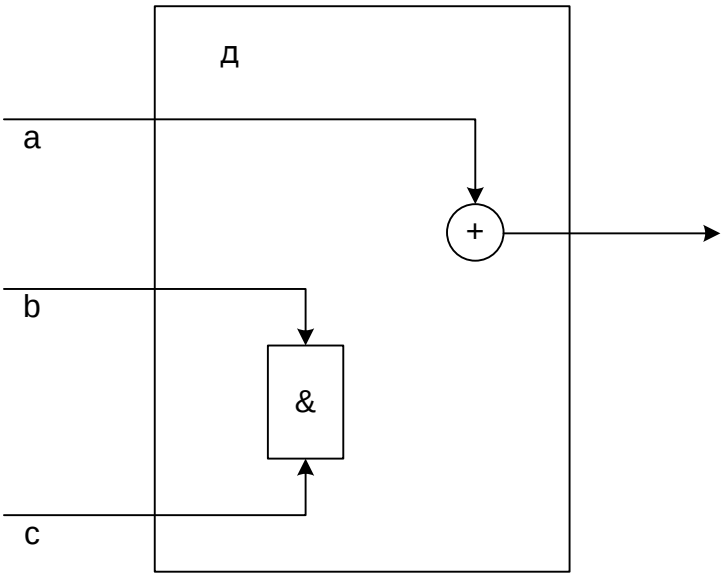


Рис. 6.10. Блок-схема формування шифру

Метод атаки, який наведений вище називають кореляційною атакою на комбінуючий шифр. Комбінуючий шифр називають кореляційно-стійким. Якщо для будь-якої комбінації

ЛРЗ, яка входить у її склад, значення коефіцієнта кореляції між бітами цих ЛРЗ та результуючим бітом шифру дорівнює $1/2$.

Однак, після проведення математичних досліджень виявилося, що чим вище ступінь не лінійності об'єднуючої функції нелінійного фільтру тим нижче його кореляційна стійкість і навпаки. Розробники потрапили між двома криптоаналітичними атаками. Одним з методів виходу з цієї ситуації є використання в об'єднуючий функції додаткових елементів пам'яті. Такі чарунки зберігають декілька біт, які характеризують попередні стани функції, та змішують їх до неї ж на етапі обчислень. (рис. 6.11.).

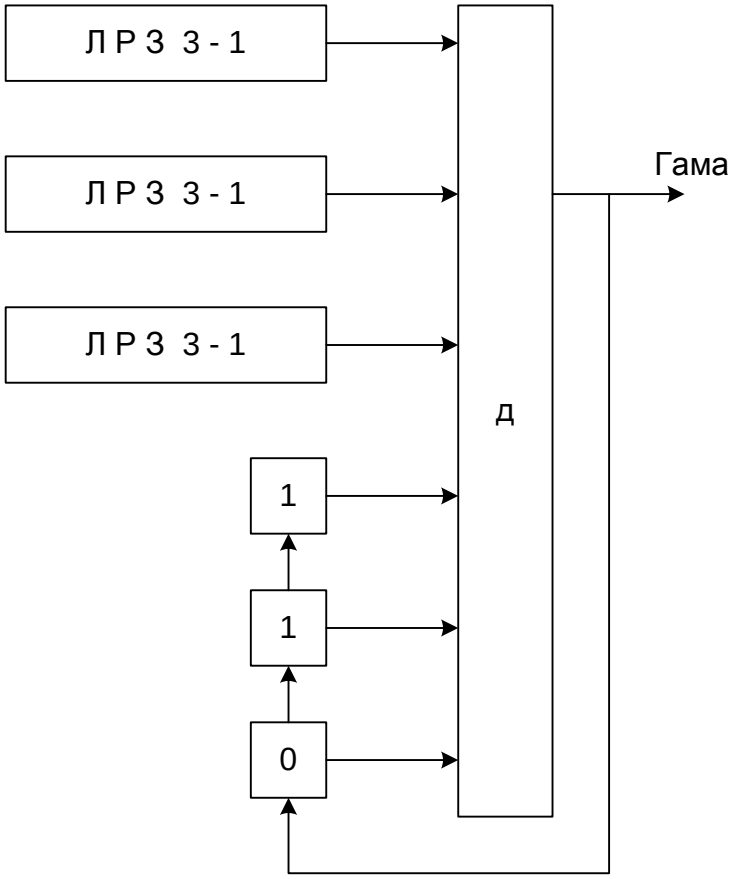


Рис. 6.11. Використання в об'єднуючий функції додаткових елементів пам'яті

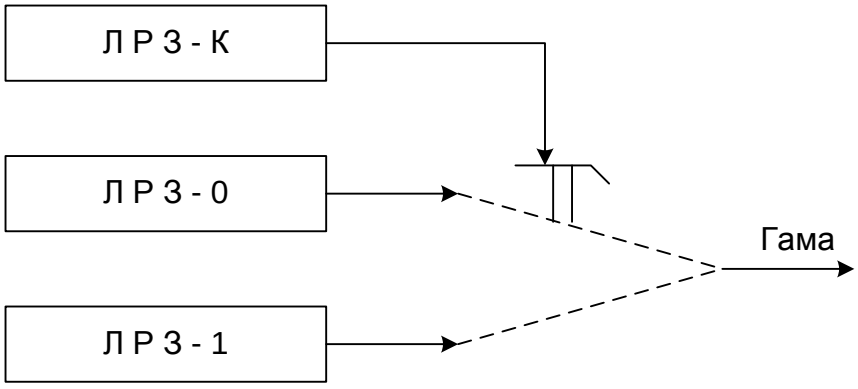


Рис. 6.12. Динамічні шифри, які будуються також на базі декількох ЛРЗ

Динамічні шифри будуються також на базі декількох ЛРЗ, але об'єднують їх не на рівних засадах, а за схемою „начальник-підлеглий". Так, наприклад. У схемі, яка наведена на рис. 6.12., біт, який породжується керуючим регістром, визначає біт. Якого з підлеглих ЛРЗ (першого чи другого) буде подано на вихід всього алгоритму. Біт з протилежного вибраному регістру відкидається.

За іншою схемою, якщо на черговому кроці керуючий ЛРЗ генерує „1" то біт підлеглого ЛРЗ на цьому ж кроці поступає на вихід системи, а якщо керуючий ЛРЗ видав „0" то біт підлеглого регістру просто відкидається. Звичайно, можливі й більш складні схеми взаємодії ЛРЗ та їх комбінацій з вище наведеними методами.

6.3.2. Основи блочного шифрування

Відмінною рисою блочних шифрів є обробки первісного по декілька (десятків, сотень) біт, тобто поблочна. Блочні шифри є логічним продовження ідеї алфавітних замін, перенесеної у новий цифровий час. Вочевидь, що при виконанні алфавітних підстановок двохлітерних пар (біграм) на інші двохлітерні пари, частотний аналіз стає вже досить складною задачею. У тому випадку, коли за якимось законом змінюються набори з 4,8 або навіть 16 символів, ні про яке частотне розкриття шифрів мови іти не може – обсяг шифротексту, необхідного для такої атаки, росте експоненційно. Проблема, із-за якої такі схеми не були застосовані раніше, заключалися у відсутності надійного та простого у застосуванні алгоритму таких перетворень, та ще й в ідеалі й залежного тільки від ключа шифрування.

Все змінила електроніки. У сучасних системах обробки, передачі та збереження інформації двоїчне представлення даних дозволило досягти небувалої абстракції форми від змісту. Будь який інформаційний потік може бути представлений у вигляді набору уніфікованих знаків - біт. А обчислювальні машини дозволили розробити зовсім інші закони модифікації даних.

Будь який блочний шифр у загальному вигляді являє собою закон відображення множини вхідних блоків первісного тексту на множину блоків зашифрованого тексту. Крім того, цей закон дуже сильно залежить від таємного ключа шифрування. В принципі, блочний шифр – це шифр заміни над дуже великим алфавітом (з десятків та сотень біт). Потенційно будь який шифр заміни можна описати повною таблицею відповідності між вхідними та вихідними даними. Так, як це робилося й для політерних замінах. Але для того щоб описати тільки одне відображення на 64 – бітним блоком (тобто алфавітом з 2^{64} елементів) знадобиться $64 \times 2^{64} = 2^{70}$ біт запам'ятовуючого пристрою, а це ж відображення буде застосовано тільки при якомусь одному конкретному значенні ключа. Тому сучасний блочний шифр – це закон, який описує дане відображення алгоритмічно.

Кількість Біт блоці, який оброблюється називають розрядністю блока, а кількість біт у ключі розміром ключа алгоритма. Найбільш популярна на сьогоднішній день розрядність блоку – 64 та 128 при розмірі ключа 128,192 або 256 біт. У загальному вигляді процес блочного шифрування описується формулою

$$Z = E_n Crypt(x, key),$$

де x – блок первісного текста, Z – зашифрований блок, key – ключ шифрування. Розрядність зашифрованого блока в класичних блочних шифрах співпадають з розрядністю первісного блока, тому за етап шифрування поток даних не зменшується і не збільшується в розмірах. Дешифрування описується відповідно формулою

$$X = Д_e Crypt(Z, key),$$

У тих випадках, коли і для шифрування для дешифрування використовується одна й таж послідовність дій, тоб то $E_n Crypt = Д_e Crypt = Crypt$ та, відповідно. $Crypt(Crypt(Z, key), key) = X$ блочний шифр називають абсолютно симетричним такі шифри мають як переваги так і недоліки.

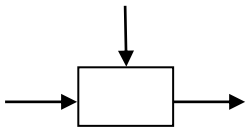
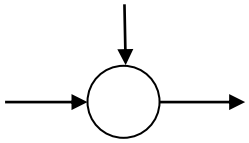
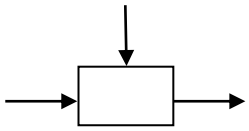
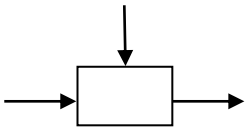
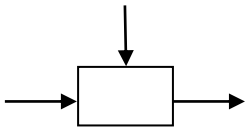
Основною ідеєю майже всіх блочних шифрів є той факт, що послідовність біт будь якої довжини Q можна представити у вигляді натурального числа у діапазонні $[0 \ldots 2^Q - 1]$. Більш того, один та й той же обсяг даних, розбиваючи на подібні блоки різними способами, можна представити як у вигляді великого набору невеликих чисел, наприклад, від 0 до 15 або від 0 до 255, так і у вигляді декількох чисел, наприклад, діапазону [0...4294967295]. Тут все залежить від схеми розбиття потока даних на блоки біт. Отже над цими натуральними числами й виконуються множина простих математичних та алгоритмічних перетворень, так званих криптопримітивів – з числа тих, які легко виконуються на сучасних ЕОМ.

Для криптоперетворень немає ніякої різниці, чи являє група біт (число), що оброблюється будь-який сенс чи ні. Наприклад, на якомусь проміжному етапі у 8-бітному блоці, який оброблюється перші два біта можуть бути взяті з третьої букви тексту, який шифрується, наступні три – з шостої, а останні три біта обчислені на основні першої, а останні три біта обчислені на основні першої та п’ятої літери. Головне, щоб після встановлення на приймальній стороні всі біти в блоці зайняли свої вірні місця та отримали правильні значення, тобто знову перетворення у текст, який має зміст. У такому абстрагуванні від змістового навантаження на проміжних стадіях і заключена сила двоїчного представлення даних.

Безсумнівно, що для однозначного дешифрування тексту на приймальній стороні всі перетворення, які були застосовані повинні бути оборотними. На жодному з етапів шифрування з послідовності, яка оброблюється не повинна виникнути втрати інформації. наведені в табл. 6.2.

Табл. 6.2

Перелік найбільш прийнятних перетворень та їх умовні позначення на схемах

Операція	Умовні позначення	Математична нотація	Примітка
Додавання		$X' = X + V$	У разі переповнення результатом розрядності операндів біт переносу відкидається – втрати інформації при цьому не відбувається
Виняткове		$X' = X \oplus V$	Операція оборотна сама собі
Множення за модулем 2^N+1		$X' = (X * V) \bmod (2^N + 1)$	Це перетворення оборотне. Множник за відомим добутком та іншому множнику знаходиться за алгоритмом Евкліда
Циклічний бітовий зсув вліво		$X' = X\ ROL\ V$	Операція є зворотною до циклічного зсуву вправа
Циклічний бітовий зсув вправо		$X' = X\ ROR\ V$	Операція є зворотною до циклічного зсуву вліво
Таблична підстановка		$X' = S - Box[X]$	

Декілька слів про табличні підстановки, які займають окреме місце у криптографічних перетвореннях. За допомогою табличних підстановок (англ.. Substitute-box-S-box) реалізують найбільш загальні закони зміни даних, які часто не відтворюються не аналітично, ні алгоритмічно. У тих випадках коли у шифрую чому алгоритмі треба реалізувати доволі складну для мікропроцесора або функцію, яка взагалі не описується алгоритмом, найбільш прийнятним рішенням є занесення її значення в масив, який зберігається у постійній або оперативній пам'яті. Таке завдання функції називають табличним.

Кількість біт у первісному операнді називають розрядність входу табличної підстановки, кількість біт у результаті – розрядністю виходу. У більшості випадків табличні підстановки використовуються у якості біективної (однозначно оборотної) функції – у цьому

випадку розрядність входу та виходу співпадають. Найбільш часто за токою схемою використовуються підстановки 4×4 (чотири на чотири) біта та 8×8 біта. Оборотне перетворення $\left(S-Box^{-1}\right)$, якщо у ньому є потреба, задають дешифруючій стороні також таблицею такого ж розміру. У випадку коли від підстановок не вимогають оборотності, разом з традиційними застосовуються підстановки $4\times8, 8\times32$ біта деякі інші.

Запис функції в таблиці має свої переваги та недоліки. У порівнянні з довгим обчисленням функції виборка з таблиці виконується значно швидше . але ці дві операції не можна порівняти за швидкістю зі звичайним додаванням або XOR, тому що одним з операндів у вибірці завжди є чарунка пам'яті, і передбачити заздалегідь, яка з чарунок буде потрібна, неможливо. Тому на сучасних процесорах таблична вибірка виконується часних процесорах таблична вибірка виконується доволі швидко тільки тоді, коли вся таблиця розміщена в кеш-пам'яті процесора. У протилежному випадку кожна операція вибірки ініціює багато тактовий процес звертання до оперативної пам'яті. Все це накладає жорсткі обмеження на розмір таблиці, яка зберігається та, відповідно, розрядність її входу та виходу.

Однією з незаперечних переваг табличних підстановок є швидкість у відношенні до нелінійних операцій. Практично всі наведені у табл.6.2. операції, окрім множення за модулем 2^{N+1} табличних підстановок, мають дужу високу лінійну залежність між вхідними та вихідними значеннями. А це дуже пагано у відношенні крипостійкості шифра до лінійного криптоаналізу. Для підвищення стійкості шифра до цього класу атак таблична підстановка набагато краще операції множення за модулем 2^{N+1}, і є на сьогодні найбільш прийнятним нелінійним перетворенням.

У тих випадках, коли від перетворень не вимогають оборотності за вхідними параметрами, додатково до наведених вище оборотних функцій використовуються операції, які наведені у табл.6.3.

Табл.6.3.

Основні необоротні криптопримітиви

Операція	Умовні позначення	Математична нотація	Примітка
Множення		$X' = (X \cdot V) \bmod (2^N)$	$X' = (X \times V) \bmod (2^N)$
Остача (модуль) від ділення		$X' = X \bmod V$	$X' = X \bmod V$
Арифметичний бітовий зсув вліво		$X' = X \ SHL \ V$	$X' = X \ SHL \ V$
Арифметичний бітовий зсув вправо		$X' = X \ SHR \ V$	$X' = X \ SHR \ V$

Логічне “І”		$X' = X \ AND \ V$	$X' = X \ AND \ V$
Логічне “ЧИ”		$X' = X \ XOR \ V$	$X' = X \ XOR \ V$

Покажемо, що може виступати у якості параметрів V у оборотних та необоротних операціях. Поперше це фіксовані числові контакти. Єдиним обмеженням, яким завжди користуються проектувальники блочних шифрів, є логічне обґрунтування їх вибору. У тих випадках, коли шифр повний фіксованих числових констант, вибір яких тяжко пояснити, може виникнути підозра, що розробники планомірно конструювати їх для одержання яких-небудь не документальних можливостей по розкриттю шифра. Тому, коли застосування фіксованих числових констант виконує тільки роль “перемішування” даних, їх звичайно вибирають з двоїчного запису загальновідомих, не пов’язаних ні з чим величин, наприклад, чисел π, е або φ (золотий переріз), або як контрольну суму якого-небудь розповсюдженого тексту.

Другим можливим значенням параметру V є матеріал ключа. Матеріалом ключа називають блок даних, обчислений на основі ключа шифрування і такий, що залежить тільки від нього. У найпростішому випадку матеріалом ключа може бути сам ключ (якщо його розрядність співпадає з розрядністю операцій) або довільна його частина без будь-якої обробки. Але пряме застосування ключа у перетвореннях може привести до розкриття деякої інформації про нього, наприклад, при великій кількості відомих пар “відкритий текст/ зашифрований текст” І, хоча вірогідність такої атаки дуже мала, треба перестрахуватися. Для цього у якості матеріла ключа використовують значення, які обчислені з нього за необоротною схемою. Про цьому краще за все, щоб будь який елемент матеріала залежав від усіх біт ключа, тому що навіть за найменших змін ключа (наприклад тільки в одному біті) повинен змінюватись і доволі суттєва кожен блок матеріалу ключа.

Операції, в яких у якості параметра V використовується матеріал ключа, називають перемішуванням з ключем або додаванням ключа (ніякого зв’язку з арифметичною операцією цій термін не несе) таких операцій під час шифрування одного блоку виконуються досить багато. Таким чином, вирішується одна з головних вимог до шифрів – не відновлює міcть ключа. Дійсно, якщо до блоку даних додавати одну й туж інформацію, але неодноразово та різними способами, то така інформація буде необоротна відносно доданої інформації, хоча оборотність відносно першого операнда залишиться. Наприклад, нехай X та K – чотирьох бітні первісне число та ключ відповідно (діапазон можливих значень 0...15 у кожного), тоді формула:

$$X' = \left((x + k)X \ OR \left(k + 7\right)\right) AND 1111_2$$

де нижній індекс вказує на систему числення.

Є оборотною відносно X – завжди за відомими X' та K можна відновити X, але необоротною відносно K по відомий парі X та X'. Не існує аналітичної формули, яка б обчислювала КК через X та X'. Звичайно завжди можна скласти табличну залежність, перебрав при відомому Хусі K та записав усі X', які вийшли. Але це легко зробити тільки у гіпотетичному прикладі з 16 можливих значень 12. на практиці при довжині ключа у 128 біт для вирішення цієї задачі не вистачить а ні ресурсів пам'яті для зберігання. Ні обчислювальних можливостей ЕОМ. Таким чином, багаторазове додавання матеріалу ключа за складною схемою є надійним засобом захисту блочних шифрів від атаки за відомими парами відкритий / зашифрований текст.

Третім можливим значенням параметру V є значення, обчислене від незалежної частини блоку, який шифруються. Цей метод лежить в основі схеми блочного шифрування та носить назву мережі Файштеля. Операції, які задіяні у якості другого параметру само значення блоку, який шифрується, оборотні, тільки тоді якщо вони оперують незалежними частинами блоку. Наприклад, на якомусь поміжному етапі на перші байт операцію XOR накладається значення п'ятого байта і так далі. Оборотність забезпечується на тій підставі, що на приймальній стороні алгоритм, підходячи до де шифровки цього місця, вже "знає" значення п'ятого байта, яким проводиться накладання, та повторним виконанням XOR відновлюється перший байт. Проблема виникла б, якщо на переший байт наклали функцію від цього ж першого байта. Тоді, навіть не дивлячись на потенційну оборотність операції, дешифруючи сторона не змогла б обрахувати значення V і зайшла б у глухий кут .

Однією з найбільш розповсюджених схем блочних шифрів є мережа. Блочний шифр, побудований за такою схемою, складається з багаторазових повторень, які носять назву циклів або раундів декількох видів операцій, що носять назву шару. Розбиття всього процесу шифрування на декілька одно тип них шарів дозволяє:

- скоротити розмір програмного коду використанням циклу;
- уніфікувати "алгоритмічну формулу" шифрування і, як наслідок спростити перевірку стійкості шифра до відомих видів криптоатак;
- зробити шифр таким, який легко ускладнюється у разі необхідності (шляхом збільшення кількості раундів);
- ввести поняття ключів раунда, на які розбиваються матеріал ключа.

Деякі з шарів не містять у собі процедур змішування з ключем. Звичайно вони виконують функції оборотного змішування даних всередині блоку, або захищають блочний шифр від якого-небудь конкретного класу криптоатак. Такі шари виконують свої перетворення завжди за однією і тією схемою. У тих шарах, де в якості параметрів операцій використовуються матеріал ключа, на кожному раунді використовуються завжди все нові та нові блоки з матеріалу ключа – ключі раунда. Тому кожен такий шар виконує своє унікальне

перетворення матеріалу. Ця схема дозволяє поряд з уніфікованістю перетворення за невідомим ключем схему.

Однією з найбільш простих та раніх мереж є SP – мережа (SP - network) кожний раунд якої складається з двох шарів. Свою назву ця мережа отримала від скорочення англійських слів: Substitution (підстановка) та Permutation (перестановка). У шарі підстановки над даними виконуються перетворення класу додавання, виключаю чого ЧИ, табличних підстановок, у якості параметрів використовуються константи та матеріал ключа. У шарі перестановки біти або зрідка байти міняються місцями всередині блоку звичайно за фіксованою (не залежного від ключа) схемою.

Більш сучасною модифікацією технології мереж є KASLT – мережа з трьома шарами у кожному раунді. Перший шар – додавання ключа (Key Addition, KA) – виконує змішування даних з ключем раунда. Змішування виконується звичайно якою-нибудь простою операцією – додаванням або XOR. Другий шар - підстановка (Substitution, S) – виконує алгоритмічну або частіше табличну підстановку для, забезпечення нелінійних якостей шифра. Третій шар – лінійне перетворення (Linear Transformation, LT) виконує активне оборотне змішування даних всередині блоку.

Як видно, у порівняні з SP мережею тут додавання ключа винесено у окремий шар, розподілені лінійна та нелінійна частини перетворень, а змішування даних виконується за допомогою лінійних перетворень, які швидко реалізуються в програмі.

Практично незалежною від двох попередніх розробок і дуже популярною на цей час є схема блочних шифрів яка носить назву мережа Файштеля (рис. 6.13). У кожному з її раундів тільки по одному шару, тобто усі перетворення однотипні. Але сама структура перетворень специфічна: на деяку частину блоку, який шифрується оборотною операцією накладається значення функції (можливо, необоротної), яка обчислена від іншої частини блоку.

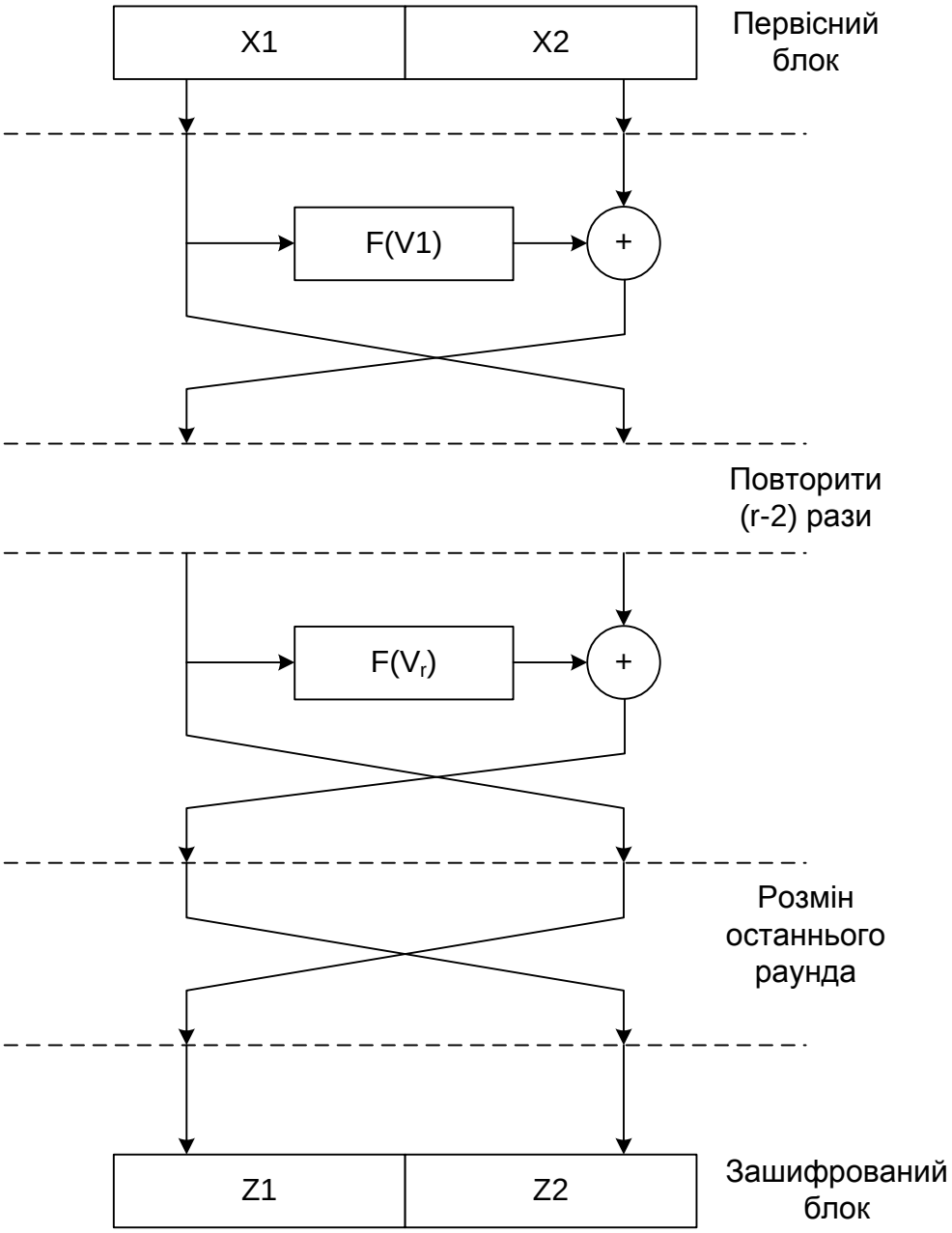


Рис. 6.13. Мережа Файштеля

Незалежні потоки інформації, які породжені з первісного блоку, носять назву вітки мережі. У класичній схемі їх дві. Величини V1 носять назву параметрів мережі, звичайно їх роль відіграють матеріали ключа. Функція F носить назву утворюючий. Оптимальна кількість раундів для мережі Файштеля К – від 8 до 32. мережа Файштеля є оборотною. Вона має таку якість, що навіть якщо у якості утворюючої функції F буде використано необоротне перетворення, то і в цьому випадку весь цей ланцюжок буде відновлювальним. Це виникає в наслідок того, що для оборотного перетворення мережі Файштеля не потрібно обчислювати функцію F^{-1} – і під час дешифрування обчислюється тільки пряме значення F. Оборотність вимагається тільки для операції накладання F на вітку, яка шифрується у цьому раунді, тому тут частіше всього використовуються XOR та зрідка арифметичне додавання.

Більш того, мережа Файштеля, в якій для накладання значення F використовуються операція XOR, симетрична. Виключаючи ЧИ оборотнього своїм же повторенням, і тому інверсія останнього обміну віток робить можливим розкодування блоку тією ж мережею Файштеля, але з оборотнім порядком параметрів V1. Відзначимо, що для оборотностиі мережі Файштеля не має значення, чи є кількість раундів парним чи, непарним. У більшості реалізацій мережі Файштеля пряме та зворотне перетворення виконується одним і тим же фрагментом програмного кода, який оформлений у вигляді процедури, якому в якості параметру передається вектор величини V1 або у первісному (для шифрування), або у інверсному (для дешифрування) порядку.

З незначними доробками мережу Файштеля можна зробити и абсолютно семеричним шифром, тобто таким, що виконує функція шифрування та дешифрування одним і тим же набором операцій. Модифікація мережі Файштеля з такими якостями наведена на рис. 6.14. Основна особливість її полягає у зворотному порядку у другій половині циклу. Треба відмітити, що як риз із-за цієї недостатньо дослідженої специфіки такої схеми її використовують у криптоалгоритмах з великою обережністю. Справа в тому, що є потенційна можливість ослаблення зашифрованого тексту оборотними перетвореннями.

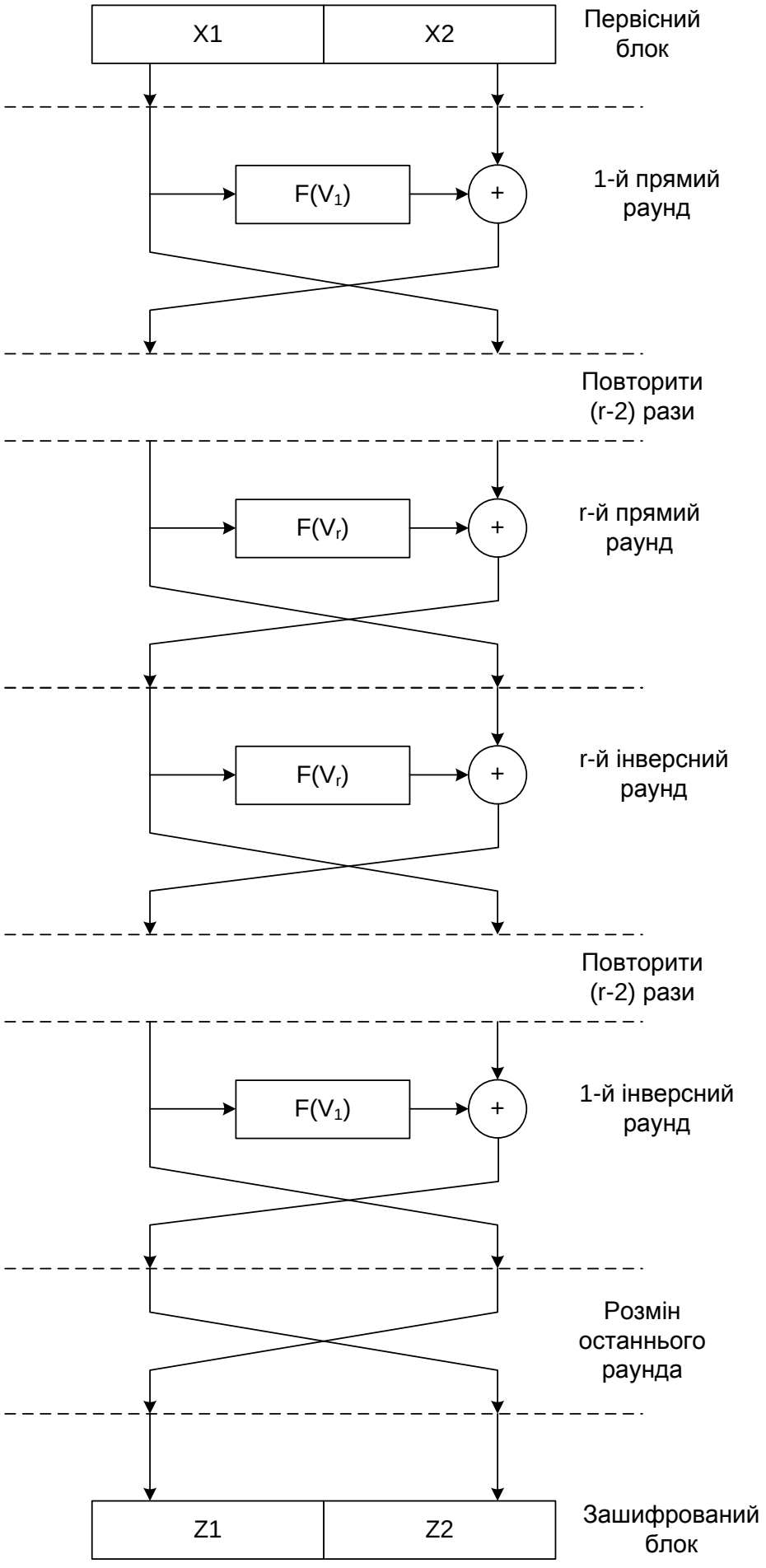


Рис. 6.14. Модифікація мережі Файштеля

А ось модифікація мережі Файштеля для більшої кількості віток застосовують значно частіше. Це в першу чергу пов’язано з тим, що при великих розмірах блоків, які шифруються (128 та більше біт) стає незручно працювати з математичними функціями за модулем 64 та вище. Як відомо, основні одиниці інформації, які обробляються процесорами на сьогоднішній день –це байт і подвійне машинне слово – (32 біта). Тому все частіше у блочних криптоалгортмах зустрічається мережа Файштеля з 4 вітками. А для більш швидкого змішування інформації поміж вітками застосовуються дві модифіковані схеми які носять назву тип – 2 та тип – 3. За рахунок часткового об’єднання обробки потоків у двух останніх схемах кількість раундів у них лише ненабагато більше кількості раундів у мережі Файштеля з двома вітками.

Далі розглянемо практику блочного шифрування у хронологічному порядку з початку його розробки у 70 – роках минулого століття. У 1980 році в США було прийнято національний стандарт шифрування даних DES (Data Encryption Standard). Алгоритм роботи цього стандарту являє собою класичну мережу Файштеля з 16 раундів з додаванням вхідної та вихідної та вихідної перестановки біт, з розрядністю блока –64 біта розмірами ключа 56 біт. Загальна структура алгоритму наведена на рис. 6.15.

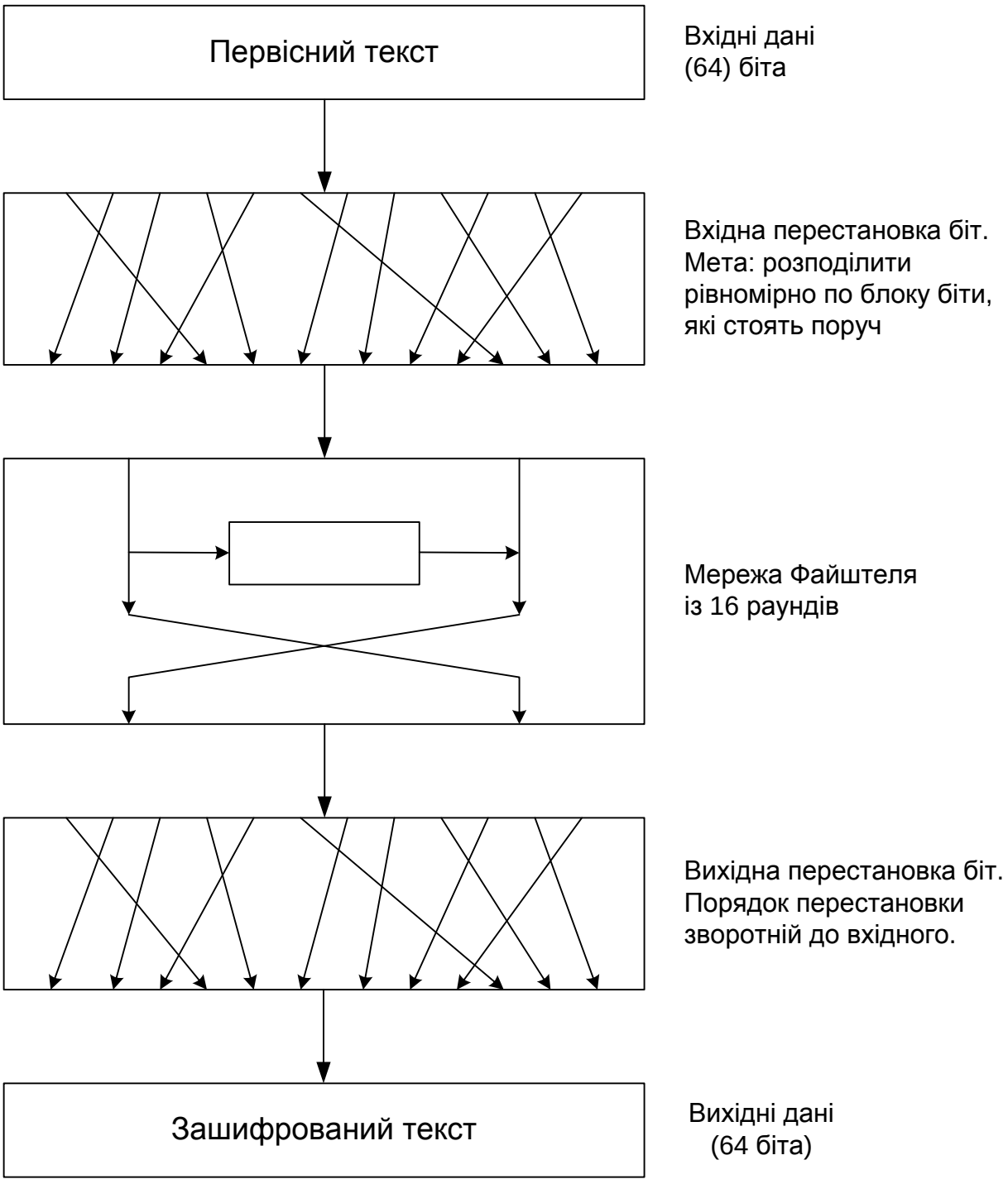


Рис. 6.15. Загальна структура алгоритму

Загальна формула для обчислення індексів у псевдокоді має вигляд:

цикл по і від 0 до 63

$$OUT[i_5 i_4 i_3 i_2 i_1 i_0] = IN[(7-(i_2 i_1 i_0))|(i_4 i_3)|1-(i_5))],$$

де запис X_r символ означає r-q біт у запису чисел, X, | це конкатенація (зчеплення) цифр у двоїчному запису чисела.

Додавання матеріала ключа виконується тільки в мережі Файштеля тому тільки вона виконує шифрування даних.

Розрядність ключів раундів які застосовуються у DES дорівнює 48 бітам. Для симетричності алгоритму шифрування / дешифрування в DES як і в класичній мережі Файштеля, виконується додатковий розмін останнього обміну віток. Це дозволяє виконувати шифрування та дешифрування одним і тим же програмним кодом, здійснюючи передавання йому у першому випадку ключі раундів у прямому порядку $(k_0, k_1 \ldots k_{15})$, а в другому випадку – у зворотному. Загальний вигляд мережі Файштеля алгоритму DES наведено на рис. 6.16.

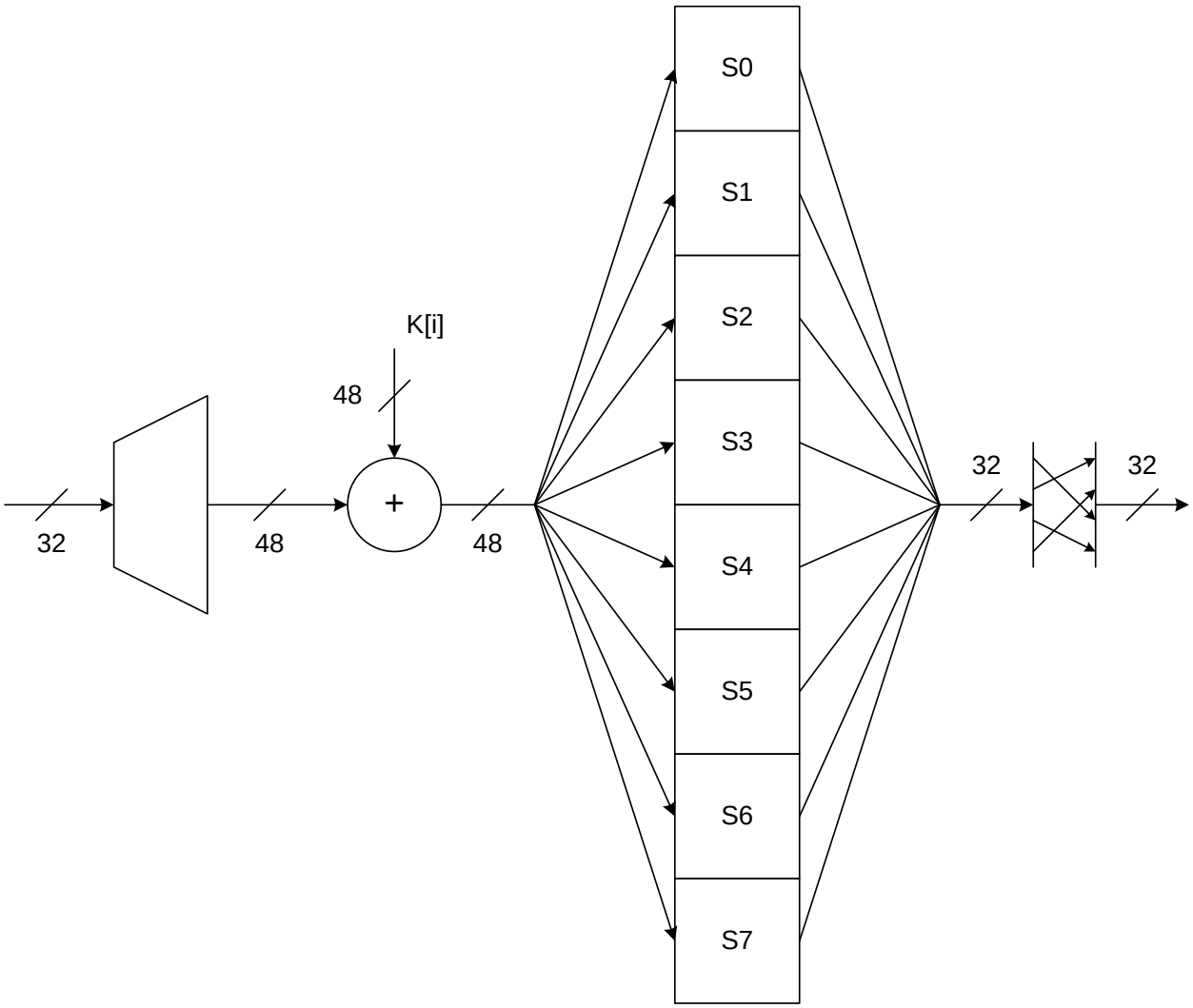


Рис. 6.16. Мережа Файштеля алгоритму DES

Утворююча функція мережі в алгоритмі DES складається з 4 операцій:

1. перестановка біт / розширення блоку за допомогою повторень за вказаною схемою;
2. накладання ключа раунда операцією XOR;
3. табличні підстановки;
4. перестановка біт.

Розширення вхідних даних виконуються на рівні біт шляхом запису деяких з них у вихідний потік двічі. У результаті з 32 біт утворюється 48 – бітний блок інформації який

співпадає за розміром з ключем раунда. Накладання ключа раунда виконується операцією XOR з рядністю операції – 48 біт.

Табличні підстановки, які застосовуються в DES, мають розрядність 6×4 біта. 48 – бітний блок даних після накладання ключа розбивається через свою табличну підстановку, яка позначається як S_0, S_1 та таке інше. В результаті отримуємо 8 блоків по 4 біта у кожному: всього 32 біта – первісна розрядність вітки, яка обробляється.

Заключною операцією утворюючої функції є перестановка біт всередині 32 – бітного блока, який відповідає за змішування інформації. Загальний вигляд одного раунда мережі Файштеля алгоритма DES наведено на рис. 6.17

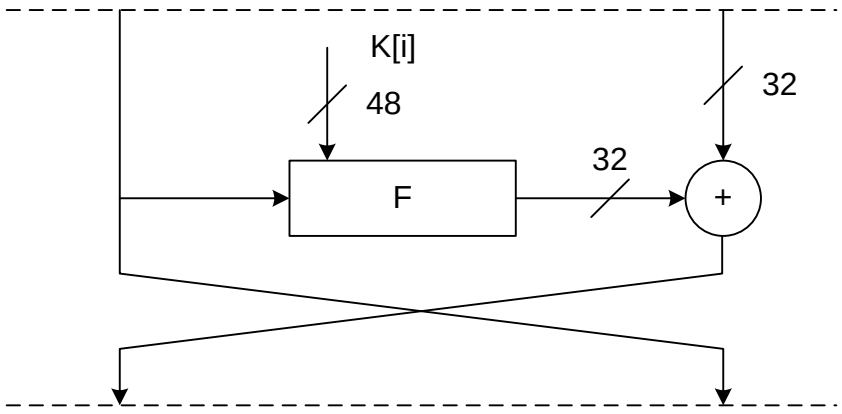


Рис. 6.17. Один раунд мережі Файштеля алгоритма DES

Розширення ключа (створення ключів раунда) виконується в DES за такою схемою значущих. На основі 56 значущих біт із ключа на початковому етапі створюються за окремим законом два 28-бітних вектора Со та До. Ці закони встановлюють порядок послідовності вибору біт з ключа.

Інститутом стандартизації рекомендовано під час зберігання ключа для DES використовувати найпростіше завадостійке кодування – перевірку парності. Тому в кожному байті значущими є тільки перші 7 біт а восьмий додається до запису виходячи з правила кількості одиниць у двоїчному кожного байту непарно. Таким чином, при існуючий розрядності ключа у 56 біт зберігається він 64 – бітній структурі. Саме цим пояснюється поява в законі вибору біт для Со та До номерів, більших 56, та відсутністю біт з номерами 8, 16, 24, 32, 40, 48, 56, 64 (вони є контрольними тобто незначущими)

Для генерації кожного чергового ключа раунда k_i вектори Со та До циклічно зсуваються вліво на визначену кількість розрядів. А, для вибору 48 біт ключа і-го раунда, який одержали після циклічного зсуву вектора $C_i D_i$ об'єднуються, та з 56 біт масиву, що вийшов відбирають за окремим законом 48.

Аналізуючи принцип шифрування в DES, впадає в очі значна кількість бітових перестановок та виборок у алгоритмі. І, це не давно, тому, що основною схемою

проектувальниками планувалася тільки апаратна реалізація. Цьому підлягає й накладання ключа саме операцією XOR, яка реалізується у цьому випадку найбільш просто та розпаралелено, з невеликим розміром та мінімальною кількістю табличних підстановок. Апаратна реалізація алгоритму окремій або вмонтованій мікросхемі дозволяє досягти високої швидкості шифрування при досить малих пристроях.

Єдиним нелінійним елементом алгоритму є етап табличних підстановок в утворюючій функції. Розробники алгоритму не пояснили принцип вибору таблиць, які використовуються, але привели декілька правил яким задовольняють вибрані таблиці з метою захисту від деяких видів криптоаналізу.

Алгоритм має деякі специфічні властивості, які, на думку багатьох спеціалістів, не є значно вразливими. Першою особливістю є закон: якщо $Y = E_n Crypt(X, KEY)$, то $Y' = E_n Crypt(X', KEY')$, де X' - побітна інверсія X, Y' побітна інверсія Y, KEY' - побітна інверсія KEY.

Другою особливістю є наявність серед множини 2^{56} ключів чотирьох слабких ключів (weak KeyS). Під час шифрування даних будь яким з цих ключів серед 2^{64} вхідних даних існує 2^{32} блоки, які в результаті шифрування перетворюються самі в себе, тобто для них $E_n Crypt(X, WEAK\_KEY) = X$ не дивлячись на те, що вірогідність такого марного шифрування дуже велика ($1/2^{32}$ - для криптографії це дуже великий ризик), вірогідності того що сам ключ виявиться слабким, дуже мала $(1/2^{54})$. Це дозволяє вважати наявність слабких ключів у DES скоріше оригінальною особливістю ніж реального вразливістю.

Хоча, за багато років DES зарекомендував себе надійним шифром, йому довелося піти з ринку конкурентно – здатних шифрів. Це є наслідком його орієнтації на апаратну реалізацію та занадто малий розмір ключа.

Стрімкий злет потужності обчислювальної техніки вніс значні корективи в напрямки розвитку криптографії. Найбільш простим представником сімейства програмно-орієнтованих надійних блочних шифрів є TEA (Tiny Encryption Algorithm). Переклад цієї назви на українську мову може бути як “крихітний криптоалгоритм”. Це класична мережа Файштеля з 64 раундів. Алгоритм оптимізовано під 32 – розрядний мікропроцесор, розмір блоку – 64 біта.

Результат функції, яка утворилася накладається на незалежну вітку операцією “складання”, тому відновити первісний текст простим оберненням порядку ключів раунда не вдається. Отже, алгоритм TEA є прикладом несиметричної мережі Файштеля, в якому для дешифрування треба реалізувати окрему процедуру, яка є досить проста.

Існує також TEA: розширення ключа. Цей алгоритм використовує 128 бітний ключ, який перетворюється в ключі раунда за дуже простою схемою. Ключ розбивається на чотири 32 – розрядних машинних слова k_0, k_1, k_2, k_3. У всіх парних (рахуючи з О) раундах у якості 64 – бітного ключа раунда використовується пара (k_0, k_1), у непарних – пара (k_2, k_3). У загальноприйнятій схемі номер раунда позначається переміною і, кількість раундів – r, компоненти ключа раунда - як насив $k[\ ]$ (він використовує прохідну нумерацію за машинними словами – нолевому ранді використовується $k[0]$ та $k[1]$, у першому $k[2]$та $k[3]$ і таке інше) у такому випадку загальна формула створена 128 компонент матеріала ключа для TEA має такий вигляд $k[i] = k(i \bmod 4)$

Алгоритм, який був розроблений на заміну DES та, на відміну від TEA, отримав широке застосування носить назву IDEA (Interational Dat Encryption Algorithm). Правами на цей алгоритм володіє Швейцарський федеральний технологічний інститут ETHZ (Swiss Federal Institute of Tehnology Zurich) та компанія Ascom Tech Ltd.

IDEA побудована за схемою, яка схожа на мережу Файмтеля та носить назву узагальненої мережі Файмтеля. Первісний бдок даних довжиною у 64 біта розбивається на 4 вітки – всі операції в IDEA виконуються у 16-бітній арифметиці. Потім у кожному з 8-раундів над вітками та матеріалом ключа виконується у спеціально підібраній черговості три операції додавання, виключне 4И та модифіковане множення. Модифіковане множення позначають на схемах символом *. Довжина ключа алгоритму складає 128 біт.

Модифіковане множення являє собою звичайне множення за модулем 65537(2^{16}+1) з двома умовами. По-перше, якщо будь який з множників дорівнює 0, то перед множенням він заміняється на 2^{16}. По-друге, якщо число, після взяття модуля дорівнює 2^{16}, то воно заміняється на 0. Визначено таким чином операція має такі властивості:

відображує пару 16-розрядних чисел на 16-розрядне число;

оборотня (за відомим результатом та одному з множників в можливо однозначно визначити другий множник).

Для досягнення симетричності шифрування/дешифрування після восьми раундів над віками виконується додаткове перетворення. За допомогою такого доповнення розробники досягли того, що для дешифруванн в IDEA використовувається та на сама процедура, але в якості 52 компонент матеріала ключа їй передається спеціальним чином модифіковані компоненти.

Далі зупинимось коротко, на единому з офіційно надрукованих радянських блочних шифрів який, з годом був розкритий та був замінений на більш сучасний. Цей ГОСТ 28147-89 у 1989 році був прийнятий державним стандартом блочного шифрування і використовувався багатьма фахівцями з захисту інформації.

ГОСТ 28147-89 оперує 64 бітним блоком даних, здійснюючи шифрування за допомогою 256-біного ключа. Структура криптоалгоритму являє собою класичну мережу Файстеля із 32 раундів з двома вітками.

Розширення ключа виконується за дуже простою схемою. 256-бітний ключ розбивається на вісім 32-біних машиних слів. Вони номеруються з K_0 до K_7. 32 компоненти матеріала ключа отримують їх застосуванням у такому порядку:

$$K[0]\ldots K[31] = K_0K_1\ldots K_6K_7K_0K_1\ldots K_6K_7K_0K_1\ldots K_6K_7K_7K_6\ldots K_1K_0$$

У останній четвертій секції 8 машинних слів ключа записують у зворотньому порядку. Для дешифрування (за властивостями симетричної мережі Феймтеля) використовують той же код, але у зворотньому порядку ключів раунда.

Недостатня довжина ключа DES, його орієнтація на апаратну реалізацію та, як наслідок використання на практиці великої кількості маловідомих криптоалгоритмів спонукало уряд Сполучених Штатів до об'яви конкурсу на криптостандарт блочного шифрування початку нового віку. Конкурс отримав назву AES (Advanced Encryption Standart) – "поліпшений стандарт шифрування".

Вимоги до нового стандарту були такі:

шифр повинен бути блочним;

шифр повинен мати довжину блока, яка дорівнює 128 бітам;

шифр повинен підтримувати ключі довжиною 128, 192 та 256 біт.

Переможцем став алгоритм PIJNDAEL.

Цей блочний шифр розвиває нетрадиційну для останнього десятиріччя структуру: прямокутні KASLT – мережі. Ця структура отримала свою назву із-за того, що блок, який шифрують представлено у вигляді прямокутника (4x4 або 4x6 байт), і потім над ним по строчно, за стовпцями і побайтно виконуються криптоперетворення KASLT являє собою абревіатуру англійських термінів в Key Addition (додавання ключа), Substitution (таблична підстановка) та Linear Transposition(лінійне змішування). Цей шифр з варіативним розміром блока і довжиною ключа. Едині вимоги до цих параметрів – їх кратність 32 бітам. Розмір блоку надалі визначається як $Nb \times 32$, довжина ключа $Nk \times 32$. Кількість раундів мережі , які необхідні для стійкого шифрування залежить від цих двох параметрів.

Згідно з вимогами $Nb = 4$ (тобто 4×4 байти), але потенційно шифр може працювати й з більшими за розміром блоками.

Перед початком раундів KASLT – мережі на блок накладається операцією XOR перша порція матеріалу ключа. Раунди крім останнього, складаються з повторення чотирьох операцій: табличної, підстановки, циклічного зсуву строк, лінійного перемішування стовпців та додавання матеріалу ключа. У останньому раунді ці операції повторюються утому ж порядку, але з них виключено лінійне перетворення стовпців.

Накладання матеріалу ключа виконується операцією XOR. Матеріал добувається із масиву розширеного ключа K послідовно по чотири 32 – бітних блока у кожному раунді. При накладанні ключа прямокутна матриця розглядається як 4 стовпця з 32 – бітними записами у кожному. Див. рис. 6.18.

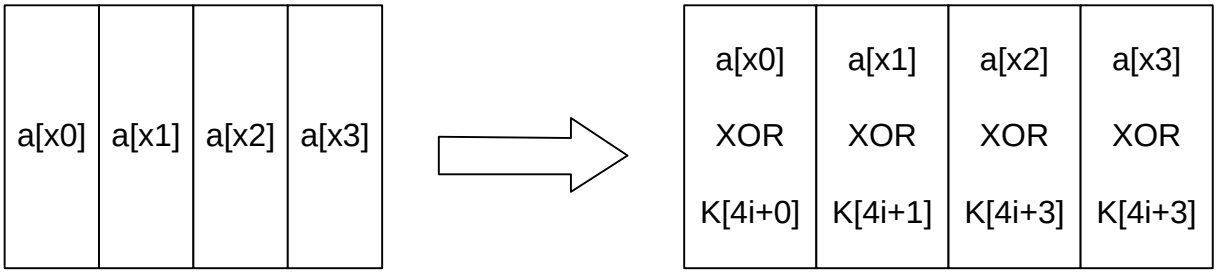


Рис. 6.18. Накладання матеріалу ключа

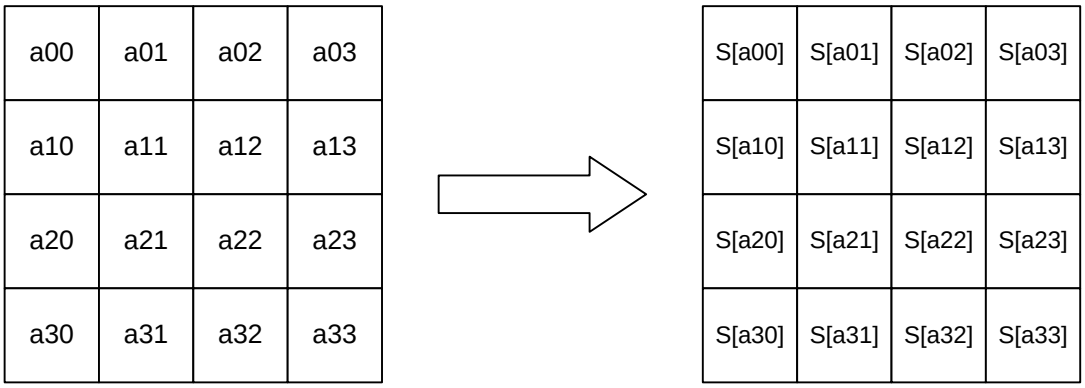


Рис. 6.19. Таблична підстановка 8×8 біт за допомогою однієї таблиці S

Таблична підстановка 8×8 біт виконується за допомогою однієї таблиці S над кожним з 16 байт незалежно. Після підстановки кожний байт розміщується на своє первісне місце у прямокутній матриці (Рис. 6.19). підстановка S має алгоритмічний запис, але у більшості випадків її зручніше зберігати вже обчисленої у вигляді масиви з 256 байт.

Циклічний зсув строк виконує функцію горизонтального розповсюдження змін у блоці, який шифрується. Нульова (сама верхня) строка матриці залишається без змін. Перша циклічно зсувається 1 байт праворуч байт, який був “виштовхнутий” за межі таблиці самий правий байт розміщується на пусте місце у самому початку строки. Друга строка зсувається циклічно праворуч на два байти, а третя (сама нижня) натри байти . Див рис. 6.20. Лінійне перемішування (рис. 6.21) всередині стовпців виконується за допомогою такого математичного апарату. Стовпець представляють у вигляді поліному четвертого ступеню з коефіцієнтами із діапазону 0...255, потім виконується його множення на фіксований поліном $C(x)=3x^3+x^2+x-2$ за модулем полінома (x^4+1). Утворюючим поліномом, який не приводиться розробники вибрали $M(x)=x^8+x^4+x^3+x+1$. Так наприклад, множення двох чисел 65_{16} * $4A_{16}$ буде мати такий вигляд:

$$65_{16} * 4A_{16} = (01100101_2) * (01001010_2) = (x^6 + x^5 + x^2 + 1) + (x^6 + x^3 + x) \bmod (x^8 + x^4 + x^3 + x + 1) =$$
$$= (x^{12} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^7 + x^6 + x^3 + x) \bmod (x^8 + x^4 + x^3 + x + 1) =$$

// коефіцієнти розраховуються за модулем 2, тому x^8, x^6 та x^3 скорочуються

$$= (x^{12} + x^{11} + x^9 + x^7 + x^5 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^7 + x^6 + x^5 + x^2 + x + 1) =$$
$$= (11100111_2) = E7_{16}$$

a00	a01	a02	a03
a10	a11	a12	a13
a20	a21	a22	a23
a30	a31	a32	a33

a00	a01	a02	a03
a13	a10	a11	a12
a22	a23	a20	a21
a31	a32	a33	a30

Рис. 6.20. Циклічний зсув строк

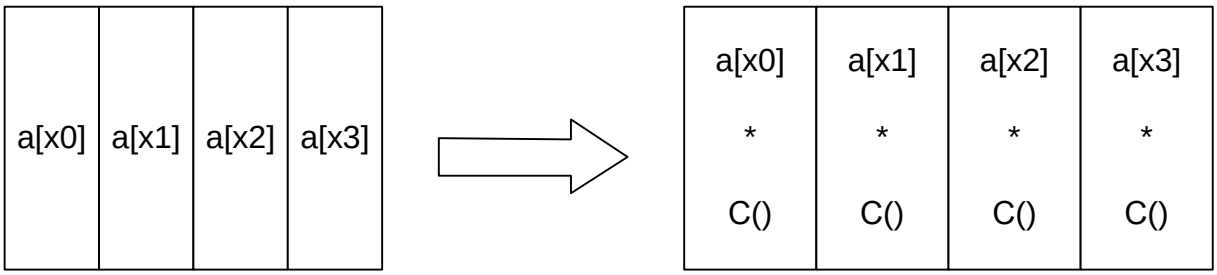


Рис. 6.21. Лінійне перемішування всередині стовпців

Для проведення такого множення на архітектурах з достатнім обсягом ресурсів використовується таблична підстановка, що значно швидше виконання всіх операцій порозрядно на слабких обчислювальних потужностях оптимізованна двох байт виконується за 7 зсувів та максимум 14 операцій XOR (для конкретних "маленьких" коефіцієнтів $C(x)$ які вибрані в Rijndael, потрібно максимум 2 зсува та 4 XOR).

Завдяки властивостям криптопримітивів, які використовуються повну модифікацію одного стовпця у раунді Rijndael EOM, які мають хочаб 4 Кбайта вільної оперативної пам'яті ,можна представити у вигляді чотирьох табличних підстановок $T_0 ... T_3$ розміром 8×32 біта з наступним об'єднанням результатів операцією XOR:

$$A_j^{'} = T0[a[0, j]] \; XOR \; T1[a[1, j-1]] \; XOR$$
$$T2[a[2, j]] \; XOR \; T3[a[3, j-3]] \; XOR \; K[j]$$

У табличній підстановці T „сховані" таблична підстановка S та лінійне перемішування стовпця, вибір коефіцієнтів елементів $a[...]$, які забезпечують циклічні зсуви строк. У результаті виходить дуже ефективна за швидкістю реалізація. При цьому можна відмітити,

що на сучасних процесорах усі 4 Кбайт таблиць T за інтенсивного використання розміщуються у кеші процесора першого рівня.

Дешифрування виконується виконанням у зворотному порядку криптопримітивів, які інверсні до шифруючих. Накладання матеріалу ключа зворотно самому собі. Зсув строк виконується циклічно в зворотній бік. Таблична підстановка S замінюється на інверсну їй S^{-1}. Поліном лінійного перемішування $C(x) = 3x^3 + x^2 + x + 2$ вибрано так, що до нього існує інверсний поліном $D(x) = OB_{16}x^3 + OD_{16}x^2 + O9_{16}x + OE_{16}$, $C(x) \cdot D(x) = 1$.

6.4 Асиметрична криптографія та цифровий підпис.

Підводячи підсумки розгляду симетричної криптографії зазначимо, що якщо користувач бажає конфіденційно вести справу з N партнерами, йому треба мати N секретних ключів, а загальна кількість ключів у системі зростає від кількості абонентів за формулою $N_X(N-1)/2$. Крім того, з'являються питання довіреної доставки ключів абонентам та такої ситуації, коли одержувач, дешифрував повідомлення, може внести в нього зміни, а потім посилатися на документ, начебто вже отриманий в такому вигляді.

Асиметрична ж криптографія вирішує це питання кардинально інакше – по-перше, кількість ключів скорочується до $2 \cdot N$. А симетричну криптографію застосовувати для конфіденційного зберігання інформації на своєму власному твердому диску неможливо.

При асиметричній криптографії кожний абонент інформаційного поля, володіє двома ключами – відкритим (відомий всім іншим абонентам) та закритим (відомий тільки йому та таким, що зберігається у суворій таємниці). Відкритий ключ використовується для відправки повідомлень і з його допомогою на основі спеціального алгоритму будь-хто може провести асиметричне шифрування яке необоротне без знання закритого документа. А ось дешифрувати повідомлення зможе тільки той, хто володіє закритим ключем. Тобто тільки законний одержувач.

Якщо асиметричну схему використовувати навпаки (тобто коли для шифрування задіяно закритий ключ), з невеликими доповненнями породила ще одну величезну галузь сучасної криптографії – електронно цифровий підпис (ЕЦП). Тут користувач обчислює контрольну суму повідомлення, шифрує її таємним ключем та приклеює шифрограму до повідомлення.

Під час створення електронного підпису під документом в неї закладається достатньо інформації, щоб будь який одержувач зміг засвідчитись за допомогою відкритого ключа відправника. Що тільки він міг підписати, як наслідок, відправити це повідомлення.

Але при цьому в підпису повинно бути недостатньо інформації, щоб добути з неї сам таємний ключ відправника. Таким чином технологія ЕЦП дуже нагадує асиметричний шифр тільки навпаки.

Зазначимо, що асиметричне шифрування та ЕЦП вирішують зовсім різні завдання: перше – забезпечення конфіденційності послання, друге – автентичність відправника та цілісність повідомлення. Тому цілком можливо і чисто використовують шифроване повідомлення. а потім його підпис за допомогою ЕЦП.

В основі будь якої схеми асиметричного шифрування або інверсної їй схеми ЕЦП лежить конкретна тяжковирішуєма математична задача. При цьому до даної задачі насправді є спосіб знайти рішення, але для цього треба володіти деякою додатковою інформацією (*trapdoor* - таємні двері).

В якості відкритого ключа в асиметричній криптографії вибирається якесь рівняння, яке і є цією тяжковирішуємою для всіх задачею. Але під час складання цього рівняння може вирішити його так, що особа, яка знає деяку додаткову інформацію про це рівняння може вирішити його за розумний часовий термін. Це дозволяє вибрати так розмір всіх параметрів задачі, що процедури шифрування або, скажемо, підписання документа тривають долі секунди, а на розкриття їх без знання таємного ключа треба десятиріччя.

При асиметричному шифруванні отримувач повідомлення публікує у якості відкритого ключа частину параметрів рівняння, яке тільки він, знаючи закритий ключ, зможе вирішити. Відправник повідомлення дробить повідомлення на блоки потрібної довжини та перетворює їх у великі натуральні числа і тим самим закінчує формування рівняння. У якості шифровки надсилаються деякі параметри рівняння або його значення відносно якогось вектора, чого недостатньо для зловмисника, щоб поновити первісне повідомлення. Але їх достатньо для одержувача, щоб вирішити за допомогою закритого ключа рівняння та відновити доданий відправником параметр, який і є первісним текстом.

Під час формування ЕЦП процес іде дещо у іншому напрямку. Відправник листа додає до листа деяку частину закритого ключа у такому вигляді, щоб за нею неможливо було повністю відновити закритий ключ. Але цієї інформації достатньо, щоб допомогти будь кому бажаючому (тому, хто перевіряє ЕЦП) вирішити те саме рівняння, на базі якого побудована ця схема ЕЦП. У якості інших параметрів рівняння, той хто перевіряє підставляє контрольну суму отриманого листа та значення з відкритого ключа відправника. Якщо рівняння успішно розрішилося, тобто при підстановці всіх даних воно перетворилося у рівність, то це означає, що лист з цією контрольною сумою відправив саме той абонент, чий підпис під ним стоїть. Якщо ж рівність не вийшла. То на якомусь з етапів вийшов збій у каналі зв’язку або ж зловмисне збільшення банківського платежу в десять разів.

З практичних схем асиметричного шифрування найбільш відома схема RSA, яка була винайдена трьома дослідниками (*Ronald Rivest, Adi Shamir, Leonard Adleman*).

Перший етап будь якого асиметричного алгоритму – створення пари ключів для RSA схеми складається з таких операцій:

- вибирають два великих простих (ті, що поділяються на одиницю та самих себе) числа p та q;
- вибирають n. Яке дорівнює $(p \cdot q)$;
- вибирають довільне число $e(e < n)$, таке, що найбільший загальний подільник (НЗП) $(e,(p-1)\cdot(q-1)) = 1$, тобто e повинно бути взаємно простим з числом $(p-1)\cdot(q-1)$;
- методом Евкліда вирішується в цілих числах рівняння $e \cdot d + (p-1)\cdot(q-1)\cdot y = 1$. Тут невідомими є перемінні d та y - а метод Евкліда якраз і знаходить множину пар (d, y), кожна з яких є рішення рівняння у цілих числах;
- пара чисел (e, n) - публікують як відкритий ключ. Число d зберігають у суровій таємниці бо це і є закритий ключ який дозволяє читати всі послання, зашифровані за допомогою пари чисел (e, n).

Другий етап є власно шифрування за допомогою відкритого ключа.

1. Відправник розбиває своє повідомлення на блоки, які дорівнюють $K - [\log_2(n)]$ біт, де квадратні дужки означають взяття цілої частини від дрібного числа. Такий блок може бути інтерпретований як число з діапазону $(0;\ 2^K - 1)$.
2. Для кожного такого числа (назвемо його m_i) обчислюється вираз $C_i = ((m_i)^e) \bmod n$. Блоки c_i і є зашифроване повідомлення.

Їх можна без остраху передавати відкритим каналом. Тому що операція піднесення до степеня за модулем простого числа є тією самою тяжковирішуємою математичною задачею.

Третій етап – дешифрування повідомлення за допомогою таємного ключа. Окремий випадок теореми Ейлера стверджує, що якщо число n представити у вигляді добутку двох простих чисел p та q, то для будь якого X має місце рівність:

$(x^{(p-1)\cdot(q-1)}) \bmod n = 1$.

Для дешифрування RSA - повідомлень скористаємося цією формулою. Піднесемо дві його частини у ступінь $(-y)$: $(x^{(-y)(p-1)(q-1)}) \bmod n = 1^{(-y)} = 1$. Після помноження обох частин рівності на x отримаємо $(x^{(-y)(p-1)(q-1)+1}) \bmod n = 1x = x.$ А тепер нагадаємо, як створювався відкритий та закритий ключі. Величина d була підібрана за допомогою алгоритму Евкліда так, що $e \cdot d + (p-1)(q-1)y = 1$, тобто $e \cdot d = 1 + (-y)(p-1)(q-1)$. Як наслідок, у останньому

виразі ступені на число ($e \cdot d$). Одержимо $(x^{(e \cdot d)}) \bmod n = (x^{(-y)(p-1)(q-1)+1}) \bmod n = 1 \cdot x = x$. Тобто для того, щоб прочитати повідомлення $c_i = ((m_i)^e) \bmod n$, достатньо піднести його до ступеню d за модулем n: $((c_i)^d) \bmod n = ((m_i)^{(e \cdot d)} \bmod n = m_i$. Загальний вигляд системи *RSA* наведено на рис. 6.22.

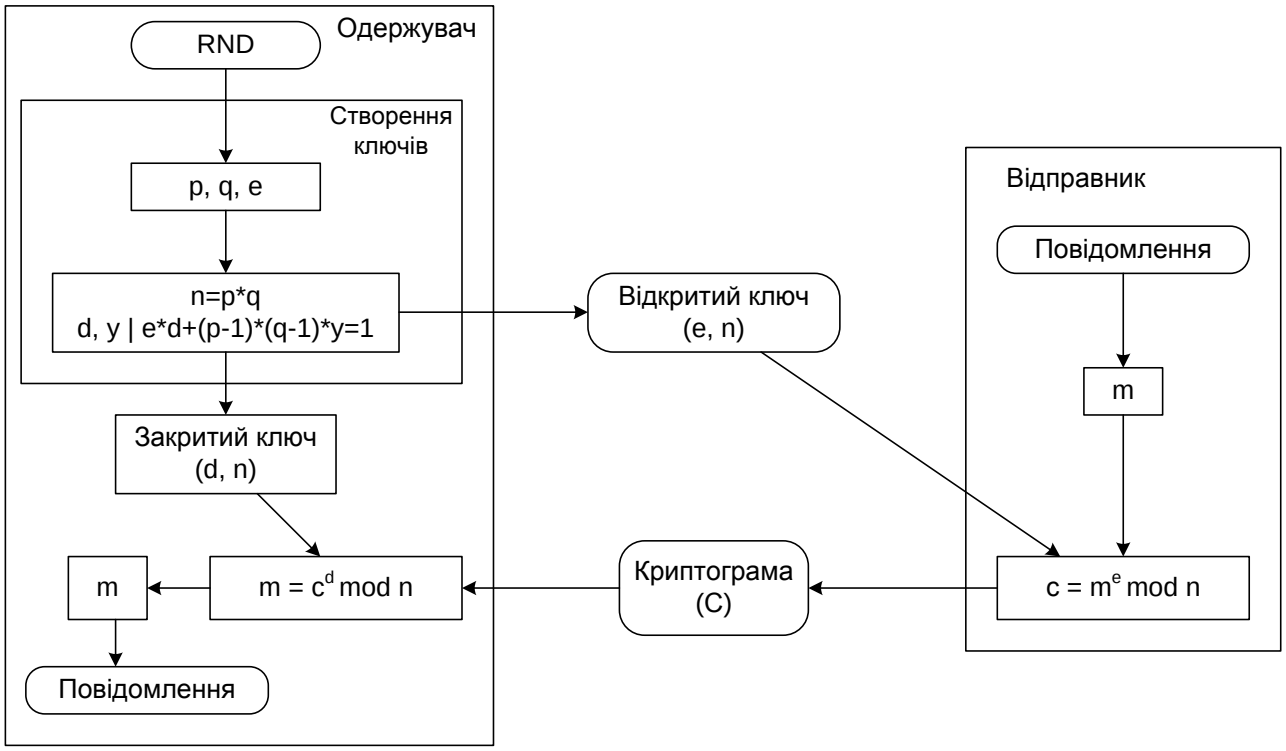


Рис. 6.22. Загальний вигляд системи *RSA*

Слід підкреслити, що двома необхідними властивостями для будь якої асиметричної схеми є:

1. Неможливість прочитати повідомлення, знаючи тільки відкритий ключ.
2. Неможливість вирахувати закритий ключ за відкритим.

Для схеми *RSA* тією самою тяжко вирішуваною математичною задачею, яка стоїть на охороні першої вимоги, є проблема здобуття кореню високих ступіней у кінцевому полі, тобто, знаючи в яку ступінь підносилось число i що отримали в результаті, знайти первісне число дуже важко (звичайні методи здобуття коренів не працюють внаслідок операції $(\bmod n)$, яка застосовувалась над результатом.

Друга вимога виконується виходячи із складності обчислення іншої математичної задачі – розкладання на множники (факторизація) великих чисел. Якби цей процес зайшов в поліноміальний термін, то зловмисник міг би, розклавши на подільники n, обчислити самостійно число $(p-1)(q-1)$ і тим самим, знаючи e, вирахувати секретний ключ d. На щастя, і перша і друга математичні задачі поки що не розрушуються за поліноміальний час. Але, якщо видатні математики вирішать хоча б одну з цих задач, всі криптографічні системи,

які використовують схему RSA будуть зламані за декілька днів. У такій залежності від математики знаходяться всі без винятку схеми асиметричного шифрування та цифрового підпису.

За останній час були виявлені алгоритми злому схеми RSA для деяких її параметрів. Тому, зараз принципи вибору простих чисел p та q - доповнився низкою додаткових досліджень:

- числа $(p+1)$ та $(q+1)$ повинні містити в своєму розкладі на множники великі прості подільники (назвемо їх $p_{\sup}$ та $q_{\sup}$);
- числа $(p-1)$ та $(q-1)$ також повинні містити в своєму розкладі на множники великі прості подільники (назвемо їх $p_{sub}+q_{sub}$), при цьому такі, щоб числа $(p_{sub}-1)$ та $(q_{sub}-1)$ також містили в своєму розкладі досить великі подільники;
- числа p та q повинні дуже близько співпадати за порядком довжини (це природня вимога в плані атаки повним перебором – потенційно зловмисник у цьому випадку першим знайде обов'язково менший подільник, і як наслідок, стійкість всієї схеми залежить від розміру саме меншого подільника). Але небажано, щоб вони виявились поруч один з одним за значенням.
- Таємний ключ d не повинен у результаті процедури створ0ення ключів виявитися дуже маленьким. Якщо така умова випадково виконалась, треба „перевибрати" випадкове число e та повторити процедуру обчислення d;
- Кожен абонент мережі повинен використовувати унікальне значення n. Неприпустимо використання схеми, при якій супервізор ключів роздає абонентам пари e,d, відповідаючи одному й тому ж n, в надії, що абонент не зможе розкласти n на множники без знання p та q. Це не так – за відомими e,d та n останнє розкладається на множники за поліноміальний час. Тобто у будь якого абонента такої мережі з'являється можливість читати повідомлення усіх інших користувачів.

У сучасній криптографії порогом розкриття схеми RSA вважається довжина n в 512 біт. Ця величина знаходиться на „межі довіри". На сьогоднішній день спеціалізований чіп вартістю 10 млн.$ розкриває RSA ключ довжиною 1024 біта за 1 рік, а чип вартістю 10 тис.$ ключ довжиною 512 біт за 10 хвилин.

Далі. Розглянемо приклад роботи схеми RSA на невеликих числах. Зрозуміло, що ніяких додаткових вимог на вибір чисел p та q не висуваємо. Нехай $p=5$ а $q=11$, тоді $n=55$. У якості відкритого ключа e виберемо число 7. таким чином весь відкритий ключ має вигляд $(e=7,n=55)$. Обчислимо закритий ключ d: рівняння $e\cdot d+(p-1)(q-1)y=1$

має вигляд $7d + 40y = 1$ та в цілих числах рішення $d = 23, y = -4 = 51$. Таким чином, закритий ключ є числом 23.

Нехай якийсь відправник бажає передати абоненту комбінацію біт 100111_2, її числовий еквівалент 39_{10}. Підносимо 39 у ступінь відкритого ключа $e = 7$ за модулем $n = 55 : (39^7 \bmod 55) = 19$. Число 19 є шифрограма і воне передається каналом зв'язку. Одержувач після переходу повідомлення підносить його у ступінь $d = 23 : (19^{23} \bmod 55) = 39$. Первісне повідомлення таким чином відновлено.

Інверсія асиметричного алгоритму *RSA* для отримання схеми цифрового підпису є самою простою схемою з усіх алгоритмів ЕЦП. Для формування електронного підпису відправник виконує над контрольною сумою документа h тіж самі дії, що й при шифруванні, але використовує не відкритий ключ одержувача, а свій особистий закритий ключ, тобто $sign_i = (h_i^d \bmod n)$. Відкритий та закритий ключі просто змінюються місцями. На приймальній стороні одержувач підносить підпис у ступінь відкритого ключа d відправника і отримує $(sign_i^e \bmod n) = (h_i^{de} \bmod n) = h_i$ (Згідно тих же формул, що й в асиметричному шифруванні *RSA*). Якщо значення, яке вийшло після піднесення у ступінь співпадає з вирахуваною незалежно на приймальній стороні контрольною сумою документа, то перевірка вважається виконаною, а документ справжнім. Ніхто, крім відправника . не знаючи d, не може вирахувати такий підпис $sign_i$, щоб піднесення його в ступінь відкритого ключа e дало потрібну контрольну суму – це такаж сама тяжковирішувальна задача, що й в асиметричному шифруванні *RSA*. Тобто, спорядити документ таким підписом $sign_i$ міг тільки дійсний Володар закритого ключа. Схема ЕЦП наведена на рис. 6.23.

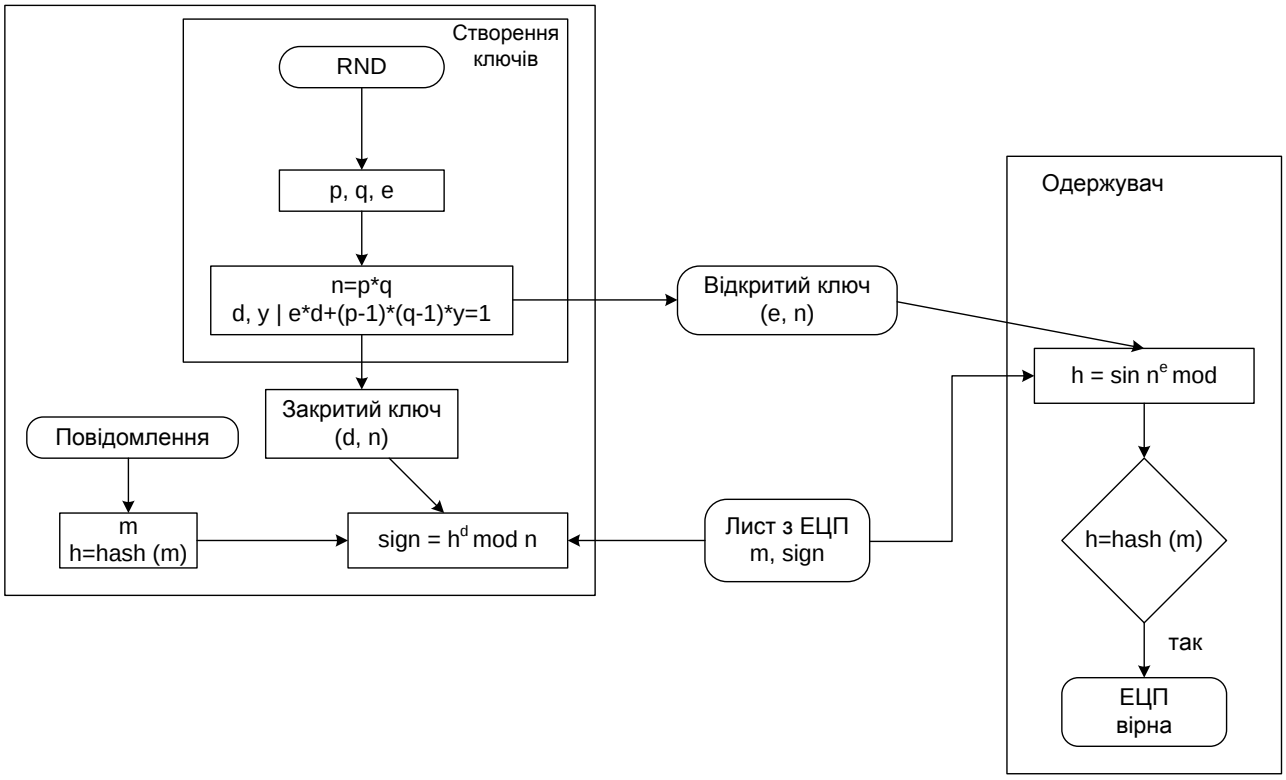


Рис. 6.23. Схема ЕЦП

Використання таємного ключа для цифрового підпису, тобто розкриття деякої інформації про нього не зашкодить йому. Навіть перехопивши велику кількість підписаних повідомлень, зловмисник не зможе з їх допомогою вирахувати d за поліноміальний час, а довжини ключа, який застосовується на цей час вистачить на декілька десятків років стійкості.

І все таки при користування ЕЦП, треба дотримуватися деяких правил: наприклад, ніколи не підписувати того, що не створював сам, а прийнято за правило підписувати тільки контрольну суму свого повідомлення, навіть якщо все воно таке мале, що розміщується в один блок перетворень RSA. При цьому для таких цілей завжди використовуються тільки крипостійкі (необоротні) контрольні суми – так звані ХЕШ-функції. Вони не дають зловмиснику можливості сформувати документ так, щоб його контрольна сума співпала з бажаним значенням (u).

Необхідно пам’ятати, що процедури ассиметричного шифрування дуже повільні. Цей нодоліек, щоправда успішно може бути подолано Об’єднанням асиметричного шифрування з блочними штифтами. Звичайно весь текст повідомлення перетворюється звичайним блочним шифром, але використанням випадкового, тільки що створеного ключа сеанса, а ось сам ключ сеансу шифрується як раз асиметричним алегоритмом за допомогою відкритого ключа одержувача та розміщюється на початок шифрограми.

Серед найбільш відомих практичних схем асиметричного шифрування є схема RSA, яку розробили в 1978 році Рональд Рівестом, Аді Шамір та Леонард Адельман. А також схеми ним Рабіна, Ель Гамальта та Марка Еліса.

Питання для самоперевірки

1. Що стало революційним кроком у розвитку криптографії?
2. Наведіть узагальнену схему класифікації шифрів.
3. ЩО таке абсолютна практична стійкість шифрів?
4. Назвіть рекомендовану довжину ключів для комерційних та державних потреб.
5. Яка характерна риса поточних шифрів.
6. Що використовується у якості бази при побудові поточних шифрів?
7. Яка відмінна риса існує при побудові блочних шифрів?
8. Які перетворення застосовуються у блочному шифруванні?
9. Що є однією з найбільш розповсюджених схем блочних шифрів?
10. Що є основою стандарту шифрування DES?
11. Назвіть характерні особливості шифру, створеного за ГОСТ 28147-89
12. Який алгоритм став переможцем конкурсу ASE у 2000 РОЦІ?
13. Яка характерна особливість асиметричного шифрування?
14. В чому різниця між асиметричним шифруванням та електро-цифровим підписом?
15. Назвіть практичні схеми асиметричного шифрування.

Розділ 7. Методи закриття мовних сигналів

7.1. Загальні положення

Найбільш радикальним заходом запобігання підслуховування телефонних розмов є використання криптографічних методів захисту. Перші технічні системи захисту почали розроблятися зразу після винайдення телефону.

Головною метою при розробці систем передачі мови є збереження тих її характеристик, що найбільш важливі для сприйняття слухачем.

Безпека зв'язку при передачі мовних повідомлень ґрунтується на використанні великої кількості різних методів закриття повідомлень, що змінюють характеристики мови таким чином, що вона стає нерозбірливою і невпізнаною для зловмисників, які підслуховують або перехватили закрите мовне повідомлення. Вибір методів закриття залежить від виду конкретного застосування і технічних характеристик каналу передачі.

У мовних системах зв'язку відомі два основних методи закриття мовних сигналів, що розділяються за способом передачі каналом зв'язку: аналогове скремблювання і дискретизація мови з наступним шифруванням [13].

Кожний з цих двох методів має свої переваги і недоліки. Так, наприклад, у перших двох системах, представлених на рис7.1 (А і В), у каналі зв'язку при передачі присутні фрагменти вихідного, відкритого мовного повідомлення, перетворені в частотній і/чи часовій областях. Це означає, що ці системи можуть бути атаковані криптоаналітиком супротивника на рівні аналізу звукових сигналів. Тому раніше вважалося, що поряд з високою якістю і розбірливістю відновленої мови аналогові скремблери можуть забезпечити лише низьку чи середню, у порівнянні із системами цифрового кодування і шифрування, ступінь закриття (таємності) [13]. Однак новітні (розроблені в останні роки) алгоритми здатні забезпечити не тільки середній, але іноді і дуже високий рівень таємності в системах типу В (див. рис.7.1) [13].

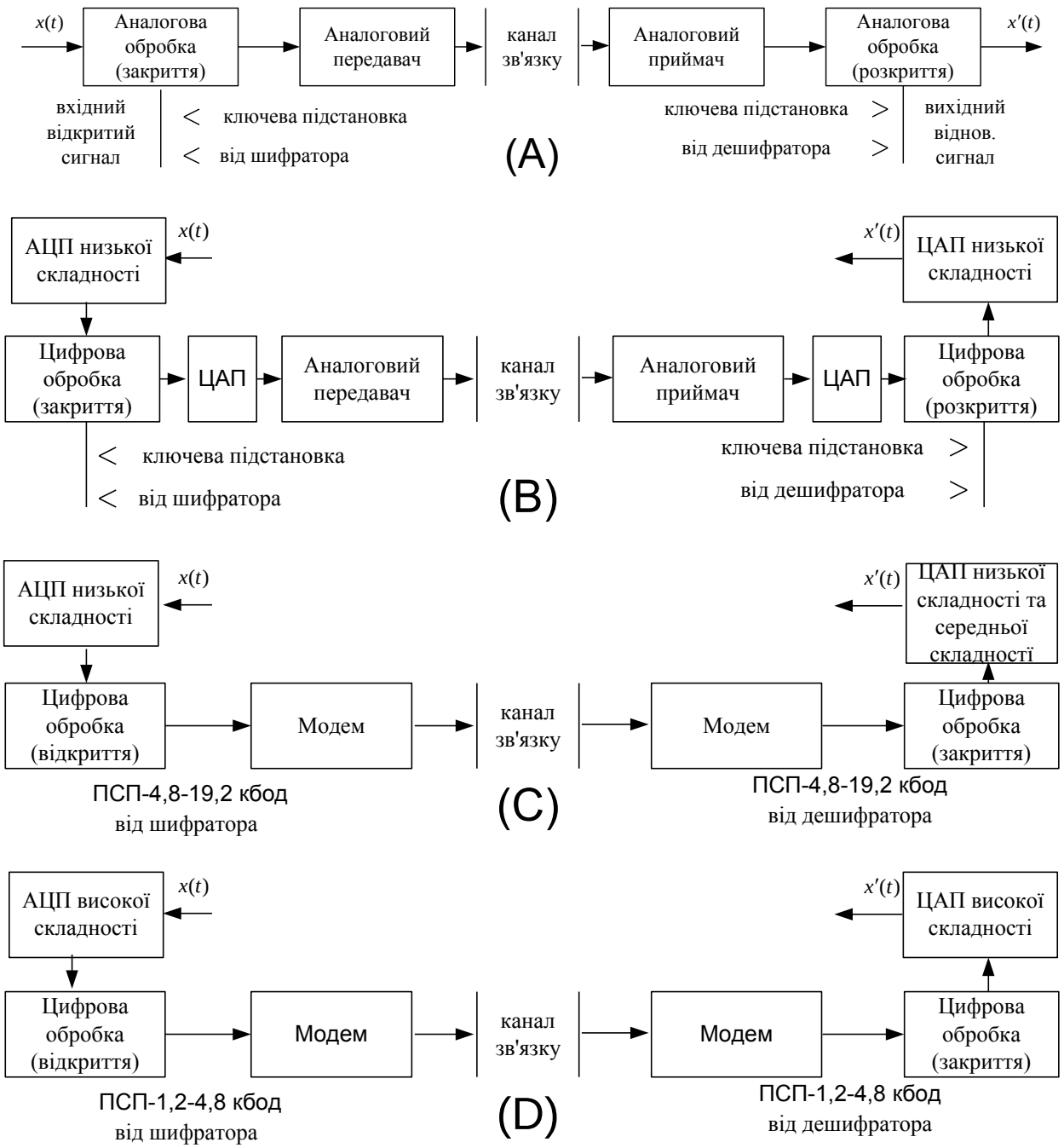


Рис.7.1. Види систем закриття мови

АЦП/ЦАП - аналогово-цифрове/цифро-аналогове перетворення; ПСП - псевдовипадкова послідовність.

Аналогові скремблери: мовні скремблери найпростіших типів на базі часових і/чи частотних перестановок відрізків мови (A); комбіновані мовні скремблери на основі частотно-часових перестановок відрізків мови, представлених дискретними відліками, із застосуванням цифрової обробки сигналів (B).

Цифрові системи закриття мови: широкосмугові (B) і вузькосмугові (D). Системи типу C і D не передають якої-небудь частини вхідного мовного сигналу. Мовні компоненти кодуються в цифровий потік даних, що змішується з псевдовипадковою послідовністю, що

формуються ключовим генератором по одному з криптографічних алгоритмів, і отримане в такий спосіб закрите мовне повідомлення передається за допомогою модему в канал зв'язку, на приймальній кінці якого здійснюються зворотні перетворення з метою одержання відкритого мовного сигналу.

Технологія виготовлення широкосмугові систем закриття мови типу (С) добре відома, не представляє особливих труднощів технічна реалізація використовуваних для цих цілей способів кодування мови типу АДІКМ (адаптивної диференціальної імпульсно-кодової модуляції), ДМ (дельта-модуляції) і т.п. Але представлена такими способами дискретизована мова може передаватися лише по спеціально виділеним широкосмугові каналам зв'язку зі смугою пропускання, що звичайно лежить у діапазоні 4.8-19.2 кГц, і не придатна для передачі по лініях телефонної мережі загального користування [13], де необхідна швидкість передачі даних повинна складати 2400 біт/с. У таких випадках використовуються вузькосмугові системи закриття типу D, головними труднощами при реалізації яких є висока складність алгоритмів стискання мовних сигналів, здійснюваних у вокодерних пристроях.

За допомогою дискретного кодування мови з наступним шифруванням завжди досягався високий ступінь закриття, але в минулому цей метод не знаходив широкого поширення в повсюдно наявних вузькосмугові каналах зв'язку через низьку якість відновлення переданої мови.

Останні досягнення в розвитку низькошвидкісних дискретних кодерів дозволили значно поліпшити якість мови без зниження надійності закриття.

Кажучи про рівень, чи ступень таємності систем закриття мови, слід зазначити, що ці поняття дуже умовні. До цього часу не вироблено на цей рахунок чітких чи стандартів правил. Однак у ряді джерел [13] основні рівні захисту визначають як тактичний і стратегічний, що в деякому змісті перегукується з поняттями практичної і теоретичної стійкості криптографічних систем закриття даних:

- тактичний, чи низький, рівень використовується для захисту інформації від підслуховування сторонніми особами на період часу, вимірюваний, хвилинами або днями. Існує велика кількість простих методів, здатних забезпечити такий рівень захисту при прийнятній вартості;

- стратегічний, чи високий, рівень захисту інформації від перехоплення використовується в ситуаціях, які припускають, що висококваліфікованому, технічно добре оснащеному фахівцю буде потрібно для дешифрування перехопленого повідомлення період часу від декількох місяців до багатьох і багатьох років.

Часто використовується і поняття середнього ступеня захисту, що займає проміжне положення між тактичним і стратегічним рівнем закриття.

7.2. Аналогове скремблювання

Найбільша частина апаратури засекречування мовних сигналів використовує в даний час метод аналогового скремблювання [13], оскільки, по-перше, це дешевше, по-друге, ця апаратура застосовується в більшості випадків у стандартних телефонних каналах зі смугою 3 кГц, по-третє, забезпечується комерційна якість дешифрованої мови і, по-четверте, гарантується досить висока стійкість закриття.

Аналогові скремблери перетворять вихідний мовний сигнал за допомогою зміни його амплітудних, частотних і часових параметрів у різних комбінаціях. Скрембльований сигнал може потім бути переданий по каналі зв'язку в тій же смузі частот, як і вхідний, відкритий. В апаратах такого типу використовується один чи кілька принципів аналогового скремблювання [13] з числа перерахованих нижче:

1) скремблювання в частотній області: частотна інверсія (перетворення спектра сигналу за допомогою гетеродина і фільтра), частотна інверсія і зсув (частотна інверсія з мінливим стрибкоподібно зсувом несучої частоти), поділ смуги частот мовного сигналу на ряд піддіапазонів з наступною їхньою перестановкою й інверсією;

2) скремблювання в часовій області (розбивка блоків або частин мови на сегменти з перемішуванням їх у часі з наступним прямим і/чи реверсивним зчитуванням);

3) комбінація часового і частотного скремблювання.

Як правило, усі перестановки яким-небудь чином виділених сегментів або ділянок мови в часовій і/чи в частотної областях здійснюються за законом псевдовипадкової послідовності, вироблюваної шифратором на ключі, що міняється від одного мовного повідомлення до іншого [13].

Методи мовного скремблювання вперше з'явилися під час другої світової війни. Серед останніх досягнень у цій області слід зазначити широке використання інтегральних схем, мікропроцесорів і процесорів цифрової обробки сигналів (ЦПОС). Усе це забезпечило високу надійність пристроїв закриття мови зі зменшенням їхнього розміру і вартості.

Аналоговим скремблерам удалося уникнути багатьох труднощів, зв'язаних з передачею мовного сигналу і/чи його параметрів, властивим цифровим системам закриття мови, і в теж час досягти значеного рівня розвитку, що забезпечує середню і навіть високий ступінь захисту мовних повідомлень. Оскільки скрембльовані мовні сигнали в аналоговій формі лежать у тій же смузі частот, що і вхідні відкриті, це означає, що їх можна передавати по звичайним комерційним каналам зв'язку, які використовуються для передачі мови, без вимоги якого-небудь спеціального обслуговування, такого, як, наприклад, модеми. Тому пристрої мовного скремблювання не такі дорогі і значно менш складні, ніж пристрої дискретизації з наступним цифровим шифруванням.

Аналогові скремблери, по їхньому режиму роботи, можна розбити на два наступних класи [13]:

1) статичні системи, схема кодування яких залишається незмінною протягом усієї передачі мовного повідомлення;

2) динамічні системи, що постійно генерують кодові підстановки в ході передачі (код може бути змінений у процесі передачі кілька разів протягом кожної секунди).

Очевидно, що динамічні системи забезпечують більш високий ступінь захисту, оскільки різко обмежують можливість легкого прослуховування переговорів сторонніми особами.

Процес аналогового скремблювання являє собою складне перетворення мовного сигналу з його наступним відновленням (зі збереженням розбірливості мови) після проходження перетвореного сигналу по вузькосмугових каналу зв'язку, підданому впливу шумів.

Можливе перетворення мовного сигналу по трьох параметрах: амплітуді, частоті і часу. Вважається, що використовувати амплітуду недоцільно, тому що змінення в часі загасання каналу і відношення сигнал/шум роблять надзвичайно складним точне відновлення амплітуди переданого сигналу. Практичне застосування одержало тільки частотне і часове скремблювання і їхні комбінації. Як вторинні ступіні скремблювання в цих системах можуть використовуватися обмежені види амплітудного скремблювання [13].

Як уже відзначалося вище, існує два основних види частотних скремблерів -інверсний і смуговий. Обоє засновані на перетвореннях спектра вхідного мовного сигналу для приховання переданої інформації і відновленні отриманого мовного повідомлення шляхом зворотних перетворень.

Інверсний скремблер здійснює перетворення мовного спектра, тотожне повороту частотної смуги мовного сигналу навколо деякої середньої точки (рис. 7.2). При цьому досягається ефект перетворення низьких частот у високі частоти, і навпаки.

Даний спосіб забезпечує невисокий рівень закриття, тому що при перехопленні легко встановлюється величина частоти, що відповідає середній точці інверсії в смузі спектра мовного сигналу.

Деяке підвищення рівня закриття забезпечує смуго-здвиговий інвертор, що здійснює поділ смуги на дві субсмуги, при цьому точка розбивки виступає в ролі деякого ключа системи [13]. Надалі кожна субсмуга інвертується навколо своєї середньої частоти. Цей вид скремблювання, однак, також занадто простий для розкриття при перехопленні і не забезпечує надійного закриття. Підвищити рівень закриття можна шляхом зміни за деяким законом частоти, що відповідає точці розбивки смуги мовного сигналу (ключа системи) [13].

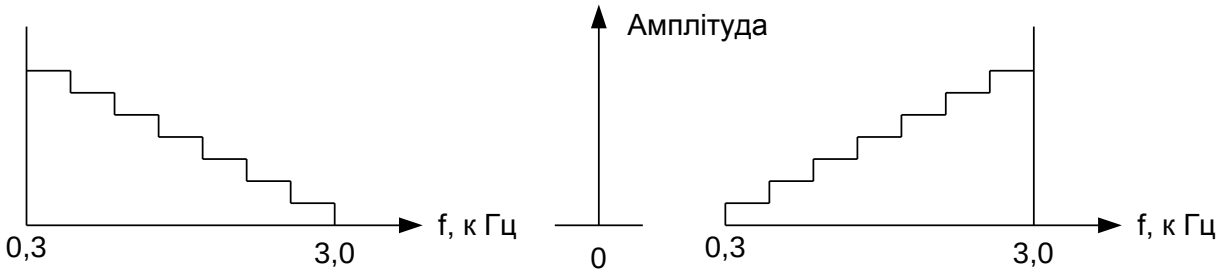


Рис. 7.2. Принцип роботи інвертора спектра мови

Мовний спектр можна також розділити на кілька частотних смуг рівної ширини і зробити їхнє перемішування й інверсію за деяким правилом (ключ системи). Так функціонує смуговий скремблер (рис. 7.3).

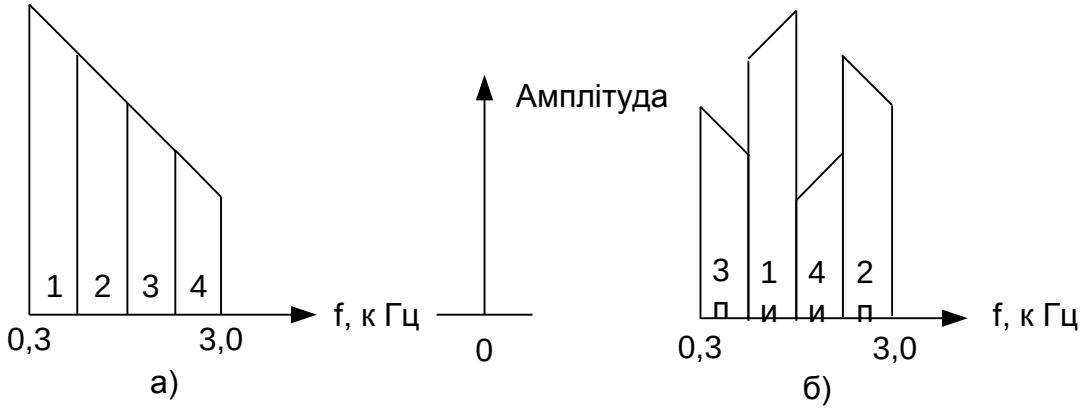


Рис.7.3. Принцип роботи 4-х смугового скремблера мови

Часові скремблери засновані на двох основних способах закриття: інверсії за часом сегментів мови і їхній часовій перестановці [13]. У порівнянні з частотними скремблерами затримка в часових скремблерів набагато більше, але існують різні методи її зменшення.

У скремблерах з часовою інверсією мовний сигнал поділяється на послідовність часових сегментів і кожний з них передається інверсно в часі - з кінця [13]. Такі скремблери забезпечують обмежений рівень закриття, що залежить від тривалості сегментів. Відомо, що для досягнення розбірливості повільної мови необхідно, щоб довжина сегмента складала близько 250 мс. Це означає, що затримка системи буде дорівнює приблизно 500 мс, що може виявитися неприйнятним для деяких додатків.

Для підвищення рівня закриття застосовують перестановки часових відрізків мовного сигналу в межах фіксованого кадру (рис. 7.4). Правило перестановок є ключем системи, зміною якого можна істотно підвищити ступінь закриття мови. Залишкова розбірливість залежить від тривалості відрізків сигналу і кадру і зі збільшенням останнього зменшується [13].

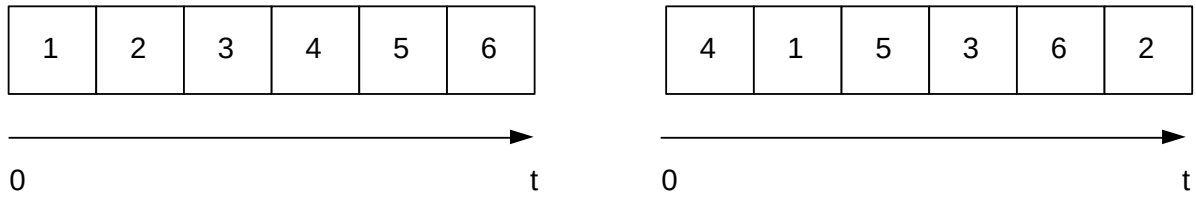


Рис. 7.4. Схема роботи часового скремблера з перестановками у фіксованому кадрі

Головним недоліком скремблера з фіксованим кадром є велике значення часу затримки системи, яка дорівнює подвоєній тривалості кадру [13]. Цей недолік усувається в скремблеру з перестановкою часових відрізків мовного сигналу з ковзним вікном. У ньому число комбінацій можливих перестановок обмежено таким чином, що затримка будь-якого відрізка не перевершує встановленого максимального значення. Кожен відрізок вихідного мовного сигналу як би має часове вікно, усередині якого він може займати довільне місце при скремблюванні. Це вікно сковзає в часі в міру надходження в нього кожного нового відрізка сигналу. Затримка при цьому знижується до тривалості вікна [13].

Використовуючи комбінацію часового і частотного скремблювання, можна значно підвищити ступінь закриття мови. Комбінований скремблер набагато складніше звичайного і вимагає компромісного рішення на вибір рівня закриття, залишкової розбірливості, часу затримки, складності системи і ступеня спотворень у відновленому сигналі [13]. Кількість же всіляких систем, що працюють по такому принципі, обмежено лише людською уявою. В [13] представлені різні варіанти комбінованих скремблерів на основі частотно-часових перестановок.

Як приклад такої системи розглянемо скремблер, схема якого представлена на рис. 7.5, де операція частотно-часових перестановок дискретизованих відрізків мовного сигналу здійснюється за допомогою чотирьох процесорів цифрової обробки сигналів, один із яких може реалізовувати функцію генератора випадкової послідовності (ключа системи закриття).

Зміна ключа системи дозволяє підвищити ступінь закриття, але вимагає введення синхронізації на прийомній стороні системи. Основна частина енергії мовного сигналу зосереджена в невеликій області низькочастотного спектра (від 300 до 3500 Гц), тому вибір варіантів перемішування обмежений, і багато систем характеризуються відносно високою залишковою розбірливістю [13].

Істотне підвищення ступеня закриття мови може бути досягнуте шляхом реалізації в смуговому скремблері швидкого перетворення Фур'є (ШПФ). При цьому кількість припустимих перемішувань частотних смуг значно збільшується, що забезпечує високий ступінь закриття без погіршення якості мови. Можна додатково підвищити ступінь закриття шляхом здійснення затримок різних частотних компонентів сигналу на різну величину. Приклад реалізації такої системи показаний на рис. 7.6. [13].

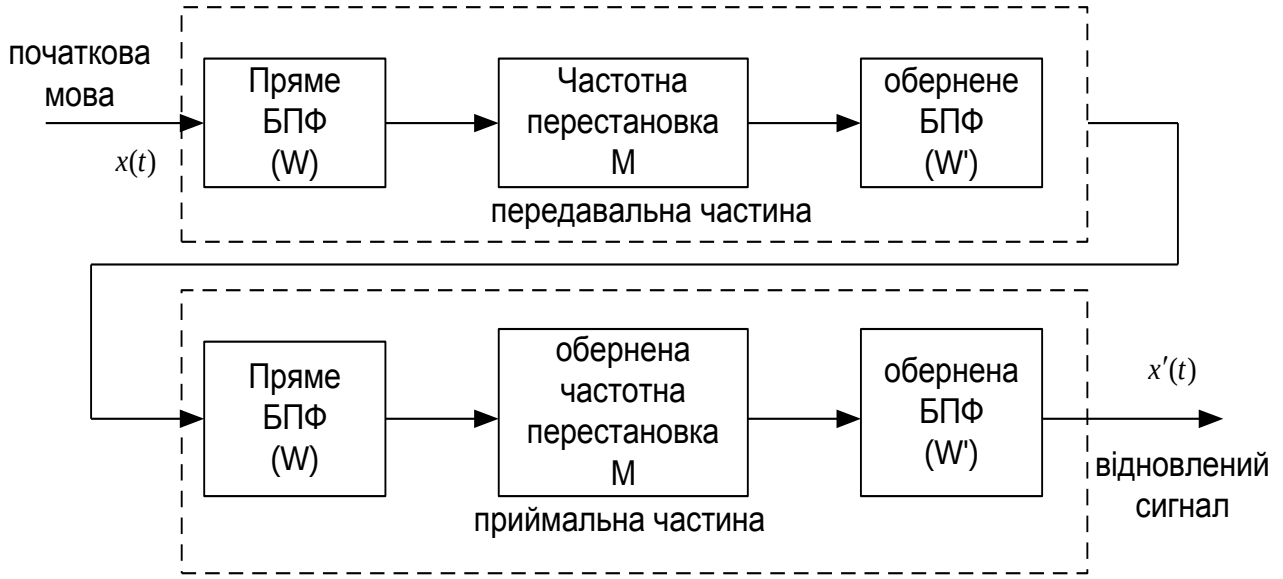


Рис. 7.6. Основна форма реалізації аналогового скремблера на основі ШПФ

Головним недоліком виконання ШПФ є виникнення в системі великої затримки сигналу (до 300 мс) [13], яка обумовлена використанням вагових функцій. Це значно ускладнює застосування таких пристроїв у дуплексних системах зв‘язку.

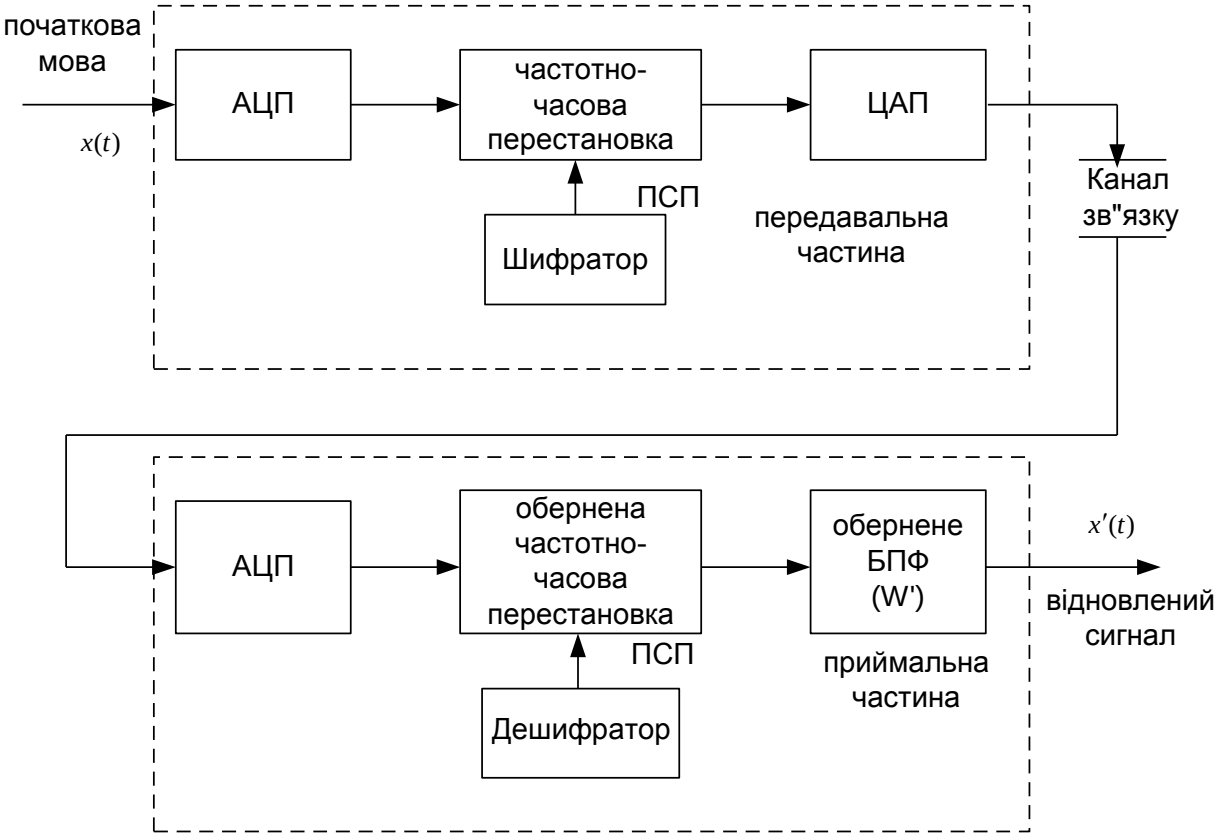


Рис. 7.5. Блок-схема комбінованого скремблера. (ПСП - псевдовипадкова послідовність)

У такому скремблері спектр оцифрованого аналогово-цифровим перетворювачем (АЦП) мовного сигналу розбивається за допомогою використання алгоритмів цифрової обробки сигналів на частотно-часові елементи, що потім перемішуються на частотно-часовій

площині відповідно до одного із криптографічних алгоритмів (Рис. 7.7) і додаються, не виходячи за межі частотного діапазону вихідного сигналу.

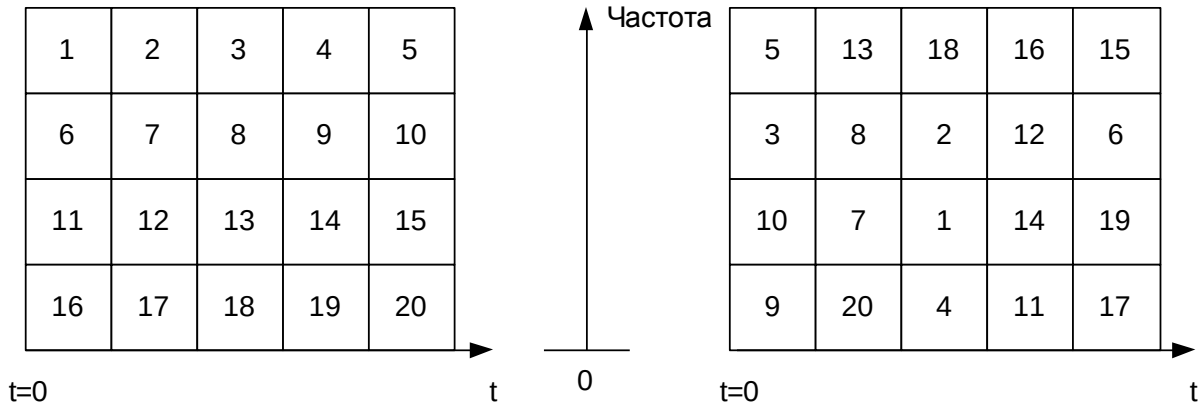


Рис. 7.7. Принцип роботи комбінованого скремблера

У представленій в [13] системі закриття мови використовуються чотири процесори цифрової обробки сигналів. Кількість частотних смуг спектра, в яких виробляються перестановки з можливою інверсією спектра, - чотири. Максимальна затримка частотно-часового елемента за часом дорівнює п'яти. Отриманий у такий спосіб закритий сигнал за допомогою цифро-аналогового перетворювача (ЦАП) переводиться в аналогову форму і подається в канал зв'язку. На прийомному кінці виробляються зворотні операції по відновленню отриманого закритого мовного повідомлення. Стійкість представленого алгоритму порівнянна зі стійкістю систем цифрового закриття мови.

Далі розглянемо особливості застосування аналогових скремблерів у системах радіозв‘язку. Як відомо, скремблери всіх типів, за винятком найпростішого (з частотною інверсією), вносять спотворення у відновлений мовний сигнал. Границі часових сегментів порушують цілісність сигналу, що неминуче приводить до появи позасмугових складових. Небажаний вплив роблять і групові затримки складових мовного сигналу в каналі зв'язку. Результатом спотворень є збільшення мінімально припустимого відношення сигнал/шум, при якому може здійснюватися надійний зв'язок.

Однак, незважаючи на зазначені проблеми, методи часового і частотного скремблювання, а також комбіновані методи успішно використовуються в комерційних каналах радіозв'язку для захисту конфіденційної інформації.Особливість засобів радіозв'язку, на відміну від приведених вище, полягає в їх <ефірній оголеності>поширенні на досить великі відстані. Це ще більш полегшує процедуру прослуховування: одержати доступ до радіоканалу незрівнянно простіше, ніж наблизитися до оптоволоконного кабелю, що лежить у коробах на глибині декількох метрів під землею. Таким чином, знімання інформації з ефіру є один з основних способів для осіб, що займаються промисловим шпигунством, тому що це не вимагає фізичної присутності поблизу джерела або одержувача повідомлення. В

даний момент індустрія виробництва засобів радіозв'язку прагне до того, щоб цілком перейти на виробництво цифрового обладнання. Але частка аналогового на ринку усе ще значна. Крім того, потрібно враховувати і те, що багато вітчизняних організацій на 90 % використовують аналогові пристрої. Так, силові структури, структури безпеки, охорони й інші подібні їм державні установи широко застосовують професійне устаткування з фазовою чи частотною модуляцією. Ці радіосигнали є аналоговими і, відповідно, можуть бути легко прослухані. Тому питання захисту інформації, переданої по аналогових каналах зв'язку, для України надзвичайно актуальним, і цю задачу необхідно вирішувати. Ця необхідність не є чимось нездійсненним. У таких ситуаціях використовують скремблер - один з найбільш популярних пристроїв **захисту** радіопереговорів від прослуховування при використанні аналогового радіоустаткування. Скремблери для радіостанцій виробляються багатьма фірмами; серед них -Transcrypt International, Communico, MX COM, MIDIAN, Selectone, а також фірми, що роблять радіотермінали. Розглянемо деякі найбільше часто використовувані методи перетворень низькочастотного сигналу в малогабаритних аналогових скремблерах.

Мовний спектр, переданий по радіоканалу, знаходиться в діапазоні 300-3000 Гц**.** Спад амплітудно-частотної характеристики (АЧХ) обумовлений тим, що найбільша потужність сигналу знаходиться в низькочастотній частині спектра. Такий сигнал надходить у частотний інвертор спектра скремблера, де низькочастотні складові мовного сигналу перетворюються у високочастотні і навпаки. У результаті інверсний сигнал займає ту ж смугу частот, що і вихідний.Розворот спектра в цьому випадку відбувається щодо несущої частоти, що може бути фіксованою в простих скремблерах чи змінювати своє значення в часі плавно або стрибками в більш складних. Фіксована частота або її зміна є ключем системи. У таких скремблерах кількість частот інверсії може бути від 1 до 16. Це дає можливість поділу абонентів по групах. Однократна частотна інверсія сигналу є найпростішим видом аналогового скремблювання і забезпечує найнижчу криптографічну стійкість. При закритті радіосигналу за допомогою одиночної частотної інверсії нескладно розібрати (користаючись звичайним приймачем) майже до половини мовної інформації в залежності від темпу мови, теми розмов. Наприклад, цілком прослухати такий сигнал можна, маючи радіостанцію з убудованим інвертором частоти або спеціалізований радіоприймач-сканер (наприклад, AR-16 японської фірми AOR LTD). Достоїнством цього методу є дуже якісне відновлення інверсного (отриманого з ефіру) сигналу. Крім того, вартість таких пристроїв невисока. Широку гаму інверсних скремблерів ще здавна представляла компанія Midian (серії VPU-1, VPU-2, VPU-8). Найбільш відомі моделі однократної інверсії - ST-20, ST-022 (Selectone), SC20-400 (Transcrypt International).

Використовується також частотна інверсія двох і більш піддіапазонів мовного спектра. Спочатку смуга всього мовного спектра поділяється на частотні піддіапазони (у

більшості випадків на два), що потім інвертуються . Ключем цієї системи є частота розбивки спектра сигналу. Ці скремблери, на відміну від моделей, що використовують однократну частотну інверсію, трохи підвищують рівень захищеності інформації.

Для значного підвищення рівня закриття інформації застосовують динамічні скремблери. У динамічних скремблерах, на відміну від статичних, параметри перетворення мовного сигналу змінюються в часі, відповідно ці типи скремблерів вимагають синхронізації передавальних і прийомних сторін. У залежності від типу скремблера синхронізація може передаватися як на початку повідомлення, так і під час його передачі. Англійська фірма Pentone представляє скремблер SCR1 з частотною інверсією двох поддиапазонов. Подібний пристрій робить і вітчизняна компанія <Мікро Радіо> - модель KMR-1. Ці типи скремблерів можуть бути як статичними, так і динамічними.

Існують також скремблери в яких використовується безперервна зміна несущої частоти мовного сигналу під час усієї розмови. Несуща частота змінюється в часі по пилкоподібній траєкторії**.** У більшості таких скремблерів синхронізація параметрів зміни частоти присутня протягом усього часу розмови. Тому що ця синхронізація передається одночасно з мовним сигналом, то відновлений сигнал виходить не дуже високої якості. Однак при звичайному прослуховуванні цей метод робить мову цілком невпізнанною.

На ринку використовують скремблери як з повільним хитним кодом - VPU-10A, VPU-10B (Midian), так і зі швидким -ST-25, ST-26 (Selectone), SC20-440, SC20-450 (Transcrypt International).

В деких скремблерах використовується стрибкоподібна зміна частоти інверсії. Частота в цьому випадку змінюється псевдовипадковим чином, стрибкоподібно. Закономірність зміни повинна бути однаковою як у пристрої, що шифрує, так і в тому, що дешифрує. У більшості таких пристроїв у переданому сигналі присутній початковий синхронізуючий пакет, у якому міститься алгоритм зміни частоти інверсії для прийомної сторони. У більш складних динамічних скремблерах для підвищення рівня захисту переданої інформації такий алгоритм може змінюватися при кожному наступному встановленні сеансу зв'язку. Мовний сигнал у випадку використання цього типу скремблерів, на відміну від простого статичного, втрачає свою цілісність. У залежності від моделі скремблера частота інверсії може мінятися від 1 до 1000 разів у секунду. Чим більше кількість змін у секунду, тим вище рівень захисту інформації, але, як наслідок, нижче якість відновленого сигналу.

Недолік більшості скремблерів зі стрибкоподібною зміною частоти інверсії в тім, що для передачі синхронізуючого пакета оператор змушений у початковий момент робити паузу. У випадку зв'язку через ретранслятор радіостанція з таким скремблером не завжди може надійно з'єднуватися з іншою радіостанцією. Справа в тім, що в ретрансляторах існує так звана прозорість (нелінійність звукових трактів), внаслідок чого первісний пакет,

проходячи через тракти ретранслятора, може спотворитися. Для підвищення надійності такого з'єднання необхідно збільшити тривалість передачі первісного пакета (іноді до 1 с), що може створювати значні незручності.

Перевага таких скремблерів полягає в тім, що у випадку досить швидкої зміни частоти інверсії (наприклад, 800-1000 разів/с) вони мають відносно високий рівень захисту переданої інформації. Наприклад, якщо швидкість зміни складає один раз у секунду, то 40-60 % інформації можна прослухати дуже простим технічним методом. Широку серію скремблерів, що використовують стрибкоподібну зміну частоти інверсії,робить фірма Transcrypt International. Розповсюджені серії - 410 (зміна частоти інверсії 1 раз/с), 430 (300 разів/с), 460 (1000 разів/с), 480 (800 разів/с). Наведемо приклади принципових схем аналогових скремблерів.

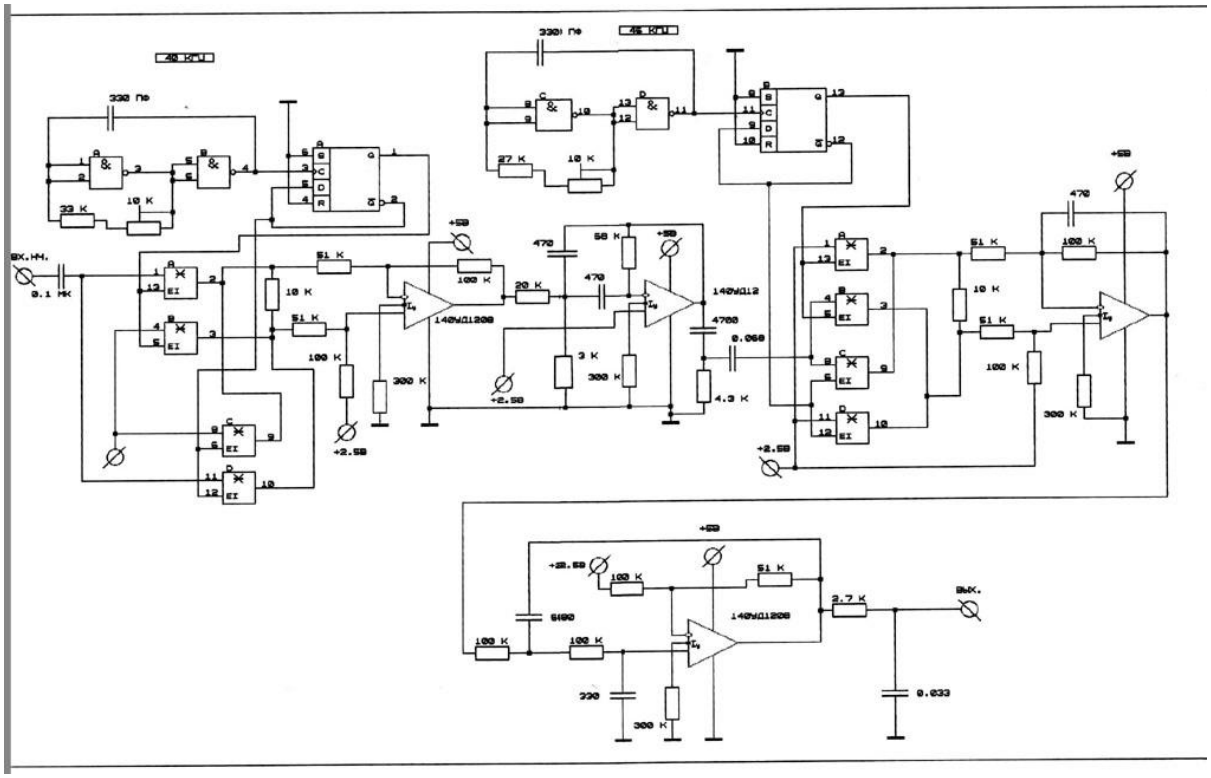


Рис. 7.8. Схема перетворювача спектру мовного сигналу

Схема призначена для зрушення або інверсії спектра мовного сигналу (частоти 300 - 3000 Гц). Після такого перетворення можна змінити тембр чи голосу зробити мова цілком нерозбірливої. .

Принцип роботи: Для перетворення використовується принцип односмугової модуляції. Вхідний сигнал надходить на балансовий модулятор, керований частотою 20 кгц. Схема модулятора складається з ОП 140УД1208 і 4-х аналогових ключів (м.сх 561КТ3) .На виході модулятора маємо спектр із 2-х бічних смуг, розташованих симетрично відносно 20 кГц . Також на виході присутній вихідний НЧ сигнал. Для подальшої обробки використовується тільки верхня бічна смуга. Вона виділяється смуговим фільтром на ОП

140УД1208, потім відбувається додаткова фільтрація за допомогою ФВЧ. Отримана верхня бічна смуга надходить на другий балансовий модулятор (у даному випадку це детектор). Його схема аналогічна схемі першого модулятора, а тактова частота 23 кГц. Після перетворення вихідний сигнал фільтрується за допомогою ФНЧ. Тому що в даній схемі частота другого перетворювача знаходиться вище, ніж верхня границя верхньої бічної смуги, то на виході маємо мовний сигнал з інвертованим спектром. Якщо вибрати частоту тактування другого перетворювача в межах 17-21 кГц, то можна одержати мовний сигнал зі зміненим тембром голосу.

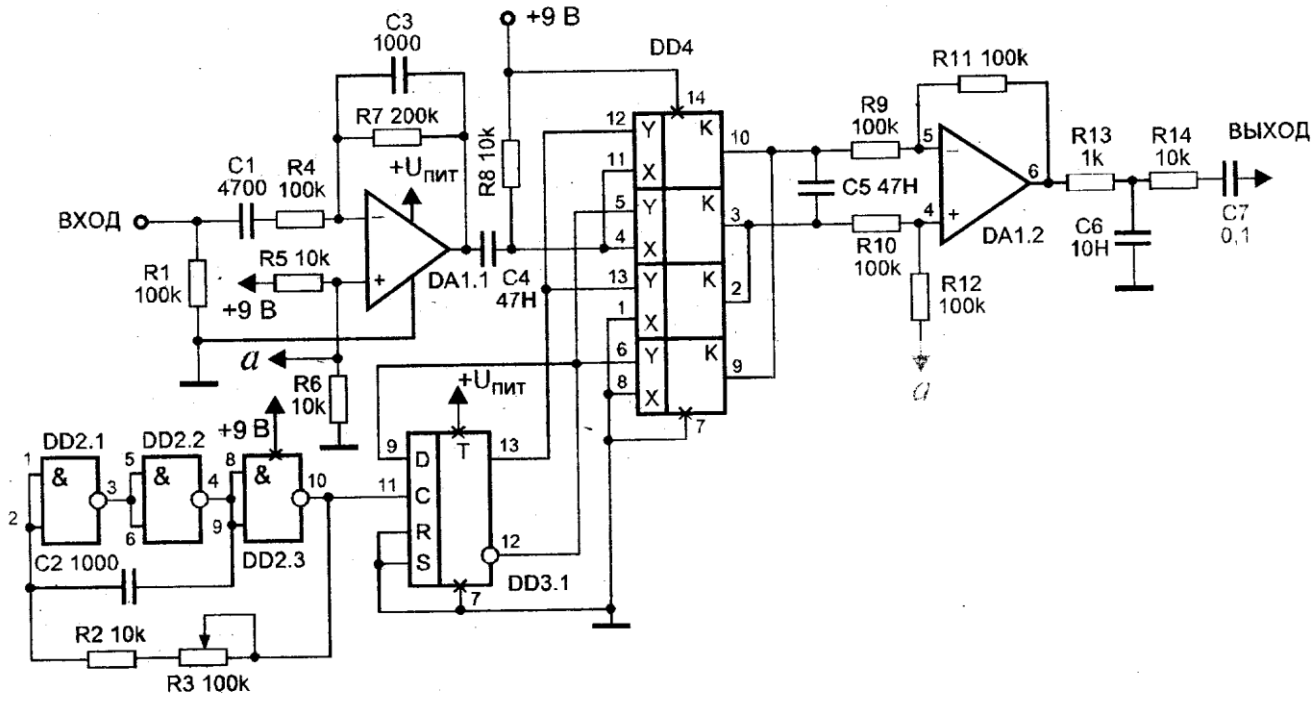


Рис. 3.16. Шифратор звуковых сообщений

Більш високу криптостійкість забезпечують скремблери, що використовують цифрову технологію сигнальної обробки. Усе це стало можливим завдяки застосуванню сигнальних процесорів DSP (Digital Signal Processor). Шифрувальний модуль у цифровій формі записує мовний сигнал для невеликого відрізка часу. Потім цей сигнал підрозділяється на менші блоки, що рівні між собою за тривалістю. Блоки в межах часового відрізка перебудовуються в зворотному порядку за визначеним правилом криптографічного перетворення, що відрізняється в кожному окремому випадку. Правило перемішування інтервалів визначає ключ системи. Природно, що при використанні цього методу відбувається деяка затримка сигналу, що залежить від тривалості інтервалів (чим більше тривалість інтервалів, тим більше затримка сигналу і, відповідно, вище рівень захисту), Оскільки в більшості випадків дані синхронізації посилаються безупинно зі звуковим сигналом, користувач має можливість

наступного з'єднання (його скремблер може декодувати навіть у випадку переривання прийому до початковий момент). Незважаючи на складність шифрування, звукові фільтри DSP-процесора забезпечують високу якість відновлюваного сигналу. Типові моделі скремблерів часового перетворення - ST-50, ST-51, ST-52 (Selectone).

І нарешті, вищий рівень криптостійкості для аналогових радіостанцій забезпечують цілком цифрові скремблери серії DES (Data Encryption Standard) фірми Transcrypt. Спочатку низькочастотний сигнал піддається дискретизації (оцифровці), потім відбувається кодування відповідно до алгоритму DES. Такий сигнал в ефірі чутний як безперервний потік даних.

7.3. Дискретизація мови з наступним шифруванням

Альтернативним аналоговому скремблюванню методом передачі мови в закритому виді є шифрування мовних сигналів, перетворених у цифрову форму, перед їхньою передачею (див. рис. 7.1 C та D). Цей метод забезпечує більш високий рівень закриття в порівнянні з описаними вище аналоговими методами. В основі пристроїв, що працюють по такому принципі, лежить представлення мовного сигналу у виді цифрової послідовності, що закривається за одним з криптографічних алгоритмів.

Основною метою при розробці пристроїв цифрового закриття мови є збереження тих її характеристик, що найбільш важливі для сприйняття слухачем. Одним зі шляхів є збереження форми мовного сигналу. Цей напрямок застосовується в широкосмугових цифрових системах закриття мови. Однак використання властивості надмірності інформації, що міститься в людській мові дозволяє використати смугу частот більш ефективно. Цей напрямок розробляється у вузькосмугових цифрових системах закриття мови.

Збереження форми сигналу вимагає високої швидкості передачі і, відповідно, використання широкосмугових каналів зв'язку. Наприклад, при імпульсно-кодовій модуляції (ІКМ), яка використовується в більшості телефонних мереж, необхідна швидкість передачі, дорівнює 64 кбіт/с. У випадку застосування адаптивної диференціальний ІКМ вона знижується до 32 кбіт/с і нижче. Для вузькосмугових каналів, що не забезпечують такі швидкості передачі, необхідні пристрої, що виключають надмірність мови до її передачі. Зниження інформаційної надмірності мови досягається параметризацією мовного сигналу, при якій характеристики мови, істотні для сприйняття, зберігаються.

Таким чином, правильне застосування методів цифрової передачі мови з високою інформаційною ефективністю є украй важливим напрямком розробок пристроїв цифрового закриття мовних сигналів. У таких системах пристрій кодування мови (вокодер), аналізуючи форму мовного сигналу, робить оцінку параметрів перемінних компонентів моделі генерації мови і передає ці параметри в цифровій формі по каналу зв'язку на синтезатор, де відповідно

до цієї моделі по прийнятих параметрах синтезується мовне повідомлення. У таких моделях мовний сигнал представляється у виді нестаціонарного процесу з обмеженою швидкістю зміни параметрів через механічну інерцію голосових органів людини. На малих інтервалах часу (до 30 мс) параметри сигналу можуть розглядатися як постійні та повільно змінюються в часі. Чим коротше інтервал аналізу, тим більше точно може бути представлена динаміка мови, але при цьому потрібно більш висока швидкість передачі даних. У більшості практичних випадків використовуються 20-мілісекундні інтервали і досягається швидкість передачі даних 2400 біт/с.

Найбільш розповсюдженими типами вокодерів є смугові та з лінійним передбаченням. Метою будь-якого вокодера є передача параметрів, що характеризують мову і мають низьку інформаційну швидкість. Смуговий вокодер досягає цього шляхом передачі амплітуди декількох частотних смуг мовного спектра. Кожен смуговий фільтр такого вокодера збуджується при попадання енергії мовного сигналу в його смугу пропущення. Тому що спектр мовного сигналу змінюється відносно повільно, набір амплітуд вихідних сигналів фільтрів утворить придатну для вокодера основу. У синтезаторі параметри амплітуди кожного каналу керують коефіцієнтами підсилення фільтра, характеристики якого подібні характеристикам фільтра аналізатора. Таким чином, структура смугового вокодера базується на двох блоках фільтрів - для аналізу і синтезу. Збільшення числа каналів поліпшує розбірливість, але при цьому потрібно велика швидкість передачі. Компромісним рішенням звичайно стає вибір 16-20 каналів при швидкості передачі близько 2400 біт/с.

Смугові фільтри в цифровому виконанні будуються на базі аналогових фільтрів Баттерворта, Чебишева, еліптичних і інших. Кожен 20-мідісекундний відрізок часу кодується 48 бітами, з них 6 біт приділяється на інформацію про основний тон, один біт на інформацію "тон-шум", що характеризує наявність чи відсутність вокалізованої ділянки мовного сигналу, інші 41 біт описують значення амплітуд сигналів на виході смугових фільтрів.

Існують різні модифікації смугового вокодера, пристосовані для каналів з обмеженою смугою пропускання. При відсутності твердих вимог на якість синтезованої мови вдається знизити кількість біт переданої інформації з 48 до 36 на кожні 20 мілісекунд, що забезпечує зниження швидкості до 1800 біт/с. Зменшення швидкості передачі до 1200 біт/с можливо у випадку передачі кожного другого кадру мовного сигналу й у ньому додаткової інформації про синтез пропущеного кадру. Втрати синтезованрї мови від таких процедур не занадто великі, достоїнством же є зниження швидкості передачі сигналу.

Найбільше поширення серед систем цифрового кодування мови з наступним шифруванням одержали системи, основним вузлом яких є вокодери з лінійним передбаченням мови (ЛПР).

Метод з лінійним передбаченням мови (ЛПМ) працює блоками відліків, для кожного з яких обчислюється та передається частота основного тону, його амплітуда та інформація про тип збуджуючої дії.

Тут управляючий вхід або сигнал збудження змодельований у вигляді послідовності імпульсів на частоті основного тону (для голосних звуків мови) або випадкового шуму (для приголосних звуків мови).

Комбіновані спектральні складові потоку від голосових зв'язок, голосового тракту та звукоутворення за рахунок губ можуть бути представлені цифровим фільтром із параметрами, що змінюються та передаточною функцією:

$$H(z) = \frac{G}{1 - \sum_{j=1}^{P} a_j z^{-j}} = \frac{G}{A(z)}, \qquad (7.1)$$

де $A(z) = 1 - \sum_{j=1}^{P} a_j z^{-j}$.

Параметри, які характеризують голосовий тракт, є коефіцієнти *A(z)* та масштабний множник *G*.

Перетворюючи рівняння (7.1) у часову область, можна отримати рівняння для імпульсної характеристики $\nu(h)$, яка відповідає *H(z)*:

$$\nu(h) = G\lambda(h) + \sum_{j=1}^{P} a_j \nu(h-j). \qquad (7.2)$$

рівняння (7.2) називають різницевим рівнянням LPC. Воно встановлює, що поточне значення вихідного сигналу $\nu(h)$ може бути визначено сумою зваженого поточного вхідного значення та зваженої суми попередніх вихідних виборок. Як наслідок, в LPC аналізі проблема може бути сформульована таким чином: задані виміряні значення сигналу $\nu(h)$, потрібно визначити параметри передатної функції системи *H(z)*.

Якщо оцінку a_j записати як α_i, то похибка (різниця) може бути визначена у вигляді

$$e_h = \nu(h) - \sum_{j=1}^{P} \alpha_j \nu(h-j). \qquad (7.3)$$

Визначимо мінімальну середньоквадратичну похибку оцінки

$$E = m\{e_h^2\} = m\left\{\left[\nu(h) - \sum_{j=1}^{P} \alpha_j \nu(h-j)\right]^2\right\}. \qquad (7.4)$$

А після при рівняння похідних від E по α_j до нуля для $j = 1,..., P$, одержимо

$$m\left\{\left[\nu(h) - \sum_{j=1}^{P} \alpha_i \nu(h-j)\right]\nu(h-j)\right\} = 0, \quad i = 1,..., p, \qquad (7.5)$$

що витікає з ортогональності $e(h)$ та $\nu(h-j)$ для $i=1,...,p$.

Рівняння (7.5) можна перетворити до вигляду

$$\sum_{j=1}^{P}\alpha_j R_h(i,j)=R_h(i,0),$$

(7.6)

де $R_h(i,j)=m\{\nu(h-i)\nu(h-j)\}$ -

(7.7)

- кореляція між $\nu(h-j)$ та $\nu(h-i)$.

Таким чином, коефіцієнти α_i можуть бути знайдені з рівнянь (7.5) та (7.6). операція диференціювання рівняння (7.6) може бути застосована тільки у випадку, якщо модель мовного сигналу стаціонарний випадковий процес. Але мовний сигнал не є таким на великому відрізку часу. Припущення про стаціонарність справедливо лише для коротких сегментів мови. Тому, математичне очікування (7.7) заміняється поточною кінцевою сумою малих за довжиною відліків.

Після визначення коефіцієнтів α_i до прогнозованих коефіцієнтів у формулі (7.2) треба додати масштабний коефіцієнт *G*. Загально прийнято визначати цей множник так, щоб повні енергії сигналів. які пройшли через фільтр з імпульсною характеристикою $\nu(h)$ та фільтр з імпульсною характеристикою, яка має тільки полюси, були рівні.

Порядок визначення коефіцієнтів *G* такий.

Нехай $\nu(h)$ - імпульсна характеристика фільтра. Яка відповідає формулі (7.2), а $R(h)$ - її кореляційна функція. Імпульсна характеристика $\nu(h)$ задовільне розносному рівнянню:

$$\nu(h)=\sum_{j=1}^{P}a_k\nu(h-j)+G\delta(h), \qquad (7.8)$$

звідки, після перетворень можна знайти

$$G^2=R_v(0)-\sum_{j=1}^{p}a_j R_v(j) \qquad (7.9)$$

таким чином, якщо прогнозуючі коефіцієнти a_j знайдені, то масштабний множник G повністю визначається рівнянням (7.9).

Для моделювання мовного сигналу, який змінюється в часі методами LPC, пам'ятаючи при цьому про умови стаціонарності, треба обмежити аналіз короткочасними блоками.

Це досягається при усередненні рівняння (7.6) кінцевою сумою, тобто

$$R_h(i,j)=m\{v(h-i)v(h-j)\}=\sum_n v_h(n-i)v_h(n-j) \qquad (7.10)$$

Лінійне передбачення при аналізі мовних сигналів звичайно використовується у двох напрямках. Одно з них проведення короткочасного спектрального аналізу мови. Другий напрямок – побудова систем аналіз-синтез.

Параметри, які входять у функцію передбачення, через формулу (7.1) визначають параметри передатної функції голосового тракту. Може бути запропоновано декілька варіантів структури аналізатора, який придатний для побудови синтезатора та який реалізуё передатну функцію голосового тракту. Структуру прямої форми можна отримати безпосередньо за коефіцієнтами функції передбачення. З іншого боку, вираз (7.1) можна перетворити у добуток і отримати структуру каскадної форми.

У всіх випадках параметри синтезатора неперервно оновлюються під час зміни кадрів мови, які аналізуються. Щоб запобігти ефектів, які пов'язані зі скачками значень параметрів, треба плавно змінювати параметри за допомогою інтерполяції при переході від однієї ділянки мови до іншої. Під час прямої форми синтезу може виникнути ситуація, яка відповідає нестійкому фільтру, хоча первісні значення відносились до стійкого фільтру. У каскадній структурі стійкість забезпечується простіше.

Визначення параметрів сигналу збудження в системі аналізу-синтезу з лінійним передбаченням, як правило, грунтується на дослідженні сигналу похибки, який одержують

За допомогою пропускання первісного мовного сигналу через фільтр з характеристикою, яка зворотна тій характеристиці, що апроксимує передатну функцію голосового тракту. Одержаний сигнал похибки є апроксимація сигналу, який збуджує мовне коливання. Для визначення параметрів сигналу збудження можна застосовувати один з відомих алгоритмів розпізнавання дзвінкої та глухої мови, а також оцінки періоду основного тону.

По суті всі системи, які використовують метод LPC, розрізняють лише способами генерування збуджуючої дії та вибору параметрів моделюючого фільтру.

Під час передачі мови відповідний аналізатор формує дані, які містять інформацію про збуджуючу дію (вид дії, частоту основного тону, коефіцієнт підсилення) і про вагових коефіцієнтах формуючих синтезовану мову трансвертального фільтру. При цьому звичайно застосовується метод „аналіз – синтез" (AbS – Analysis by Sinthesis), коли на основі даних , що формуються виконується в процесі передачі з дійсним повідомленням (Рис 7.9), а сигнал похибки ε_p в процессі аналізу уточнює дані, які формуються.Отримані таким чином дані перетворюються керуючим пристроєм у кодове слово (від 10 до 80 біт в залежності від методу, який використовується). Обновлення кодового слова відбувається не рідше, ніж один раз у 10-25 мс. Прийнятний рівень розбірливості може бути досягнутий на швидкостях 4,8 Кбіт/с і навіть 2,4 Кбіт/с.

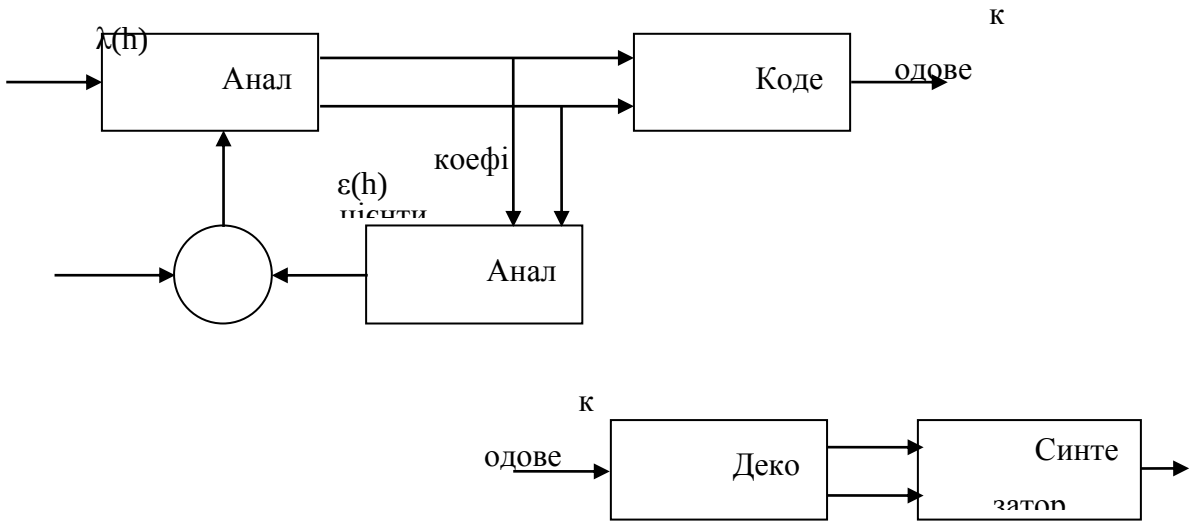


Рис. 7.9.

Основні зусилля розробників конкретних реалізацій метода LPC спрямовані, головним чином, на скорочення часу алгоритмічної затримки $\Delta\tau_З$ (інтервал часу між моментами появи повідомлення на вході передавального пристрою та появи синтезованої мови на виході приймального пристрою при безпосередньому підключенні вказаних пристроїв один до одного та зниження швидкості передачі вихідного потоку даних. У відповідності з рекомендацією G.728 затримка $\Delta\tau_З$ не повинна перевищувати 5 мс, швидкість передачі вихідного потоку даних (передача кодових слів) повинна бути 16 Кбіт/с, а якість мови, яка синтезується на виході тракту передачі не повинна бути нижче, ніж при використанні методів, які задовольняють вимогам рекомендацій G.721 та G.726.

При виконанні LPC-аналізу треба прийняти до уваги декілька важливих груп факторів. Перша група – це експлуатаційні характеристики – ефективність та стабільність. Друга група включає вибір порядку фільтра P, розмір фрейму аналізу N. При кодуванні мови вибірки мови звичайно беруть з частотою 8 кГц, що дає для аналізу спектр 4 кГц. У смузі 4 кГц максимальна кількість формат, які виділяються, дорівнює чотирьом, що потребує фільтра як мінімум $8^{го}$ порядку. Звичайно використовується $10^{ти}$ смуговий фільтр, так що резонанси формат та форма основного спектру моделюються досить точно.

Вибір розміру фрейму виконується у відповідності до умов стаціонарності. Звичайно вибирається розмір фрейму довжиною декілька тоновий періоди (приблизно 16 – 32 мс). Другий фактор — вибір точок поділу фрейму, який аналізується. Проблема в тому, що не існує єдиних методів оптимального поділу. Серед ефективних прийомів можна виділити такі: первісне спотворення сигналу до LPC-аналізу та використання часткового перекриття зважених фреймів. Перекриття фреймів покликано намаганню подолати деякі граничні ефекти фреймового LPC-аналізу. Довжина перекриття складає біля 10 – 20% розміру фрейму. З успіхом використовується інтерполяція LPC-коефіцієнтів від одного фрейму до іншого з метою згладити перехідні процеси.

Якщо LPC-аналіз точний, то оціночні параметри α_j=a_j, то $l(h)=G\lambda(h)=U(h)$, тобто, остача є збуджуючим сигналом. Щоб отримати e(h), повинен бути встановлений інверсний фільтр з передатною функцією

$$H^{-1}(Z)=1-\sum_{j=1}^{p}\alpha_j Z^{-j} \qquad (7.11)$$

Так як $S(Z)=H(Z)U(Z)$ то $U(Z)=H^{-1}(Z)S(Z)$. Сигнал похибки або збудження використовується для одержання параметрів. Однією з причин цього є те, що після інверсної фільтрації остатковий сигнал *e(h)* має суттєво менше різку зміну спектра, ніж первісний сигнал $\lambda(h)$.

Математичне представлення моделі цифрового фільтра, використовуваного у вокодеру з лінійним передбаченням, має вид кусочно-лінійної апроксимації процесу формування мови з деякими спрощеннями, а саме: кожен поточний відлік мовного сигналу є лінійною функцією P попередніх відліків. Незважаючи на недосконаліть такої моделі, її параметри забезпечують прийнятне представлення мовного сигналу. У вокодері з лінійним передбаченням аналізатор здійснює мінімізацію помилки передбачення, що представляє собою різниця поточного відліку мовного сигналу і середньозваженої суми P попередніх відліків, де P - порядок передбачення, а вагові коефіцієнти є коефіцієнтами лінійного передбачення. Оцінка якості проводиться по мінімуму середньоквадратичної величини помилки передбачення. Існує кілька методів мінімізації помилки. Загальним для усіх є те, що при оптимальній величині коефіцієнтів передбачення спектр сигналу помилки наближається до білого шуму і сусідні значення помилки мають мінімальну кореляцію. Відомі методи поділяються на двох категорій: послідовні і блочні, які одержали найбільше поширення.

У вокодері з лінійним передбаченням мовна інформація передається трьома параметрами: амплітудою, сигналом "тон/шум" і періодом основного тону для вокалізованих звуків. Так, відповідно до федерального стандарту США, період аналізованого відрізка мовного сигналу складає 22,5 мс [8], що відповідає 180 відлікам при частоті дискретизації 8 кГц. Кодування в цьому випадку здійснюється 54 бітами, що відповідає швидкості передачі 2400 біт/с. При цьому 41 біт приділяється на кодування десяти коефіцієнтів передбачення, 5 - на кодування величини амплітуди, 7 - на передачу періоду основного тону, і 1 біт визначає рішення "тон/шум". При здійсненні подібного кодування передбачається, що всі параметри незалежні, однак у природній мові параметри корелоьвані і можливо значне зниження швидкості передачі даних без втрати якості, якщо правило кодування оптимізувати з урахуванням залежності всіх параметрів. Такий підхід відомий за назвою векторного кодування. Його застосування до вокодеру з лінійним передбаченням дозволить знизити швидкість передачі даних до 800 біт/с і менш із дуже малою втратою якості.

Основною особливістю використання систем цифрового закриття мовних сигналів є необхідність використання модемів. У принципі можливі наступні підходи при проектуванні систем цифрового закриття мовних сигналів:

1) цифрова послідовність параметрів мови з виходу вокодерного пристрою подається на вхід шифратора, де піддається перетворенню по одному з криптографічних алгоритмів, потім надходить через модем у канал зв'язку, на прийомній стороні якого здійснюються зворотні операції по відновленню мовного сигналу, у яких задіяні модем і дешифратор (див. рис7.1.В). Модем являє собою окремий пристрій, що забезпечує передачу даних по одному з протоколів, рекомендованих МККТТ. забезпечуються або в окремих пристроях, або в програмно-апаратній реалізації самого вокодера;

2) функції шифрування та дешифрування забезпечуються самим модемом (так званий модем, що засекречує,) звичайно по відомих криптографічних алгоритмах типу DES та іншим. Цифровий потік, що несе інформацію про параметри мови, з виходу вокодера безпосередньо надходить на такий модем. Організація зв'язку по каналі аналогічна вищенаведеної.

Щоб позбутися недоліків кодерів форми і вокодерів, був розроблений гібридний метод кодування, що поєднує переваги обох методів. По виду аналізу гібридні кодери діляться на два класи: з частотним поділом і часовим поділом.

Головна концепція кодування з частотною розбивкою складається в поділі мовного спектру на частотні смуги чи компоненти. Відповідно можуть використовуватися або набір фільтрів, або блок-перетворювач. Після кодування і декодування ці складові використовуються для точного відтворення моделі вхідного сигналу шляхом підсумовування сигналів, отриманих на виході фільтрів, чи інверсних значень, отриманих після перетворення. Головне допущення при кодуванні з частотною розбивкою полягає в тому, що сигнал, що піддається кодуванню, дуже повільно змінюється в часі і може бути описаний миттєвим спектром. Це пов'язано з тим, що в більшості систем, а особливо в системах реального часу, у сучасний момент доступний тільки короткочасний сегмент вхідного сигналу. У випадку використання набору фільтрів частота ω фіксована, так що $\omega = \omega_0$, а сигнал частотного домену $S_h(e^{j\omega_0})$ являє собою сигнал на виході постійного в часі лінійного фільтра з імпульсною характеристикою $v(h)$ збуджуваного модульованим сигналом $\lambda(h)e^{-j\omega_0 h}$:

$$S_h(e^{j\omega_0}) = v(h) \otimes \left[\lambda(h)e^{-j\omega_0 h}\right], \qquad (7.12)$$

де $v(h)$ визначає ширину смуги мовного сигналу $\lambda(h)$ навколо центральної частоти ω_0 і є імпульсною характеристикою аналізуючого фільтра; знак $\otimes$ означає згортку функцій.

При використанні блоку, що реалізує перетворення Фур'є, часовий індекс h фіксується на значенні, $h = h_0$, а $S_{h_0}(e^{j\omega_0})$ являє собою звичайне перетворення Фур'є зваженої послідовності $v(h_0 - m)\lambda(m)$:

$$S_{h_0}(e^{j\omega_0}) = \Im\left[v(h_0 - m)\lambda(m)\right] \tag{7.13}$$

де $\Im[\cdot]$ - перетворення Фур'є. Тут $v(h_0 - m)$ визначає відрізок часу аналізу відносно моменту часу $h = h_0$ і є "вікном аналізу" $\omega(h_0 - m)$.

Рівняння синтезуючого набору фільтрів

$$\hat{\lambda}(h) = \frac{1}{2\pi v(0)} \int_{-\pi}^{\pi} S_h(e^{j\omega}) e^{j\omega n} d\omega \tag{7.14}$$

може бути представлене як інтеграл (чи сума) компонентів - короткочасних спектрів $S_h(e^{j\omega_0 h})$ з несучими частотами ω_0.

Для синтезу за допомогою блоку перетворення рівняння виглядає таким чином:

$$\hat{\lambda}(h) = \frac{1}{V(e^{j0})} \sum_{r=-\infty}^{\infty} \Im^{-1}\left[S_r(e^{j\omega})\right] \tag{7.15}$$

Його можна інтерпретувати як суму інверсних перетворень Фур'є застосованих до часових сигналів $v(r - h)\lambda(h)$.

В останніх розробках шифраторів нового покоління застосовують алгоритм мовоутворення CELP.

Цей метод заснований на лінійній авторегресійній моделі процесу формування і сприйняття мови і входить у групу методів *аналізу через синтез*, що реалізують сучасні й ефективні алгоритми інформаційного стиску мовних сигналів. Алгоритми даного класу займають проміжне положення між кодерами форми сигналу, у яких зберігається форма коливання мовного сигналу в процесі його дискретизації і квантування, і параметричними вокодерами, заснованими на процедурах оцінки і кодування невеликого числа параметрів мови, поєднуючи переваги кожного з них.

Лінійна авторегресійна модель процесу формування мовних сигналів з локально постійними на інтервалах 10...30 мс параметрами одержала в даний час найбільше поширення. Для цієї моделі

$$\lambda(h) = \sum_{m=1}^{M} a(m)\lambda(h - m) + x(h) \tag{7.16}$$

де M - порядок моделі; $\lambda(h)$ - послідовність відліків мовного сигналу; $a(m)$ - коефіцієнти лінійного передбачення, що характеризують властивості голосового тракту; $x(h)$ - породжуюча послідовність, чи сигнал збудження голосового тракту.

Авторегресійна модель мовного сигналу описує його з досить високим ступенем точності і дозволяє застосовувати розвинутий математичний апарат лінійного передбачення. При цьому забезпечується більш висока якість декодованої мови, стійкість до вхідного акустичного шуму і помилок у каналі зв'язку у порівнянні із системами з іншими принципами кодування.

У рамках даної моделі найбільш перспективними методами кодування вважаються методи "аналізу через синтез" з використанням багатоімпульсного збудження. Новизна багатоімпульсного збудження полягає в тому, що в сигналі залишку лінійного збудження вибираються такі його значення, що найбільш важливі для підвищення якості синтезованої мови. При цьому використовувана в процедурі аналізу через синтез схема кодування, крім обліку помилок квантування, включає критерії суб'єктивної оцінки якості мовного сигналу, що забезпечує природне звучання синтезованої мови.

При багатоімпульсному збудженні сигнал залишку лінійного передбачення представляється у виді послідовності імпульсів з нерівномірно розподіленими інтервалами і з різними амплітудами (близько 8-10 імпульсів за 10 мс). Амплітуди і положення цих імпульсів визначаються на покадровій основі (кадр за кадром). Основною перевагою багатоімпульсного збудження є те, що воно визначається для будь-якого мовного сегмента і при цьому не потрібно знань ні про вокалізованість даного сегменту, ні про період основного тону.

Методи аналізу через синтез використовують синтезатор (декодер) мовного сигналу як складову частину пристрою кодування. При цьому задача аналізу зводиться до процедури оцінки переданих у канал зв'язку параметрів мови, проведеної відповідно до деякого критерію неузгодженості між вихідним і декодованим сигналами. Для обліку специфіки слухового сприйняття як критерій неузгодженості звичайно використовується зважена по частоті квадратична помилка.

$$\varepsilon_{\omega} = \int_0^{F/2} \left[S(f) - S_q(f) \right]^2 \omega(f)\, df \qquad (7.17)$$

де $S(f)$ і $S_q(f)$ - перетворення Фур'є вихідного і синтезованого мовних сигналів; $w(f)$ - вагова функція. Приймаючи в увагу важливість для сприйняття мови не тільки формант, але і міжформантних областей, для алгоритмів аналізу мови через синтез у якості еталонної була запропонована вагова функція наступного виду:

$$\omega(z) = A(z) A^{-1}(z/\gamma) \qquad (7.18)$$

де $A^{-1}(z)$ - передаточна характеристика синтезуючого фільтра; γ - параметр, що регулює енергію помилки чи шум квантування. Фактично при такому вікні зважування підкреслюється помилка в міжформантних областях і тим самим забезпечується більш

рівномірний по частоті розподіл відношення потужності корисного сигналу до потужності помилки кодування.

В алгоритмах кодування з "аналізом через синтез" підвищення ефективності інформаційного ущільнення мовних сигналів здійснюється, переважно, за рахунок скорочення надмірності послідовності $x(h)$, що здійснює збудження синтезуючого фільтра $A^{-1}(z)$ лінійного передбачення та формує огинаючу сигналу, з коефіцієнтом передачі

$$A^{-1}(z)=\left(1-\sum_{m=1}^{M}a(m)z^{-m}\right)^{-1} \tag{7.19}$$

З цією метою застосовується також додатковий фільтр з характеристикою

$$P^{-1}(z)=(1-g_p z^{-T})^{-1} \tag{7.20}$$

з коефіцієнтом передбачення g_p і затримкою на період основного тону T. Фільтр виконує функції генератора квазіперіодичних коливань голосових зв'язок при вимові вокалізованих звуків.

У залежності від способу опису сигналу $x(h)$, що надходить на вхід фільтра можна виділити алгоритми кодування:

зі збудженням прорідженою послідовністю імпульсів - MPLP (Multi Pulses Lin-ear Prediction);

із самозбудженням - SELP (Self Excited Linear Prediction);

з кодовим збудженням - CELP.

Експериментально встановлено, що кодове збудження забезпечує найбільш високу якість кодування мовного сигналу, у тому числі і при наявності вхідних акустичних завад.

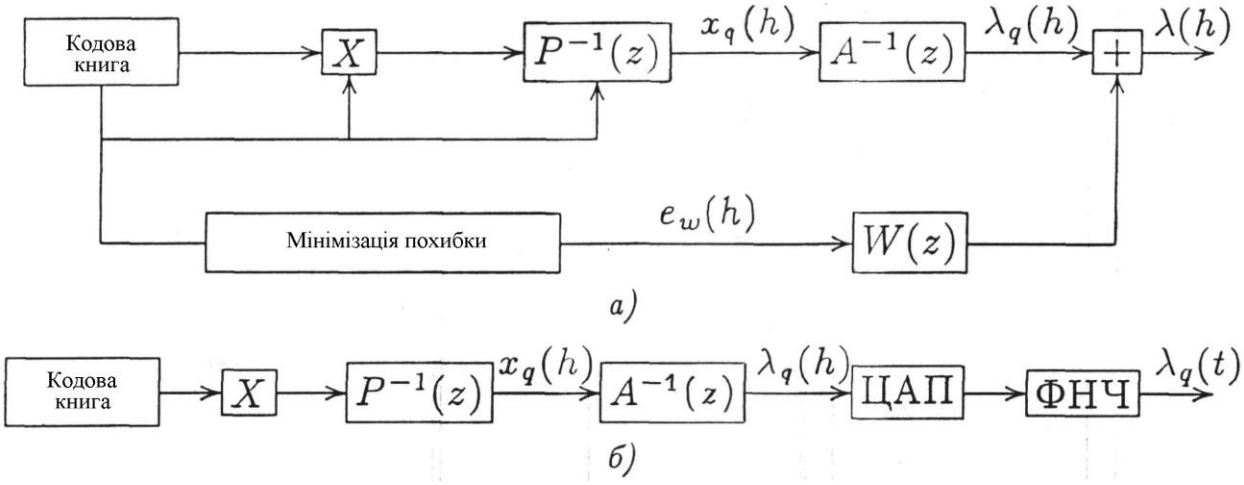


Рис. 7.10. Блок-схема кодера CELP

CELP найбільш ефективно застосовується при передачі мовного сигналу в діапазоні швидкостей від 4 до 16 кбіт/с.

Базова структурна схема передавальної (а) і приймальної (б) частин CELP-кодера показана на рис. 7.10.

Власне кажучи, в алгоритмі CELP виконується векторне квантування послідовності $x(h)$, тобто позиції вибірок і їх амплітуди в сигналі багатоімпульсного збудження оптимізуються одночасно. При цьому відрізок (сегмент) сигналу збудження вибирається з попередньо сформованої постійної сукупності - *кодової книги*, що містить досить велику кількість реалізацій, наприклад, некорельованого гаусівського шуму. Обрана реалізація підсилюється і подається на вхід ланцюга фільтрів (7.20) і (7.19).

Пошук оптимальних значень g_p і T синтезатора основного тону, коефіцієнта підсилення і номера елемента кодової книги здійснюється за допомогою "аналізу через синтез". У канал зв'язку передаються номер (індекс) елемента кодової книги з відповідним коефіцієнтом підсилення, параметри синтезатора основного тону, а також коефіцієнти лінійного передбачення, що характеризують стан голосового тракту.

Будучи однією з найпоширеніших, схема з лінійним передбаченням і збудженням від коду CELP є найкращою схемою для низьких швидкостей. У CELP є лінійний фільтр із параметрами, що змінюються в часі, для виділення грубої і точної спектральної інформації. Збудження виконується шляхом перебору усіх векторів зі збуджуючої кодової книги. Векторна послідовність, що забезпечує мінімальну зважену помилку вважається оптимальним збудженням. Процедура AbS у CELP вимагає великих обчислювальних ресурсів, а основна кодова книга, є результатом дуже великої дослідницької роботи. Хоча CELP є складним методом, він здатний синтезувати мову з високою якістю навіть на низьких швидкостях. Варіант кодування CELP обраний для багатьох систем голосового зв'язку.

Хоча CELP, головним чином, орієнтований на низькі швидкості, на ньому базуються багато стандартів. Випробування показують його прийнятність і для високих швидкостей.

Рекомендація G.723.1 визначає кодове представлення, що може використовуватися на дуже низьких швидкостях для компресії мовних чи інших аудиосигналів у засобах мультимедіа. У кодері, що реалізує рекомендації G.723.1 принциповим додатком є низькошвидкісна відеотелефонія як частина загального сімейства стандартів H.324.

Кодер забезпечує роботу на двох швидкостях - 5,3 і 6,3 кбіт/с. Більш висока швидкість забезпечує кращу якість. Проте, і більш низька швидкість забезпечує гарну якість і надає розробникам систем зв'язку додаткові можливості. І кодер, і декодер повинні обов'язково підтримувати обидві швидкості. Є можливість переключення швидкостей. Можлива також зміна робочої швидкості з використанням переривчастої передачі і заповнення шумом пауз.

Кодер G.723.1 оптимізований для стиску мови з високою якістю на встановленій швидкості при обмеженій смузі. Музика й інші аудіосигнали також можуть бути піддані компресії з використанням цього кодера, однак, не з такою ж високою якістю, як мова.

Кодер G.723.1 перетворює мову чи інші аудіосигнали у фрейми тривалістю 30 мс. Крім того, існує можливість перегляду фреймів на швидкості 7,5 мс, що призводить до загальної алгоритмічної затримки 37,5 мс. Додаткові затримки виникають через:

час, затрачуваний на обробку даних у кодері і декодері;

час передачі по лінії зв'язку;

додаткову буферну затримку протоколу мультиплексування.

Кодер G.723.1 призначений для роботи з цифровими сигналами після попередньої фільтрації смуги аналогового телефонного каналу (рекомендації G.712), дискретизації з частотою 8 кГц і перетворення в 16-бітну лінійну ІКМ послідовність для передачі на вхід кодера. Вихідний сигнал декодера перетворюється в аналоговий сигнал аналогічним шляхом. Інші характеристики входу/виходу такі ж, як і визначені рекомендаціями G.711 для 64-бітної ІКМ. Перед кодуванням дані повинні бути перетворені в 16-бітну ІКМ послідовність чи у відповідний формат після декодування з 16-бітної ІКМ.

Кодер, заснований на принципах кодування методом "аналізу через синтез" з лінійним передбаченням мінімізує зважений сигнал помилки, працює з блоками (фреймами) по 240 вибірок кожний, що на частоті дискретизації 8 кГц еквівалентно тривалості 30 мс. Кожен фрейм проходить через фільтр верхніх частот для видалення постійної складової, а потім розділяється на чотири субфрейми по 60 вибірок у кожному. Для кожного субфрейма використовується фільтр десятого порядку кодера з лінійним передбаченням. Для останнього субфрейма коефіцієнти LPC-фільтра квантуются з використанням прогнозуючого квантизатора вектора розбивки (PSVQ). Квантовані LPC-коефіцієнти використовуються для створення короткочасного зважуючого фільтра, що застосовується для фільтрації усього фрейму і для одержання зваженої оцінки мовного сигналу. На основі цієї оцінки для кожних двох субфреймів (120 вибірок) обчислюється період основного тону T_{L0}. Оцінка тону представляється блоками по 120 вибірок. Період основного тону лежить у діапазоні від 18 до 142 вибірок.

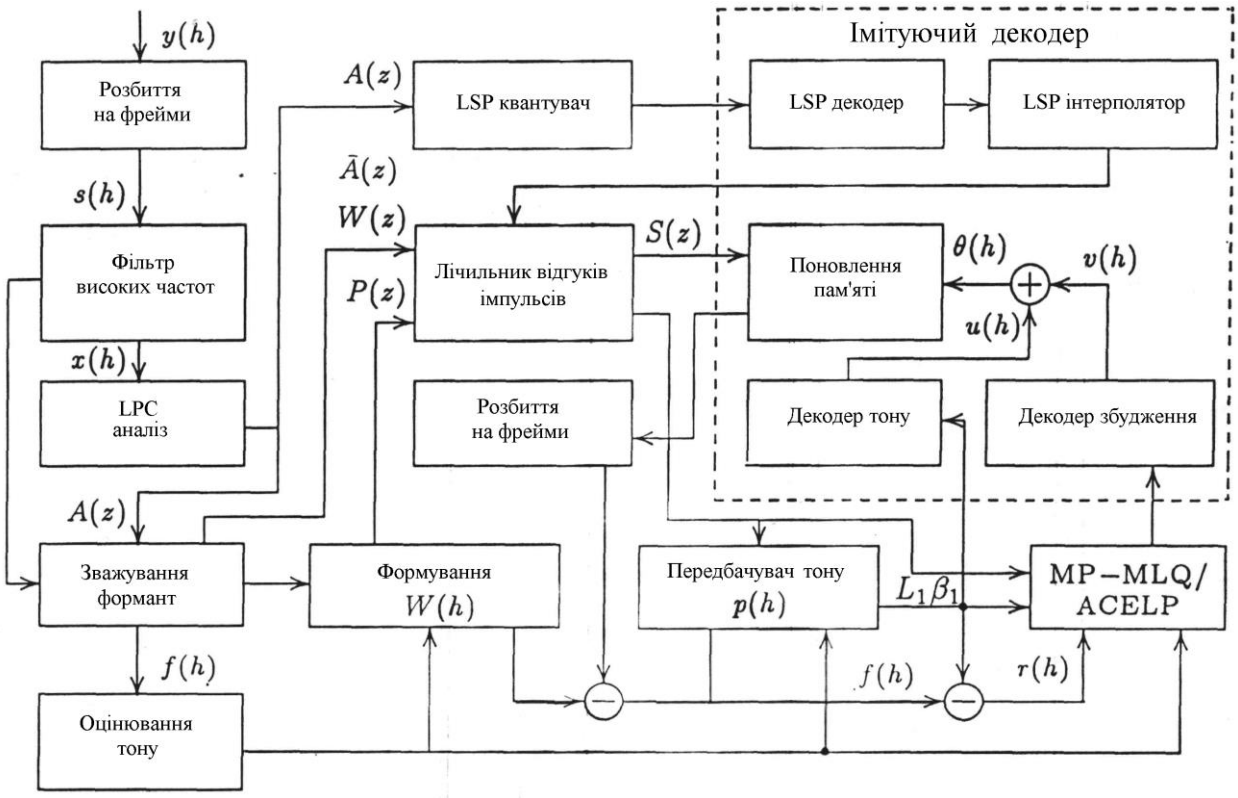


Рис. 7.11. Блок-схема мовного кодера

За допомогою обчисленої заздалегідь оцінки періоду тону створюється фільтр форми гармонічного шуму. Комбінація з фільтра синтезу LPC, фільтра зважування формант, фільтра форми гармонічного шуму використовується для синтезу імпульсної характеристики, необхідної для подальших обчислень.

Оцінки періоду основного тону T_{L0} і імпульсного відгуку використовуються при роботі передбачувача тону п'ятого порядку. Період тону обчислюється як збільшення оцінки періоду основного тону. На декодер передаються тоновий період і різницеві величини. На наступному етапі апроксимуються неперіодичні складові збудження. Для високої швидкості використовується багатоімпульсне збудження з квантуванням і алгоритмом максимальної правдоподібності (MP-MLQ), а для низьких швидкостей - алгебраїчне кодове збудження.

Блок схема мовного кодера показана на рис. 7.11.

Рекомендації ITU-T G.729 містять опис алгоритму кодування мовних сигналів на швидкості 8 кбіт/с з використанням алгебраїчного лінійного передбачення з кодовим збудженням зі спряженою структурою (CS-ACELP).

Подібний кодер створений для роботи з цифровими сигналами, отриманими після попередньої обробки аналогового вхідного сигналу фільтром низької частоти, дискретизації з частотою 8 кГц та подальшого перетворення у лінійну ІКМ для подачі на вхід кодера. Вихідний сигнал декодера конвертується в аналоговий сигнал подібним чином. Інші характеристики входу/виходу визначаються аналогічно рекомендаціями G.711 для ІКМ

послідовностей з швидкістю 64 кбіт/с. Після декодування дані повинні бути перетворені з 16-бітової лінійної ІКМ у необхідний формат.

Кодер CS-ACELP заснований на моделі з лінійним передбаченням з кодовим збудженням (CELP) і працює з фреймами мови по 10 мс, що відповідає 80 вибіркам. Кожен фрейм мовного сигналу тривалістю 10 мс аналізується для виділення параметрів CELP-моделі (коефіцієнти фільтра лінійного передбачення, індекси адаптивної і фіксованої кодових книг і коефіцієнти підсилення). Ці параметри кодуються і передаються на прийомну сторону. Розподіл біт параметрів кодера показаний в табл. 7.1.

Таблиця 7.1

Розподіл біт для алгоритму CS-ACELP на швидкості 8 кбіт/с (фрейми по 10 мс)

Параметр	Кодове слово	Субфрейм 1	Субфрейм 2	В цілому на фрейм
Пари лінійного спектра	LO, L1, L2, L3			
Затримка адаптивної кодової книги	P1, P2	8	5	13
Перевірка затримки тона	P0	1		1
Індекс фіксованої кодової книги	C1, C2	13	13	26
Запис фіксованої кодової книги	S1, S2	4	4	8
Підсилення кодової книги (етап 1)	GA1, GA2	3	3	6
Підсилення кодової книги (етап 2)	GB1, GB2	4	4	8
Всього				80

На стороні декодера ці параметри використовуються для відновлення параметрів збудження і фільтра синтезу. Мова відновлюється при фільтрації збудження фільтром короткочасного синтезу, який заснований на фільтрі лінійного передбачення десятого порядку. Довгочасний фільтр (чи фільтр синтезу тону) виконується з використанням адаптивної кодової книги. Після синтезу мови відбувається додаткове згладжування в постфільтрі.

Принцип кодування ілюструється рис. 7.12. Вхідний сигнал надходить на фільтр високих частот і масштабується в блоці попередньої обробки після чого піддається наступному аналізу. Аналіз з лінійним передбаченням (LP-аналіз) виконується один раз для фрейму тривалістю 10 мс з метою обчислення коефіцієнтів фільтра лінійного передбачення, які потім перетворюються в пари лінійного спектра (Line Spectrum Pairs, LSP) і квантуются (18 біт) з використанням двоетапного векторного квантування з передбаченням.

Сигнал збудження вибирається з використанням пошукової процедури "аналіз через синтез", при якій помилка між вихідною і відновлюваною мовою мінімізується відповідно до

вимірювання зважених спотворень. Це виконується шляхом фільтрації сигналу похибки фільтром зважування, коефіцієнти якого взяті з неквантованного LP-фільтра.

Параметри збудження (параметри фіксованої й адаптивної кодових книг) визначені для субфрейма тривалістю 5 мс (40 вибірок). Коефіцієнти квантованого і неквантованого фільтра з лінійним передбаченням використовуються для другого субфрейма, у той час як у першому субфреймі використовуються інтерпольовані коефіцієнти LP-фільтра.

Рис. 7.12. Принцип кодування

Затримка основного тону оцінюється один раз для фрейму довжиною 10 мс на основі зваженого мовного сигналу. Потім для кожного субфрейма повторюються наступні операції. Сигнал, що знаходять *x(n)* обчислюється при фільтрації залишкового лінійного передбачення у зважуючому фільтрі синтезу $W(z)/\hat{A}(z)$. При фільтрації похибки початкові стани цих фільтрів обновлюються. Це еквівалентно результату виділення нульового вхідного відгуку зважуючого фільтра синтезу із зваженого мовного сигналу. Обчислюється імпульсна характеристика $v(h)$ зважуючого фільтра синтезу, після чого виконується аналіз тону для знаходження затримки адаптивної кодової книги шляхом аналізу значення затримки поблизу основного тону з використанням сигналу, який знаходять *x(n)* і імпульсної характеристики $v(h)$. Затримка тону кодується вісьмома бітами в першому субфреймі і п'ятьмома бітами в другому субфреймі. Сигнал, що знаходять *x(n)* використовується при пошуку фіксованої кодової книги для знаходження оптимального збудження. Сімнадцятибітова алгебраїчна кодова книга використовується для збудження фіксованої кодової книги. Коефіцієнти підсилення внесків адаптивної і фіксованої кодових книг - це вектори, квантовані сімома бітами.

Принцип побудови декодера ілюструється блок-схемою на рис. 7.13. Індекси параметрів кодових книг виділяються з прийнятого потоку біт і декодуються для одержання наступних параметрів кодера, що відповідають мовному фрейму довжиною 10 мс: LP-коефіцієнти (коефіцієнти лінійного передбачення), дві часткові затримки тону, два вектори фіксованої кодової книги і два набори коефіцієнтів адаптивної і фіксованої кодових книг.

Коефіцієнти LSP інтерполюються і перетворюються в коефіцієнти LP-фільтра для кожного субфрейма. Для кожного субфрейма виконуються наступні кроки:

відновлюється збудження шляхом додавання векторів адаптивної і фіксованої кодових книг з відповідними їм коефіцієнтами підсилення;

відновлюється мова шляхом пропущення через фільтр LP-синтезу;

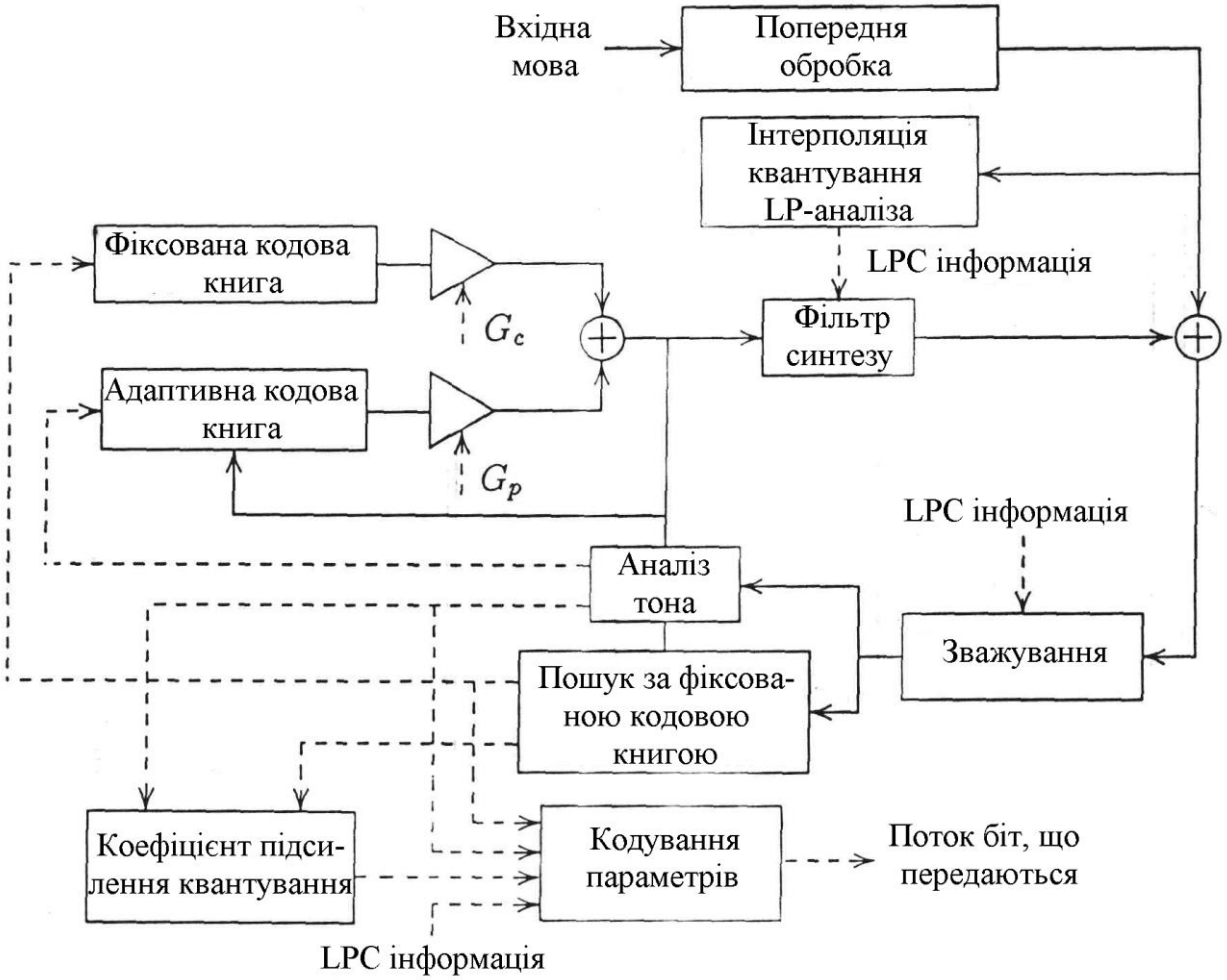


Рис. 7.13. Блок-схема декодера

відновлюваний мовний сигнал пропускається через модуль обробки, який містить адаптивний постфільтр, що складається з довгострокового і короткочасного постфільтрів синтезу, фільтр високих частот і операцію масштабування.

Кодер кодує мову й інші аудіосигнали по фреймах тривалістю 10 мс. У результаті здійснюється затримка 5 мс, що призводить у результаті до загальної алгоритмічної затримки 15 мс. Усі додаткові затримки при практичному виконанні такого кодера обумовлені наступними причинами:

часом обробки, необхідним для операції кодування і декодування;

часом передачі по лініях зв'язку;

затримкою мультиплексування, коли аудіодані поєднуються з іншими даними.

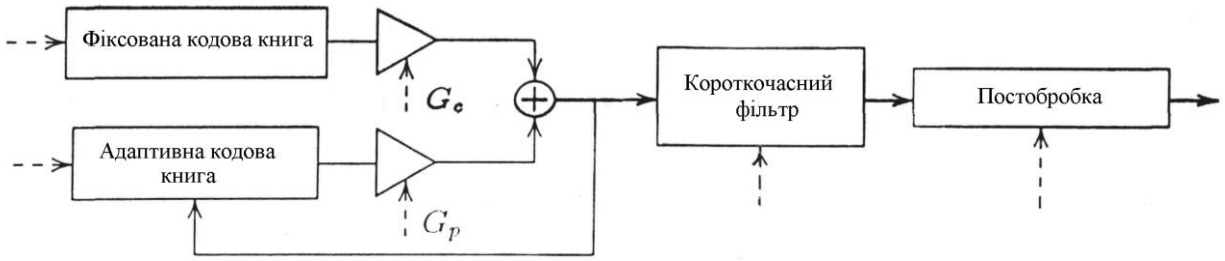


Рис. 7.14. Блок-схема адаптивного кодера CELP

Таким чином, рекомендація G.729 передбачає фрейми збудження по 5 мс і формує чотири імпульси. Фрейм з 40 вибірок розділяється на чотири частини. Перші три мають вісім можливих позицій для імпульсів, четверта - шістнадцять. З кожної частини вибирається по одному імпульсу. У результаті утворюється чотирьохімпульсний ACELP збудження кодової сторінки (рис.7.14).

Таблиця 7.2

Параметри кодерів

Параметри кодера	Кодер		
	G.729	G.729A	G.723.1
Швидкість біт, кбіт/с	8	8	5,3…6,3
Розмір фрейма, мс	10	10	30
Розмір підфрейма, мс	5	5	7,5
Алгебраїчна затримка, мс	15	15	37,5
Швидкодія, млн. оп./с	20	10	14…20
Об’єм ПЗУ, байт	5,2 К	4 К	4,4 К
Якість	Гарна	Гарна	Гарна

Для режиму 5,3 кбіт/с Рекомендація G723.1 передбачає фрейми збудження тривалістю 7,5 мс і також використовує чотирьохімпульсне ACELP-збудження кодової сторінки. Для швидкості 6,3 кбіт/с використовується технологія багатоімпульсного збудження з квантуванням і алгоритмом максимальної правдоподібності (MP-MLQ). У цьому випадку позиції фреймів групуються в підгрупи з парними і непарними номерами. Для визначеного номера імпульсу з парної послідовності (п'ятий чи шостий у залежності від того, чи є сам фрейм парним чи непарним) використовується послідовний багатоімпульсний пошук. Схожий пошук повторюється для підфреймів з непарними номерами. Для збудження вибирається група з мінімальними загальними спотвореннями.

На стороні декодера інформація кодера з лінійним передбаченням (LPC) і інформація адаптивної і фіксованої кодової книг демультиплексується і використовується для реконструкції вихідного сигналу. Для цих цілей використовується адаптивний постфільтр. У випадку кодера G.723.1 сигнал збудження перед проходженням через фільтр синтезу LPC

пропускається через LT (long-term - довгостроковий) постфільтр і ST (short-term - короткочасний) постфільтр.

7.4. Статистичний аналіз кодерів CELP

Розглянемо аналіз роботи кодерів CELP, що реалізують процедуру аналізу через синтез AbS на прикладі кодера, блок-схема якого приведена на рис. 5.25. Сигнал збудження $x(h)$ формується шляхом додавання масштабованого сигналу з адаптивної кодової книги (АКК) (додаються довгострокові частотні складові мовного сигналу) і масштабованого сигналу з великої фіксованої кодової книги (ФКК). Отриманий сигнал збудження керує синтезуючим фільтром, що моделює ефекти голосового тракту. У декодері сигнал збудження проходить через синтезуючий фільтр, формуючи відновлений мовний сигнал $\hat{\lambda}(h)$. Очевидно, що спочатку визначаються параметри фільтра, а потім уже знаходяться індекси кодових книг α і k та відповідні коефіцієнти підсилення G_1 і G_2. Параметри кодових книг вибираються так, щоб мінімізувати зважену помилку між вихідним мовним сигналом і відновленим, що досягається подачею вмісту кожної "комірки" кодової книги на синтезуючий фільтр з метою виявлення максимально схожого (по сприйняттю) зразка.

Однак на практиці вводять два спрощення строгого замкнутого аналізу. Перше пов'язано з визначенням параметрів синтезуючого фільтра. Його характеристика, для простоти, береться інверсною до характеристики фільтра короткочасного лінійного передбачення, яка мінімізує енергію сигналу помилки передбачення. Параметри синтезуючого фільтра визначаються з урахуванням збуджуючого сигналу $x(h)$, однак після того як вони визначені, більше ніякі зміни цього сигналу не враховуються. Це може означати, наприклад, що на визначенні параметрів фільтра можуть позначатися довгострокові складові, тоді як їхнє моделювання краще "залишити" для адаптивної кодової книги.

Друге спрощення строгого аналізу допускається при визначенні параметрів кодової книги. Краще, якщо замість спільного визначення параметрів кодових книг (адаптивної і фіксованої) для мінімізації зваженої похибки спочатку визначити затримку і коефіцієнт підсилення АКК, вважаючи, що сигнал ФКК дорівнює нулю. А потім, маючи сигнал АКК, визначити параметри ФКК. Таке рішення покликане знизити складність CELP-кодерів до прийнятного рівня, що, природно, веде до деякого зниження якості відтвореної мови.

Розглянемо вплив цих двох спрощень на якість відтвореної мови.

Обчислення параметрів синтезуючого фільтра. Як відзначалося вище, спрощена характеристика синтезуючого фільтра інверсна до характеристики фільтра помилки передбачення $A(z) = 1 - \alpha_1 \cdot z^{-1} - \alpha_2 \cdot z^{-2} - ... - \alpha_p \cdot z^{-p}$.

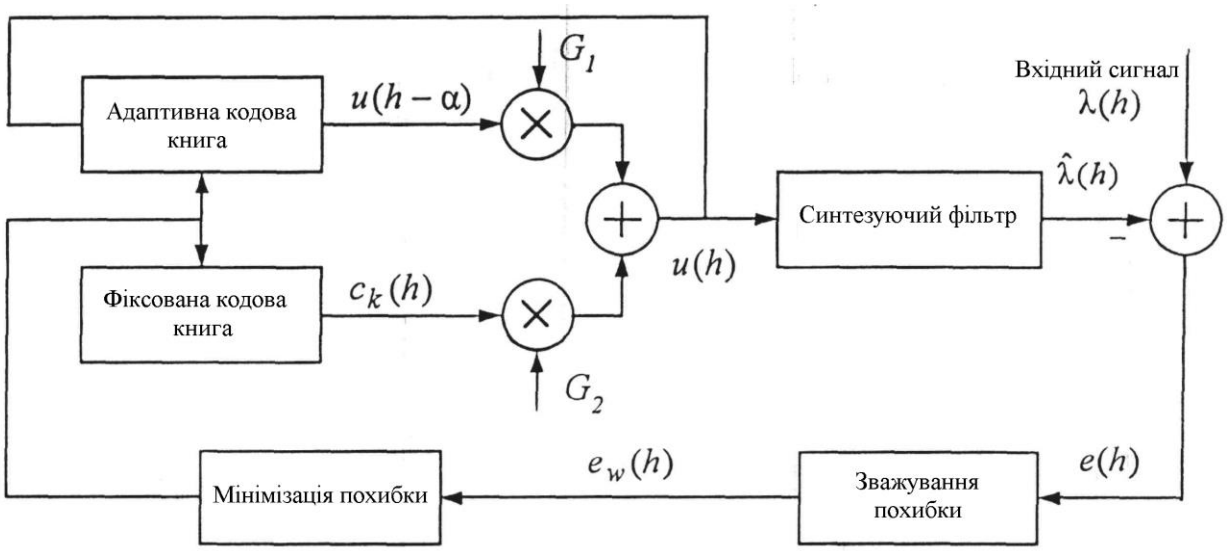


Рис. 7.15. Блок-схема синтезуючого фільтра

Цей фільтр мінімізує енергію залишку від передбачення вхідного мовного сигналу $\lambda(h)$. Тут p - порядок фільтра. Відомо, що це далеко не ідеальний шлях визначення параметрів синтезуючого фільтра. Тому, коли сигнал збудження $x(h)$ визначений, коефіцієнти синтезуючого фільтра можна перерахувати з метою збільшення відношення сигнал/шум (ВСШ) відтвореної мови. Розглянемо різні методи проведення такої оптимізації.

Один з методів оптимизації, що може бути запропонований до аналізу кодерів з багатоімпульсним збудженням, називається *відновлення по методу найменших квадратів*. Маючи сигнал збудження $x(h)$ і набір коефіцієнтів фільтра a_k, k = 1,2,...,p, відновлений мовний сигнал $\lambda(h)$ можна обчислити за допомогою виразу

$$\hat{\lambda}(h) = x(h) + \sum_{k=1}^{p} a_k \hat{\lambda}(h-k) \tag{7.21}$$

Мінімізація E - енергії сигналу помилки $e(h) = \lambda(h) - \hat{\lambda}(h)$ по всій довжині L фрейму - здійснюється за допомогою виразу

$$E = \sum_{h=0}^{L-1} (\lambda(h) - \hat{\lambda}(h))^2 = \sum_{h=0}^{L-1} (\lambda(h) - x(h) - \sum_{k=1}^{p} a_k \hat{\lambda}(h-k))^2 . \tag{7.22}$$

Очевидно, що E залежить не тільки від коефіцієнтів фільтра, але і від відновленого сигналу $\hat{\lambda}(h)$, який, у свою чергу, також залежить від коефіцієнтів фільтра. У результаті не можна прийняти частинні похідні $\partial E/\partial a_i$ за нуль і одержати систему p лінійних рівнянь для визначення набору оптимальних коефіцієнтів.

З метою спрощення аналізу зробимо наступне припущення:

$$\hat{\lambda}(h-k) \approx \lambda(h-k) \tag{7.23}$$

Тоді, підставляючи (7.19) у (7.18), одержуємо

$$E \approx \sum_{h=0}^{L-1} (\lambda(h) - x(h) - \sum_{k=1}^{p} a_k \lambda(h-k))^2 \tag{7.24}$$

Тепер прирівнюючи частинні похідні $\partial E/\partial a_i$ до нуля для i = 1, 2,..., p, можна одержати систему p лінійних рівнянь. Розв'язавши її, одержимо оновлені коефіцієнти фільтра.

Разом з тим, застосування цього методу може призвести до погіршення ВСШ. Причина полягає в необґрунтованості допущення (7.23). Щоб поліпшити сегментне ВСШ у відновленій мові, необхідно в кожному фреймі визначати параметри фільтра, використовуючи як вихідні, так і оновлені коефіцієнти, і передавати ті з них, що забезпечують максимальне ВСШ.

Обчислення параметрів збудження. Щоб знизити складність кодера, зважуючий фільтр сигналу похибки звичайно включають так, щоб вхідний $\lambda(h)$ і відновлений $\hat{\lambda}(h)$ сигнали роздільно зважувалися до проведення їхнього порівняння й обчислення похибки. Для всеполюсного синтезуючого фільтра з характеристикою $H(z) = 1/A(z)$, де $A(z) = 1 - \alpha_1 \cdot z^{-1} - \alpha_2 \cdot z^{-2} - ... - \alpha_p \cdot z^{-p}$, і зважуючого фільтра сигналу похибки $A(z)/A(z/\gamma)$, де γ - константа, що на практиці дорівнює 0,9. Каскадне з'єднання еквівалентне використанню зважуючого синтезуючого фільтра $1/A(z)$. Зважена похибка в цьому випадку

$$e_\omega(h) = \lambda_\omega(h) - \hat{\lambda}(h) = \lambda_\omega(h) - \hat{\lambda}_0(h) - G_1[x(h-a)v(h)] - G_2[c_k(h)v(h)], \tag{7.58}$$

де $\lambda_\omega(h)$ - зважений вхідний сигнал; $\hat{\lambda}_0(h)$ - відгук зважуючого синтезуючого фільтра на вхідне значення попереднього субфрейма (при відсутності іншого вхідного сигналу); $v(h)$ - імпульсна характеристика зважуючого синтезуючого фільтра.

У процесі процедури пошуку визначаються значення коефіцієнта підсилення G_1 і затримки α для АКК, а також індекс k і коефіцієнт підсилення G_2 для ФКК, що мінімізують середньоквадратичну помилку E_ω, отриману в субфреймі довжиною H:

$$E_\omega = \frac{1}{H}\left(\sum_{h=0}^{H} \lambda^2(h) - T_{\alpha k}\right), \tag{7.25}$$

де

$$T_{\alpha k} = 2(G_1 R_\alpha + G_2 R_k - G_1 G_2 Y_{\alpha k}) - G_1^2 \xi_\alpha - G_2^2 \xi_k \tag{7.26}$$

являє собою величину, збільшення якої домагаються пошуком у кодовій книзі (тобто максимальне значення $T_{\alpha k}$ вказує на успішний вибір параметрів кодової книги);

$u(h) = \lambda_{\omega}(h) - \hat{\lambda}_0(h)$ - сигнал-ознака для пошуку.

Тут

$$\xi_{\alpha} = \sum_{h=0}^{H-1} [x(h-\alpha)v(h)]^2 \text{ - енергія фільтрованого сигналу АКК;}$$

$$R_{\alpha} = \sum_{h=0}^{H-1} u(h)[x(h-\alpha)v(h)] \tag{7.27}$$

- кореляція між фільтрованим сигналом АКК і сигналом-ознакою $u(h)$. Аналогічно, ξ_k - це енергія фільтрованого сигналу ФКК $[c_k(h)v(h)]$, а R_k - кореляція між цим сигналом і сигналом-ознакою і, нарешті,

$$R_{\alpha k} = \sum_{h=0}^{H-1} [x(h-\alpha)v(h)][c_k(h)v(h)] \tag{7.28}$$

- кореляція між фільтрованими сигналами обох кодових книг.

При звичайному методі пошуку параметрів кодової книги в (7.26) спочатку вважають $G_2 = 0$. Потім для даного значення α може бути визначений оптимальний коефіцієнт підсилення G_1, якщо прирівняти до нуля значення частинної похідної $T_{\alpha k}$ відносно G_1. У результаті знайдемо значення $T_{\alpha k}$ для кожного значення α і виберемо таке значення затримки, якому відповідає максимум $T_{\alpha k}$. Параметри АКК фіксуються й аналогічна процедура проводиться для визначення параметрів ФКК k і G_2.

Можна запропонувати декілька субоптимальных методів. Розглянемо три з них.

Метод А. α і k знаходяться при використанні звичайної процедури пошуку, а потім вирази використовуються для визначення оптимальних значень G_1 і G_2.

Метод В. Вважаючи $G_2 = 0$, визначається затримка АКК α і потім, використовуючи тільки це значення, здійснюється пошук у ФКК, з якої визначаються значення G_1, G_2 і k.

Метод С. Знаходяться коефіцієнти α, k, G_1 і G_2 аналогічно методу В, а потім для відомого k обновляється α. Іншими словами, для кожного можливого α визначається G_1, G_2 і $T_{\alpha k}$ і вибирається таке значення α, якому відповідає максимальне $T_{\alpha k}$.

Зробимо порівняння перерахованих методів зі звичайним послідовним пошуком і з модернізованим одночасним пошуком в обох кодових книгах. Якщо прирівняти частинні похідні $T_{\alpha k}$ відносно G_1 і G_2 до нуля, одержимо систему двох рівнянь, розв'язавши які, знайдемо оптимальні значення коефіцієнтів підсилення для заданих індексів кодових книг α і k:

$$G_1 = \frac{R_\alpha \xi_k - R_k R_{\alpha k}}{\xi_\alpha \xi_k - R_{\alpha k}^2}; \quad (7.29)$$

$$G_2 = \frac{R_k \xi_\alpha - R_\alpha R_{\alpha k}}{\xi_\alpha \xi_k - R_{\alpha k}^2}. \quad (7.30)$$

Повна процедура пошуку передбачає обчислення ξ_α, ξ_k, R_α, R_k та $R_{\alpha k}$ для кожної пари індексів α і k щоб з їх допомогою знайти коефіцієнти підсилення G_1 і G_2.

Таблиця 7.3

Характеристики різних методів пошуку

Метод	Сегментне ВСШ, дБ	Складність
Послідовний пошук	9,7	1
Метод А	10,1	1,02
Метод В	10,3	1,3
Метод С	10,6	1,4
Повний пошук	10,8	60

Ці коефіцієнти підсилення можуть бути потім підставлені в (7.60) для обчислення $T_{\alpha k}$, максимізувати яке необхідно для правильного вибору індексів. Головні труднощі повного пошуку виникають при визначенні взаємної кореляції $R_{\alpha k}$ для кожної пари індексів кодових книг. Використання алгебраїчної фіксованої кодової книги [8] дозволяє одночасно з ξ_k і R_k визначити $R_{\alpha k}$ більш ефективно використовуючи серію з чотирьох вкладених циклів [7].

У табл. 7.3 представлені такі характеристики ACELP на 4,8 кбіт/с, як сегментне ВСШ і відносна складність для різних методів пошуку. Повний пошук дає виграш по показнику ВСШ приблизно 1 дБ у порівнянні з послідовним пошуком, але його складність у 60 разів вище. Метод С, що збільшує складність кодера приблизно на 40 % дає майже таке ж відношення ВСШ, як кодер з повним пошуком. Нарешті, метод А збільшує складність кодека на 2 %, але дає відчутне збільшення ВСШ.

7.5. Багатопозиційні фазова та амплітудно-фазова модуляція

Загальновідомо, що якщо повідомлення передається двоїчними посилками (двоїчним кодом), то швидкість передачі не може перевищувати $2\Delta F_к$ біт/с, або 2 біт/с на 1 Гц смуги пропускання каналу. Для підвищення питомої швидкості передачі інформації необхідно

перейти до багатократної модуляції (багатопозиційним кодом), при якій кожна елементарна посилка несе більше ніж 1 біт інформації.

Найбільше застосування багатократні методи найшли при фазовій модуляції. Тут кожній комбінації з n одиночних двоїчних елементів, які поступають від джерела інформації, ставиться у відповідність якесь значення фази відрізку коливань. Правило відображення двоїчної послідовності $\{a_i\}$ у послідовність сигналів $\{S_{i,к}(t)\}$ називають модуляційним кодом. Так, при двократній фазовій модуляції (ДФМ) послідовність, яка передається, розбивається на комбінації з двох елементів. Очевидно, що кількість різних комбінацій довжини m дорівнює 2^m.

Якщо розглядати відносно фазову модуляцію (ДВФМ) то $\Delta\varphi$ відповідає зсуву фаз між $i-$м та $(i-1)-$ м сигналами. Отже при ДВФМ швидкість передачі інформації вдвічі більше, ніж при ОФМ, але й вірогідність помилки також вдвічі більше. Двократна відносно фазова модуляція застосовують для передачі інформації зі швидкістю 2400 біт/с.

Збільшення швидкостей передачі до 3 біт/(Гц·с) та вище може бути отримано спільним використанням амплітудної та фазової модуляції. У цьому разі для зменшення спектра сигналу в канал передається одна бокова смуга частот.

До сучасних протоколів, які використовуються в модемах, відносяться V.32, V.32 bis і також протокол V.34. У протоколі V.32 використовується квадратурна амплітудна модуляція з частотою несучого коливання 1800 Гц та швидкістю маніпуляції 2400 Бод. Існують режими двох-, чотирьох- та шістнадцятипозиційної QAM (Quadrature Amplitude Modulation). Відповідно інформаційна швидкість у них може бути 2400, 4800 та 9600 біт/с.

Розглянемо більш детально алгоритм модуляції QAM. У цьому алгоритмі сигнал, який передається, кодується одночасно зміною амплітуди сінфазної (I) та квадратурної (Q) компонент несучого гармонійного коливання (f_c), які мають зсув по фазі відносно один одного на $p/2$ радіана. Результуючий сигнал Z формується при сумуванні цих коливань. Таким чином, QAM-модульований дискретний сигнал може бути представлений співвідношенням:

$$Z_m(t) = I_m \cdot \cos(2pf_c t) + Q_m \cdot \sin(2pf_c t) \qquad (7.31)$$

де t – змінюється в діапазоні $\{(m-1)*Dt...m*Dt\}$; m – порядковий номер дискрета часу; Dt – крок квантування вхідного сигналу за часом; p – крок квантування вхідного сигналу за амплітудою; a_m та b_m – модуляційні коефіцієнти:

$$I_m = a_m \cdot p,\ Q_m = b_m \cdot p$$

Цей же сигнал можна представити у комплексному вигляді таким чином:

$$Z = I + j \cdot Q \text{, або } Z_m = A_m \cdot \exp(2pf_c + j_m), \qquad (7.32)$$

де $A_m = \left(Q_m^2 + I_m^2\right)^{1/2}$ – алгоритм зміни амплітуди модульованого сигналу; $j_m = arctg\left(Q_m / I_m\right)$ – алгоритм зміни фази модульованого сигналу.

Таким чином, при використанні квадратурної амплітудної модуляції сигнал кодується одночасно зміною амплітуди та фази несучого коливання. На рис. 7.16 показано принцип формування результуючого коливання Z шляхом сумування вектора квадратурної складової Q з вектором синфазної складової I. Амплітуда вектора Z визначається співвідношенням A_m, а кут, який утворює вектор з вісью абсцис, визначається співвідношенням j_m.

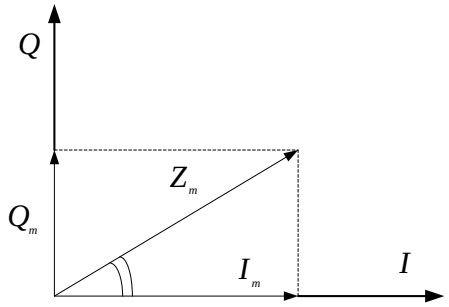


Рис. 7.16. Принцип формування сигналу QAM

У цьому алгоритмі при модулюванні синфазної та квадратурної складових несучого коливання використовується одне й те ж значення дискрета зміни амплітуди. Тому кінцівки векторів модульованого коливання утворюють прямокутну сітку на фазовій площині дійсної $-\mathrm{Re}\{z\}$ та $J_m\{Z\}$. Кількість вузлів цієї сітки визначається типом алгоритму QAM, який використовується. Схему розташування вузлів на фазовій площині модульованого QAM коливання прийнято називати сузір'ям (constellation).

Звичайно для позначення типу алгоритму QAM прийнята така схема позначення QAM–2^N. Де число 2^N відповідає кількості вузлів на фазовій сітці, а також максимальній кількості різних значень вектора модульованого сигналу. Слід зазначити, що в даному випадку значення N відповідає показнику спектральної ефективності алгоритму, який використовується.

На рис. 7.17 наведена спрощена структурна схема формування QAM модульованого сигналу.

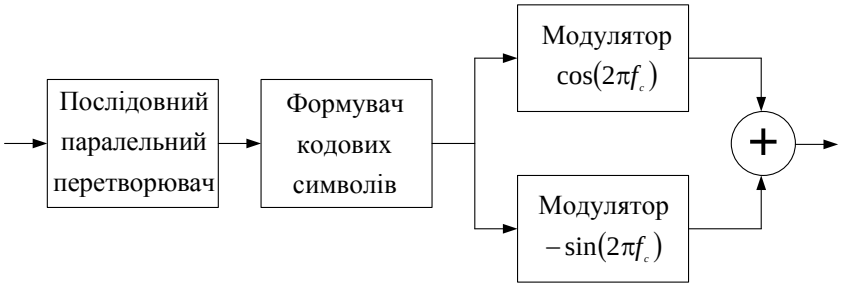


Рис. 7.17. Структурна схема формувача QAM модульованого сигналу

Формувач кодових символів перетворює двомірний кодовий символ m_j на пару кодових символів a_j та b_j. Для алгоритму QAM-16 припустимі значення a_j та b_j належать множині $\{1, 3, -1, -3\}$ і визначають відповідно значення реальної та уявної координати вектора модульованого коливання. Сформовані значення $A\{a_j\}$ та $B\{b_j\}$ використовуються для амплітудної модуляції синфазної I та квадратурної Q складових несучого коливання. На останньому етапі перетворення використовується то складання цих коливань, то формування результуючого сигналу Z.

Наприклад маємо послідовність модуляційних символів $\{m_3, m_2, m_1, m_0\}$. Отже, для алгоритму QAM-16 пара $\{m_3, m_2\}$ визначає номер квадранта фазової площини або знаки реальної та уявної координати вектора модульованого коливання таким чином:

$$
\begin{aligned}
&00 \to Sign(\mathrm{Re}\{Z\}) = 1, \qquad Sign(I_m\{Z\}) = 1.\\
&10 \to Sign(\mathrm{Re}\{Z\}) = 1, \qquad Sign(I_m\{Z\}) = -1.\\
&01 \to Sign(\mathrm{Re}\{Z\}) = -1, \qquad Sign(I_m\{Z\}) = 1.\\
&11 \to Sign(\mathrm{Re}\{Z\}) = -1, \qquad Sign(I_m\{Z\}) = -1.
\end{aligned}
$$

Пара $\{m_1, m_0\}$ визначає значення амплітуди реальної та уявної координати вектора модульованого коливання відповідно таким чином:

$$
\begin{array}{c}
m_1, m_0 \to a_j, b_j \\
0 \mid 0 \ \to \ 1 \mid 1 \\
0 \mid 1 \ \to \ 1 \mid 3 \\
1 \mid 0 \ \to \ 3 \mid 1 \\
1 \mid 1 \ \to \ 3 \mid 3
\end{array}
$$

Перетворення модуляційних символів у кодові символи виконується з застосуванням алгоритмів Грея для завадостійкого кодування даних. Так векторам модульованого коливання, які знаходяться близько один від одного на фазовій площині, ставлять у відповідність значення кодових символів, які розрізняються значенням тільки одного біта.

У якості приклада можуть бути розглянуті два вектора $Z = 1 + j$ та $Z = 1 + 3j$, яким відповідають кодові символи $\{0, 0\}$ та $\{0, 1\}$.

На цей час найбільше поширення отримали декілька варіантів QAM. Наприклад QAM-4, який кодує інформаційний сигнал зміною фази несучого коливання з кроком $p/2$. Цей алгоритм модуляції носить назву QPSK (Quadrature Phase Shift Keying) тобто квадратурна фазова маніпуляція.

Слід мати на увазі, що алгоритм квадратурної амплітудної модуляції є різновидом алгоритму гармонічної амплітудної модуляції і тому має такі властивості, як:

– ширина спактру QAM модульованого коливання не перевищує ширину спектру модулюючого сигналу;

– положення спектра QAM модульованого коливання в частотній області визначається номіналом частоти несучого коливання.

Ці корисні властивості алгоритму забезпечує можливість побудови на його основі високошвидкісних ADSL систем передачі даних по двопровідній лінії з частотним розподілом інформаційних потоків, які приймаються та передаються.

Кожний з алгоритмів QAM визначає значення таких параметрів:

– розмір модуляційного символу $N(\text{біт}) = \log_2$ кількість крапок сузір'я;

– значення символьної швидкості $f_S[\text{кбод/с}]$;

– центральна частота f_c (central rate);

– швидкість передачі даних $V = N \cdot f_S$.

Центральна частота f_c для конкретної реалізації алгоритму модуляції визначається співвідношенням:

$$f_H + f_S/2 \le f_c \le f_B - f_S/2 \qquad (7.33)$$

Параметри огинаючих ліній (масок) енергетичних спектрів модульованих сигналів ADSL регламентуються стандартом T1.413 ANSI.

Додержання цих масок забезпечує потрібний рівень електромагнітної сумісності сигналів різної природи, які передаються по різним парам в одному кабелі. Незалежно від типу алгоритма модуляції енергетичний спектр модульованого сигналу не повинен виходити за межі встановленої маски.

Завадостійкість алгоритму QAM зворотньо пропорційна його спектральній ефективності. Дія завад приводить до появи не контрольованих змін амплітуди сигналу, який передається по лінії. При збільшенні кількості кодових точок на фазовій площині відстань між ними P зменшується та, як наслідок, зростає вірогідність помилкового розпізнання спотвореного прийнятого вектора Z_m^* на приймальній стороні.

Цей алгоритм є відносно простим для реалізації і, в той же час, досить ефективним алгоритмом лінійного кодування XDSL сигналів. Сучасні реалізації цього алгоритму забезпечують високі показники спектральної ефективності. Відносно високий рівень завадостійкості QAM-модульованого сигнала забезпечує можливість побудови на основі цієї технології високошвидкісних систем передачі даних по двохпроводній лінії з частотним розподілом інформаційних потоків, які передаються та приймаються.

До недоліків алгоритму можна віднести відносно невеликий рівень корисного сигналу в спектрі модульованого коливання. Цей недолік є загальним для алгоритмів гармонічної амплітудної модуляції і проявляється в тому, що максимальна амплітуда в спектрі

модульованого коливання має гармоніку з частотою несучого коливання. Тому цей алгоритм у чистому вигляді досить рідко застосовується на практиці. Значно більше поширення отримали алгоритми, які використовують принципи QAM і в той же час вільні від його недоліків. Наприклад, алгоритм CAP (Carrier less Amplitude modulation/ Phase modulation) тобто алгоритм амплітудно-фазової модуляції з придушеною несучею.

Алгоритм CAP являє собою один з різновидів алгоритму QAM, а його особливістю є спеціальна обробка модульованого інформаційного сигналу перед його передачею в лінію. В процесі цієї обробки із спектра модульованого сигналу вилучається складова, яка відповідає частоті несучого коливання QAM. Після того, як приймач приймає інформаційний сигнал, що передавався, він спочатку відновлює частоту несучого коливання, а після цього відновлює інформаційний сигнал. Такі маніпуляції зі спектром виконуються для того, щоб зменшити частку неінформативної складової в спектрі інформаційного сигналу, що передається. Це в свою чергу виконується для того, щоб забезпечити більшу відстань сигналу, який поширюється у просторі та зменшити рівень перехресних завад у сигналів, які передаються одночасно у одному кабелі.

Таким чином, основні принципи формування лінійного коду алгоритму CAP відповідають принципам формування лінійного коду QAM. Відмінність вказаних алгоритмів є у тому, що включені додаткові процедури, які використовуються для формування та відновлення спектра CAP-модульованого сигналу.

Одна з можливих функціональних схем формування сигналу, модульованого за допомогою алгоритма CAP, показана на рис. 7.18.

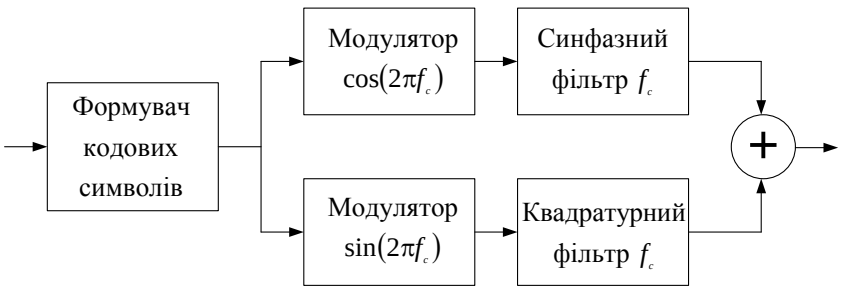


Рис. 7.18. Функціональна схема формування CAP-модульованого сигналу

У даному випадку для придушення гармоніки несучого коливання використовуються синфазний та квадратурний фільтри. Для адекватного відновлення сформованого таким чином сигналу на приймальній стороні повинна бути виконана відповідна процедура з відновлення несучого коливання. Після відновлення несучого коливання, приймач, який функціонує у відповідальності з алгоритмом CAP, відновлює власне сигнал, що передавався, з використанням тих же алгоритмів, що й приймач QAM-модульованого коливання. Тому, теоретично приймач CAP може взаємодіяти з передавачем QAM.

На цей час зустрічають такі типи алгоритму CAP, як CAP-4, CAP-8, CAP-16, CAP-32, CAP-64, CAP-128 та CAP-256. В залежності від типу алгоритму відносне співвідношення сигнал/шум (SNR) змінюється від 14,5 до 33,8 dB.

До переваг цих алгоритмів слід віднести високу енергетичну ефективність сигналу, який формується. Саме цей алгоритм теоретично здатен забезпечити максимальне значення співвідношення SNR і, як наслідок, передачу сигналу на найбільшу відстань.

Основний недолік цього метода полягає у відсутності стандарту, який визначає процедури, у відповідності з якими виконується перетворення сигналу.

7.6. Критерії оцінки систем закриття мови

Існують чотири основних критерії, по яких оцінюються характеристики пристроїв закриття мовних сигналів, а саме: розбірливість мови, впізнаваємість, ступінь закриття й основні технічні характеристики системи.

Прийнятною чи комерційною якістю відновленої на прийомному кінці мови вважається таке, коли слухач може без труднощів визначити голос того що говорить і зміст вимовного повідомлення. Крім цього, під гарною якістю переданого мовного сигналу мається на увазі і можливість відтворення емоційних відтінків і інших специфічних ефектів розмови, властивим бесідам віч на віч.

Відновленого мовного сигналу, що впливають на якість, параметри вузькосмугових закритих систем передачі мови визначаються способами кодування, методами модуляції, впливом шуму, інструментальними помилками й умовами поширення. Шуми і спотворення впливають на характеристики кожного компонента системи по-різному, і зниження якості, що відчувається користувачем, походить від сумарного ефекту зниження характеристик окремих компонентів. Існуючі об'єктивні методи оцінки якості мови і систем не пристосовані для порівняння характеристик вузькосмугових дискретних систем зв'язку, у яких мовний сигнал перетвориться в систему параметрів на передавальній стороні, передається по каналу зв'язку, а потім синтезується в мовний сигнал у приймачі.

Існуючі суб'єктивні методи вимірів розбірливості і природності відрізняються значною трудомісткістю, оскільки в цій справі багато чого залежить від використовуваного словника, обраного каналу зв'язку, діалекту, віку й емоційного стану дикторів які проводять випробуварря. Тому проведення вимірів для одержання статистично надійних і повторюваних оцінок параметрів системи при умовах, що змінюються, вимагає великих витрат.

При використанні радіоканалів ці труднощі ще більш зростають через невизначеність умов поширення, і досягти повторюваності результатів неможливо без застосування моделей радіоканалів.

Для дуплексних систем додатковий вплив на якість робить часова затримка сигналу, внесена мовним скремблером чи шифратором.

Оскільки основним показником таємності переданих мовних повідомлень є його нерозбірливість при перехопленні потенційними противниками що підслухують, порівняння по ступенях захисту є визначальним моментом при виборі користувачем конкретної системи закриття мови.

Як правило, аналогові скремблери використовуються там, де застосування цифрових систем закриття мови утруднено через наявність можливих помилок передачі (наземні лінії зв'язку з поганими чи характеристиками канали далекого радіозв'язку), забезпечують тактичний рівень захисту і добре охороняють переговори від сторонніх "випадкових ушей", що мають обмежені ресурси, будь то сусіди чи товариші по службі. Для таких застосувань придатні системи із статичним закриттям, тобто здійснюючі шифрування по фіксованому ключі.

Якщо ж необхідно зберегти конфіденційність інформації від можливих конкурентів, що володіють достатнім технічним і спеціальним оснащенням, то потрібно застосовувати аналогові скремблери середнього рівня закриття з динамічно мінливим у процесі розмови ключем. Природно, що ці системи будуть дорожче, ніж системи закриття з фіксованим ключем, однак вони настільки ускладнять роботу супротивників по розробці алгоритму, що дешифрує, що час, витрачений на це, значно знецінить добуту інформацію з перехопленого повідомлення.

Оскільки в таких пристроях закриття, як правило, перед початком повідомлення передається синхропослідовність, що містить частину додаткової інформації про ключ саме цього переданого повідомлення, у супротивника є тільки один шанс спробувати його розкрити, перебравши велику безліч ключових установок, і, якщо ключі міняються щодня, то навіть при відомому алгоритмі перетворення мови супротивнику прийдеться перебрати багато тисяч варіантів у пошуках дійсної ключової підстановки.

У випадку, якщо є припущення, що з метою добування вкрай цікавлячої його інформації супротивник може скористатися послугами висококваліфікованих фахівців і їхнім технічним арсеналом, то для того, щоб бути упевненим у відсутності витоку інформації, необхідно застосовувати системи закриття мови, що забезпечують стратегічну (найвищу) ступінь захисту. Це можуть забезпечити лише пристрою дискретизації мови з наступним шифруванням і новий тип аналогових скремблерів. Останні використовують методи перетворення аналогового мовного сигналу в цифрову форму, потім застосовують методи криптографічного закриття, аналогічні тим, що використовуються для закриття даних, після чого результуюче закрите повідомлення перетвориться назад в аналоговий сигнал і подається в лінію зв'язку. Для розкриття отриманого сигналу на прийомному кінці

виконуються зворотні перетворення. Ці новітні гібридні пристрої легко адаптуються до існуючих комунікаційних мереж і пропонують значно більш високий рівень захисту мовних повідомлень, чим традиційні аналогові скремблери, зі збереженням усіх переваг останніх у розбірливості й впізнаваємості відновленої мови.

Слід зазначити, що в системах засекречування мови, заснованих на шифрі перестановки N мовних елементів, загальне число ключів-перестановок дорівнює N!. Однак це число не відбиває реальної криптографічної стійкості системи через надмірність інформації, що міститься в мовному сигналі, а також через розбірливість недосконалим образом переставленої й інвертованої мови. Тому криптоаналітику супротивника часто необхідно випробувати лише K«N! випадкових перестановок для розкриття мовного коду. Цей момент варто враховувати при виборі надійної системи аналогового скремблювання.

Тенденції розвитку систем закриття мови

Метою сучасних досліджень методів закриття й обробки мовних сигналів є поліпшення параметрів для заданих каналів передачі з використанням досягнень мікроелектронної технології.

У найближчі десять років не очікується яких-небудь значних змін в області аналогового скремблювання. Очікується, що аналогові скремблери і далі будуть використовуватися на неякісних лініях зв'язку, поки не будуть створені надійні модеми з виправленням помилок, що виникають у процесі цифрової передачі по таких каналах.

Деякі публікації [5] свідчать про те, що розвиток цифрових процесорів обробки сигналів (ЦПОС) дозволить набагато ефективніше використовувати існуючі алгоритми при загальному зниженні габаритів і енергоспоживання апаратури закриття мовних сигналів. Завдяки розвитку ЦПОС вже вдалося набагато ускладнити смугові скремблери [5], у міру удосконалювання яких легше буде реалізовувати складні методи скремблювання, наприклад, комбіновані частотно-часові. Застосування ЦПОС дозволить підвищити якість мови за рахунок більш точних методів фільтрації й обробки. Незабаром варто очікувати появи на ринку достатньої кількості аналогових скремблерів нового типу, що забезпечують рівень захисту мовних сигналів, порівнянний з цифровими пристроями закриття мови, при високій якості й впізнаваємості відновленого мовного сигналу, властивого аналогової скремблерам. У якості одного з перспективних напрямків аналогового скремблювання в [5] розглядається гармонійна компресія в часовій області (Time Domain Harmonic Compression - TDHC), що може використовуватися для звуження смуг частот усіх видів скремблерів.

Ріст попиту на найпростіші скремблери в таких областях, де вони раніш не застосовувалися, привів до появи пристроїв закриття мови, реалізованих в одному кристалі. Так у [5] повідомляється про початок виробництва спеціалізованої мікросхеми, що дозволяє

здійснювати алгоритм закриття мови на основі часових перестановок і призначеної для використання в радіозв'язку таксі й автобусів.

Надалі серед систем дискретизації мови з наступним шифруванням поряд з наступним розвитком систем закриття мовних сигналів на основі відомих алгоритмів очікується широке поширення криптографічних систем з відкритими ключами, що, наприклад, дозволить створити нову захищену систему телефонного зв'язку з числом абонентів до 3 млн. для співробітників міністерства оборони США і його підрядчиків. Основні зусилля в області удосконалювання дискретної техніки кодування спрямовані на поєднання високих якостей звучання синтезованої мови в середньошвидкісних вокодерах з достоїнством низкошвидкісних перетворювачів - малою смугою частот. Одним з можливих способів є багатоімпульсне збудження вокодера, здатне замінити параметри основного тону й ознаки "тон/шум" набором імпульсів з різними амплітудами.

Розвитком ідеї векторного кодування є побудова вокодерів з кодовим збудженням і самозбудних вокодерів. Основний принцип їхньої роботи подібний із багатоімпульсним збудженням. Передані параметри заміняються єдиною адресою, що вибирає найбільш придатну форму сигналу збудження з числа сигналів, записаних у банку кодів.

Головні труднощі реалізації багатоімпульсного і векторного методів складаються у великій кількості розрахунків, проведених аналізатором з метою оптимального вибору форми сигналу збудження. Тому визначені зусилля спрямовані на спрощення цього аналізу.

Подальше зниження необхідної швидкості передачі можливо шляхом параметризації мови, що обгинає спектр, у залежності від частот формант і амплітуд. Труднощі точної і надійної ідентифікації формант обумовлюють низька якість формантного вокодеру. Однак при правильному керуванні його синтезатор відновлює мову з високою якістю. Використання коефіцієнтів лінійного передбачення для визначення частот формант дозволить сполучити властивості формантного вокодеру і вокодеру з лінійним передбаченням, але при більш низькій швидкості передачі. Очікується доведення швидкості передачі до величини 600 біт/с.

У більшості технічних додатків використовується мова з обмеженим словником, і перехід до кодування лише деяких звуків і слів може набагато знизити вимоги до швидкості передачі. Наприклад, для словника в 500 слів необхідна швидкість не перевершує 30 біт/с. Підвищена чутливість до помилок каналу зв'язки може бути подолана використанням завадостійкого кодування. Потенційний недолік таких систем полягає в тім, що синтезована на прийомній стороні мова не буде містити індивідуальних характеристик голосу того що говорить. Однак ці труднощі можна перебороти, використовуючи ознаку автентичності, яка передана заздалегідь. У майбутньому стане можливим керування синтезатором для імітації

характеристики,того що говорить з використанням інформації, що міститься в посилці автентичності. Далі наведемо приклади пристроїв закриття мовних повідомлень.

PRAGMA

- Автономне живлення
- Висока стійкість
- Посилена ключова система- 1024біт
- Можливість оперативної зміни майстра-ключа користувачем
- Можливість побудова конфіденційного зв'язку в необхідному місці
- Оптимізований для роботи на “далеких” каналах зв'язку (міжнародних, супутникових)

Основні характеристики

- симетричне шифрування за ДСТ 28147-89
- алгоритм мовоперетворення - CELP 4800 бод
- захист факсимільних документів шляхом **шифрування** переданого зображення,
- **у захищений факсимільний документ додається “шапка”, зовнішній вигляд якої може задавати сам користувач.**
- захист факсимільних документів відбувається автоматично, не вимагаючи втручання користувача
- захист міжкомпютерного обміну даними
- система відкритого розподілу ключів Диффи-Хеллмана (**1024 біт**) створює унікальний ключ для кожного сеансу зв'язку й виключає необхідність уведення сеансових ключів користувачем
- уведено **систему перевірки дійсності, що** виключає можливість втручання “третьої” сторони (атаки виду ”людина посередине”), навіть при наявності подібного пристрою. Вирішується це застосуванням алгоритмів “захищені переговори про узгодження ключа"
- передбачено можливість зміни ключових і ін. параметрів роботи пристрою самим користувачем

- для зручності користувачів: при необхідності оперативної зміни ключових параметрів передбачений **інжектор ключів**, що дозволяє міняти ключові параметри пристрою. При цьому здійснюється перевірка на цілісність ключових параметрів, що запобігає несанкціоноване нав'язування параметрів ключової системи
- **виключено можливість впливу виробника пристрою на систему захисту, який огранізується користувачем**
- Автономне живлення “PRAGMA” дозволяє користувачеві створювати мережі закритого зв'язку там, де Ви вважаєте за необхідне. Немає залежності від джерела живлення.
- Важливо, що “PRAGMA” забезпечує зв'язок високої якості не тільки на “близьких” міжміських каналах, але й на “далеких”- міжнародних, супутникових. Крім того, продукт оптимізований для місцевих ліній зв'язку з більшим загасанням і поганим співвідношенням сигнал/шум.
- У порівнянні із шифраторами попереднього покоління, посилена ключова система-1024 біт. Передбачено інжектор ключів, що дозволяє оперативно міняти ключові параметри без підключення до комп'ютера.

“PRAGMA” являє собою шифратор нового покоління, що дозволяє створювати конфіденційні мережі зв'язку, із захистом усього каналу, від одного шифратора до іншого, запобігає прослуховування мовних переговорів, перехоплення факсимільних документів і переданих даних при межкомп’ютерному обміні. Максимальна кількість абонентів мережі необмежено.

Якість відновленого (синтезованого) сигналу практично не відрізняється, а в багатьох випадках вище звичайного відкритого.

“PRAGMA” виконаний у вигляді приставки до телефонного (факсимільному) апарату й підключається між телефонною лінією й телефоном. Для передачі даних пристрій з'єднується з комп'ютером по послідовному комунікаційному порту (COM).

Захист мовної інформації здійснюється з використанням вокодерного перетворення по алгоритму CELP зі швидкістю передачі 4800 біт/сек. і шифрування по алгоритму ГОСТ28147-89 з високою стійкістю до розкриття.

При захисті факсимільних документів **шифрується саме зображення**, передане на швидкостях 2400-9600 біт/сек. по протоколах v.27ter, v.29 ITU-T. При цьому сигнали в телефонній лінії не відрізняються від звичайної факсимільної передачі.

При захисті межкомп’ютерному обміну пристрій працює під керуванням будь-якого комунікаційного пакета на ПЭВМ як Hayes-сумісний модем і забезпечує шифрування /дешифрування даних по алгоритму ДЕРЖСТАНДАРТ28147-89 .

Для побудови системи захищеного зв'язку необхідний як мінімум два пристрої ” PRAGMA ”. Приставки включаються в розрив між телефонним (факсимільним) апаратом і телефонною лінією в кожного абонента й забезпечують захист від прослуховування у відкритому каналі зв'язку на ділянці від одного пристрою до іншого.

При включенні живлення здійснюється самотестування пристрою й перехід у режим очікування. Про правильну роботу в режимі очікування свідчить почергове включення/вимикання індикаторів режимів роботи. У такому стані (а так само при виключеному живленні) приставка “прозора” для всіх операцій з телефонним (факсимільним) апаратом і не заважає звичайній роботі користувача.

Захист переговорів.

Перевод пристрою в режим захисту переговорів повинен виконуватись після встановлення зв'язку між абонентами й може здійснюватися декількома способами:

- натисканням кнопки;
- набором певної комбінації цифр (символів) із клавіатури телефонного апарата в режимі тонального набору;
- пристрій може включатися автоматично при виявленні службових посилок з боку другого абонента.

На період синхронізації роботи пристроїв і обміну ключовою інформацією мигає індикатор захищеного зв'язку **Secure**. При встановленні захищеного зв'язку індикатор **Secure** включений постійно.

Перехід у режим відкритого зв'язку (очікування) здійснюється натисканням відповідної кнопки або автоматично, при перемиканні у відкритий режим протилежного абонента. Якщо лягає трубка телефонного апарата, приставка відключається й вертається в режим очікування.

Захист факсимільних документів.

Захист факсимільних документів здійснюється без втручання користувача. Пристрій включається при виявленні початку факсимільної процедури, шифрує переданий документ (дешифрує прийнятий) при наявності такої ж приставки (з таким же ключем) із протилежної сторони й вертається в режим очікування.

Захищений документ позначається спеціальним рядком на початку кожної сторінки.

Передбачено можливість блокування прийому й/або передачі факсимільного документу у незахищеному режимі.

Захист даних.

Приставка “ PRAGMA ” дозволяє захистити від несанкціонованого використання документи, бази даних, передані у вигляді файлів з одного комп'ютера на інший за допомогою модему.

Пристрій при цьому включається замість звичайного модему й працює під керуванням стандартного комунікаційного пакета на ПЕОМ у режимі для виділеної лінії.

Питання для самоперевірки

1. Які методи використовуються для закриття мовних повідомлень?
2. Що таке скремблювання мови?
3. Назвіть основні види систем закриття мовних повідомлень.
4. Які параметри мови можуть змінюватись в аналогових скремблерах?
5. В чому різниця між статистичними та динамічними системами аналогового скремблювання?
6. Яким чином можна підвищити ступінь закриття в аналогових скремблерах?
7. В чому принципова різниця між аналоговим скремблером та систем дискретизації мови з наступним шифруванням ?
8. За допомогою яких пристроїв можна перейти від широкосмугових до вузько смугових систем закриття мовних повідомлень?
9. Які критерії слід застосовувати для вибору того чи іншого пристрою закриття мовних повідомлень?

Розділ 8. Дослідження особливостей технічного захисту інформації в процесах експлуатації відомчої телекомунікаційної мережі цивільної авіації України.

8.1. Аналіз сучасного стану об'єкта досліджень – мережі ATN.

8.1.1. Призначення і принципи побудови сучасних авіаційних телекомунікаційних систем.

Відповідно до вимог ICAO (International Civil Aviation Organization) авіаційний електрозв'язок (АЕЗ) у цивільній авіації (ЦА) має забезпечувати потреби в електрозв'язку наступних служб: обслуговування повітряного руху (ОПР), аеронавігаційної інформації, метеорологічного забезпечення, пошуку та рятування. При цьому мають бути виконані конкретні вимоги щодо надійності і цілісності системи, безперервності обслуговування повідомлень, затримки проходження друкованих та цифрових даних і повідомлень мовного зв'язку [1 – 2].

У теперішній час поточні потреби ОПР у більшості регіонів задовольняються за рахунок використання:

- ліній передавання та центрів мереж авіаційного фіксованого електрозв'язку AFTN (Aeronautical Fixed Telecommunication Network);
- ліній передавання та центрів загальної мережі обміну даними ICAO-CIDIN (Common ICAO Data Interchange Network);
- ліній передавання та центрів зв'язку європейського метеорологічного оперативного зв'язку;
- ліній оперативно-мовного зв'язку ОПР (мережа безпосередньої взаємодії диспетчерських пунктів БВДП);
- ліній передавання систем обміну даними між ЕОМ ОПР;
- ліній передавання мережі Міжнародного товариства з авіаційного електрозв'язку SITA (Societe International de Telecommunication Aeronautiques);
- радіоканалів зв'язку „Земля-Борт-Земля".

Авіаційний електрозв'язок у ЦА має забезпечувати вирішення таких основних задач [1 – 2]:

- передавання на борт повітряного судна (ПС) різних повідомлень по ОПР, які спрямовані на забезпечення безпеки та регулярності польотів, сервісу обслуговування пасажирів;
- передавання екіпажем ПС вказівок і розпоряджень та отримання від них донесень і

повідомлень на усіх етапах польоту від злету до посадки включно;

- передавання та приймання повідомлень про повітряну та метеорологічну обстановку;
- обмін відповідними повідомленнями з взаємодіючими пунктами управління й органами інших відомств, у тому числі міжнародних;
- взаємодію між службами та підрозділами авіапідприємств;
- передавання розпоряджень, вказівок та інших повідомлень від керівних органів ЦА в підлеглі організації і підприємства та отримання від них повідомлень і донесень.

Функції АЕЗ реалізуються сукупністю центрів комутації, вузлів зв'язку, прийомо-передавальних центрів, станцій і кінцевих пристроїв, які з'єднані між собою каналами і лініями передачі в порядку, що відповідає прийнятій системі організації зв'язку.

Авіаційний електрозв'язок має задовольняти високі вимоги щодо оперативності, надійності, достовірності та швидкості передачі повідомлень, необхідної скритності, максимальної економічності організації та функціонування.

По функціональному призначенню АЕЗ поділяється на авіаційний повітряний електрозв'язок (АПЕЗ) і авіаційний наземний електрозв'язок (АНЕЗ). По міжнародній термінології АПЕЗ відповідає авіаційна рухома служба зв'язку (R), а АНЕЗ – авіаційна фіксована служба зв'язку (AFS-Aeronautional Fixed Service).

АПЕЗ організується у відповідності з діючою структурою керування повітряним рухом (КПР) і має забезпечувати [1-7]:

- зв'язок по КПР у районах аеродрому (руління, зліт, посадка, польоти по колу та на підході до аеродрому);
- зв'язок по КПР на повітряних трасах України, на місцевих повітряних лініях (МПЛ) і при використанні авіації в народному господарстві (ВАНГ), на міжнародних повітряних трасах;
- інформаційно-командний дальній зв'язок з центральною диспетчерською службою (ЦДС) ЦА;
- радіомовлення метеоінформації екіпажам ПС;
- зв'язок ПС з планово-диспетчерською службою підприємства (ПДСП);
- зв'язок між екіпажами ПС для взаємодії (у випадку необхідності);
- зв'язок аварійно-рятувальної служби з іншими абонентами мереж АЕЗ;
- зв'язок спеціального призначення;

АНЕЗ організується з урахуванням діючої ієрархічної структури диспетчерських пунктів служби руху й органів ОПР, структури місць базування та розташування авіазагонів, аеродромів, агентств повітряних сполучень, установ, підприємств ЦА, структури інших служб і органів ЦА, установ і служб взаємодіючих відомств і має забезпечувати:

- взаємодію диспетчерських пунктів служби руху;

- польоти повітряних суден;
- керування виробничою і технологічною діяльністю інших служб ЦА;
- міжаеропортовий зв’язок;
- зв’язок агентств повітряних сполучень (АПС) і пасажирів;
- внутрішньо-аеропортовий зв’язок;
- міжнародний зв’язок;
- зв’язок по організації КПР;
- передавання та приймання метеорологічної інформації;
- комерційний зв’язок;
- виробничо-диспетчерський зв’язок;
- зв’язок спеціального призначення.

З метою усунення відомих недоліків АЕЗ і ефективного використання всіх можливостей автоматизованих систем ОПР у ЦА впроваджується інтегрована мережа передавання повідомлень ATN(Aeronautical Telecommunication Network). Вона має забезпечити міжмережну взаємодію обчислювальних систем і обладнання даних, які функціонують у наземних пунктах AFS і в межах бортових локальних мереж (Local Array Network) повітряних суден.

8.1.2. Концепція побудови авіаційної цифрової мережі інтегрального обслуговування ATN

8.1.2.1 Призначення ATN

Головною умовою успішного впровадження авіаційної цифрової мережі інтегрального обслуговування (ЦМІО) ІСАО вважає визнання таких концептуальних положень [4,7]:

- усе більше впровадження і використання засобів комп’ютеризації й автоматизації ОПР вимагає вдосконалення передавання даних між кінцевими ЕОМ та користувачами у тому числі, передавання даних між бортовими і наземними ЕОМ, які обслуговують фіксованих і мобільних користувачів;
- підвищення рівня автоматизації процесів ОПР вимагає реалізації на борту ПС і в наземних умовах інфраструктури мережі передавання даних, яка забезпечує більш широкі телекомунікаційні можливості зв'язку і більш чітку конфігурацію в порівнянні з існуючою інфраструктурою;
- реальний успіх автоматизації процесів ОПР досягається тільки в тому випадку, коли бортові обчислювальні системи забезпечують міжмережну взаємодію й оброблення даних аналогічно наземним ЕОМ, а не використовуються в теперішній якості бортових терміналів.

За визначенням МККТТ під ЦМІО (ISDN - Integrated Services Digital Network) мається на увазі така мережа електрозв'язку, в якій одні й тіж самі прилади цифрової комутації і цифрові тракти передавання використовуються для встановлення з'єднань більш ніж одного виду зв'язку [1,8]. Базою для ISDN є цифровізована мережа з ІКМ (PCM -Pulse Code Modulation).

Мережа авіаційного електрозв’язку ATN, концепція якої розроблена ICAO, є інфраструктурою міжмережної взаємодії. Вона забезпечує взаємодію наземних підмереж передавання даних, підмереж передавання даних "Повітря - Земля" (A/G - Air/Ground) і підмережі передавання даних бортового обладнання (LAN) (рис.1.1). Взаємодія реалізується завдяки спільним режимам і протоколам інтерфейсу, які базуються на міжрівневій еталонній моделі взаємодії відкритих систем (EMBBC), що рекомендована документом ISO/IEC 74981.

Взаємодія характеризує спроможність ATN забезпечити наскрізне передавання даних між кінцевими системами, навіть якщо в ATN включено різні підмережі.

Кінцевою системою (ES - End System) є система, яка охоплює сім рівней EMBBC та один або декілька прикладних процесів кінцевого користувача (рис.1.2).

Підмережею ATN називають діюче обладнання мережі передавання даних, яке використовує однорідний протокол і план та знаходиться під управлінням одного повноваженого органа. Для повідомлень, які належить передавати між наземними підмережами (АНЕЗ) і підмережами LAN на ПС, у ATN визначено перехідний елемент. Він називається роутером (трансирувальником або маршрутизатором). З'єднання підмереж, які самостійні фізично, логічно або адміністративно, виконуються міжмережними роутерами (трасирувальниками) в місцях з'єднання [2,4]. Підмережі відносяться до проміжних систем (IS - Intermediate System).

Мережа ATN призначена надавати на спеціальній основі телекомунікаційне обслуговування для передавання даних організаціям, які займаються ОПР, та агентствам, які експлуатують повітряні судна. Мережа ATN забезпечує наступні види електрозв'язку:

- зв'язок з метою обслуговування повітряного руху (ATSC - Air Traffic Services Communication);
- авіаційний оперативний контроль (AOC - Aeronautical Operation Control);
- авіаційний адміністративний зв'язок (AAC - Aeronautical Administrative Communication);
- авіаційний зв'язок для пасажирів (APC - Aeronautical Passenger Communication).

Мережа ATN [1,4]:

- надає користувачам надійний наскрізний зв'язок, необхідний для забезпечення безпечного та ефективного ОПР;
- забезпечує передавання даних, яке дозволяє виконувати вимоги користувачів щодо

захисту та безпеки зв'язку;

- базується на міжнародних стандартах передавання даних, які мають сприяти розробці сумісних систем та стимулювати надання мережних видів обслуговування на конкурентній основі;
- забезпечує різні категорії (класи) обслуговування для різних видів використання;
- визначає архітектуру, яка дозволяє об'єднувати суспільні та приватні підмережі, що забезпечує використання діючої та плануємої інфраструктури і мережних програмно-технічних засобів.

Інтегрована АНЕЗ - ATN включає наземну підмережу ОПР, яка охоплює аеродромно диспетчерські пункти (АДІ1), бази даних ОПР, бази метеоданих (БМД), пункти керування на маршруті. З допомогою роутерів наземних підмереж ОПР користувачі зв'язуються [4]:

- з місцевими наземними підмережами , а через них з базами даних авіаційного оперативного зв’язку (АОЗ);
- з підсистемами АОЗ і базою метеоданих;
- з рухомими підмережами: ВЧ-каналів цифрового зв'язку (HFDL - High Frequency Data Link);
- ДВЧ - каналів цифрового зв'язку (VDL - Very High Frequency Data Link), авіаційного мобільного супутникового зв'язку (AMSS - Aeronautical Mobile Satellite Service), каналів вторинних оглядових радіолокаторів в режимі S (SSR - Secondary Surveillance Radar Mode S), аеродромного обслуговування (Gate Link) [1,3].

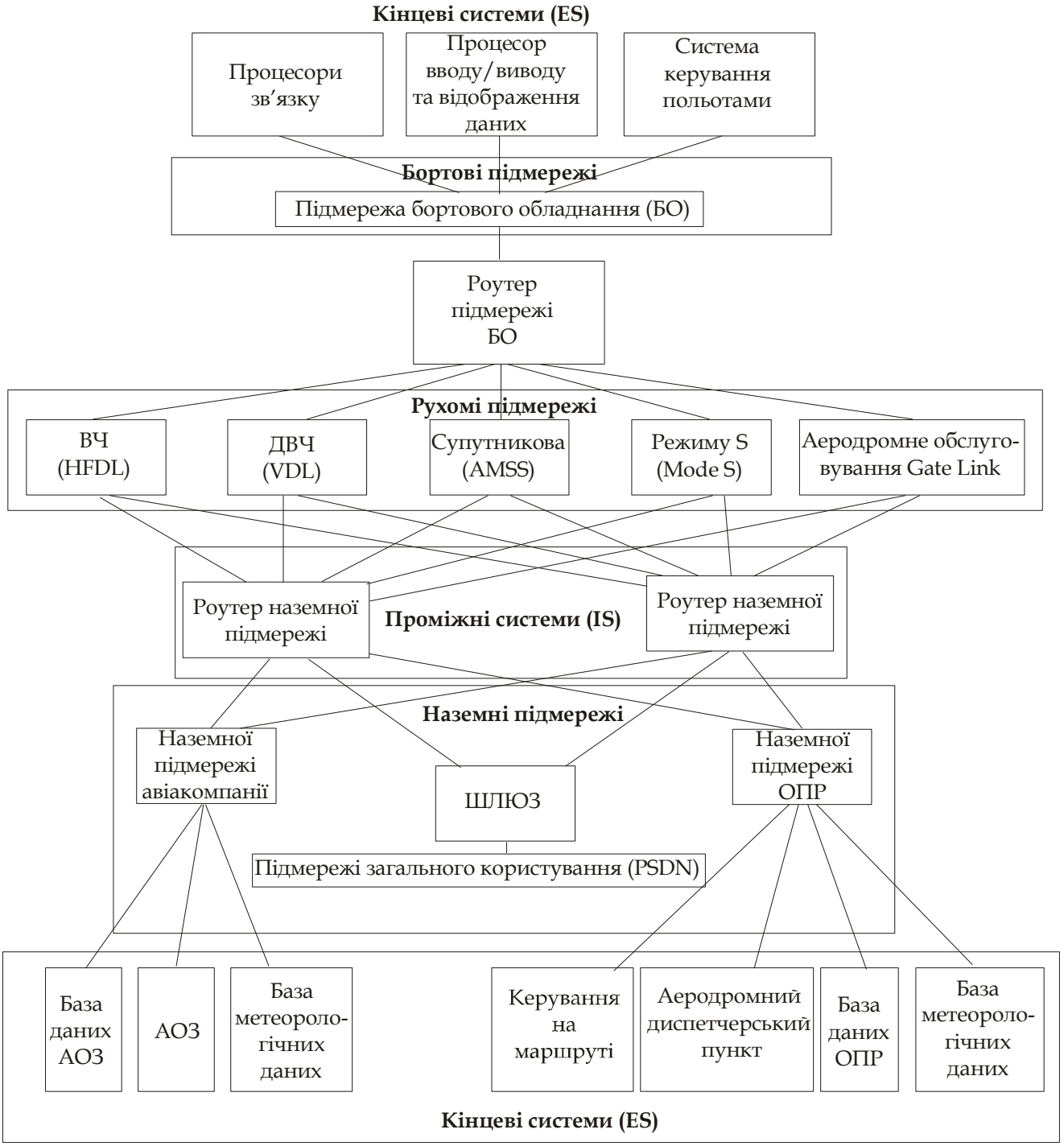


Рис 8.1 Архітектура мереж ATN

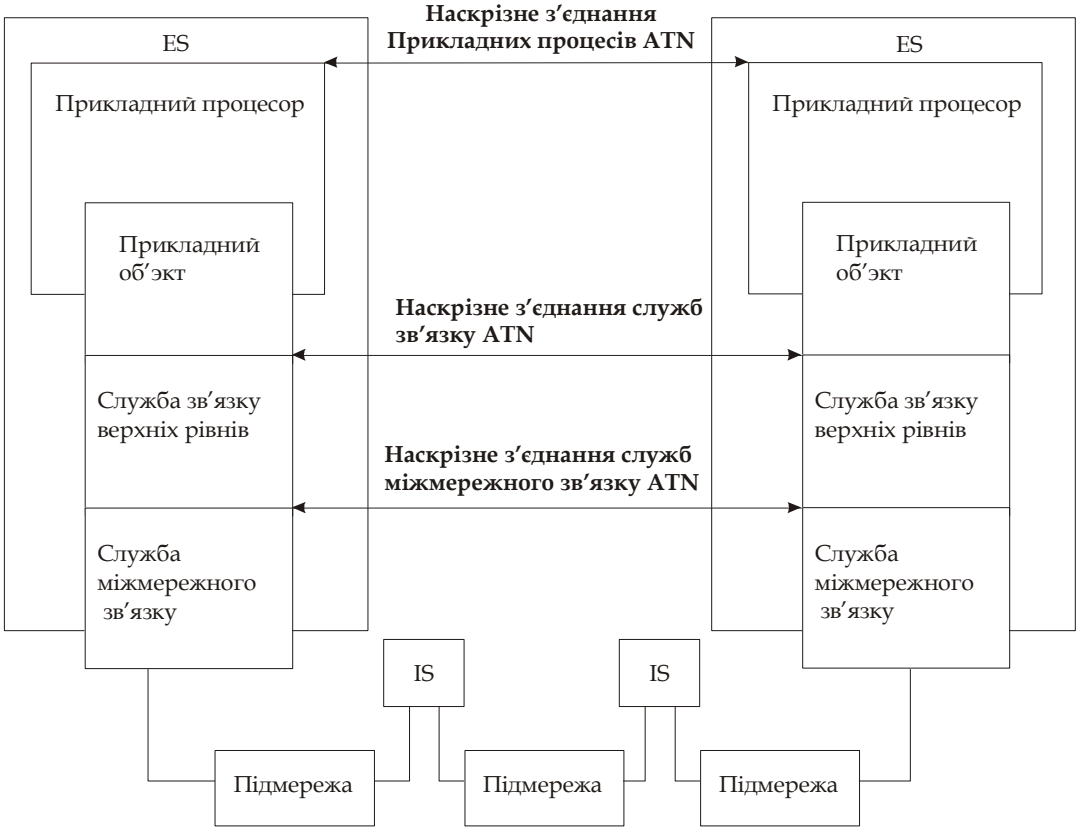


Рис. 8.2. Концептуальна модель ATN за ICAO

8.1.2.2. Системні вимоги

За рекомендаціями ICAO вимоги системного рівня являють собою технічні вимоги високого рівня, які базуються на експлуатаційних вимогах і обмеженнях технічного, адміністративного та організаційного характеру. Вимоги системного рівня виступають основою для функціональних вимог і вимог більш низького рівня.

У відповідності з рекомендаціями ICAO мережа ATN має забезпечити [1,2,4]:

- спрощений перехід до майбутніх варіантів служб авіаційного електрозв'язку;
- інтеграцію наявних користувачів і систем AFTN, CIDIN, VCS (Voice Communication System – система мовного зв'язку), ACARS (Aircraft Communications Addressing & Reporting System – система зв'язку ПС для адресації і передавання повідомлень) та інші в архітектуру ATN;
- передавання інструкцій з КПР на борт ПС по лініям ПД тільки керуючим органом ОПР в зонах повітряного простору, які йому підпорядковані;
- маршрутизацію у відповідності з встановленою стратегією маршрутизації;
- однозначну адресацію всіх кінцевих, прикінцевих і проміжних систем свого складу;
- визначення виду обміну даними тільки по дозволеним лініям передачі у відповідності з типами і категоріями повідомлень, які визначені користувачем;
- обмін прикладною інформацією, коли є одна або декілька санкціонованих ліній передавання;

- можливість, отримуючи, повідомлення визначити ініціатора обміну;
- доцільне та ефективне використання підмереж з лініями передачі, які мають обмежену ширину смуги ачстот;
- з'єднання бортової і наземної проміжних систем альтернативними рухомими підмережами;
- з'єднання бортової проміжної системи з декількома наземними проміжними системами;
- можливість державам і організаціям назначати адреси і назви в межах їх адміністративних областей;
- можливість встановлення, підтримки, висвободження та перерви рівноправних прикладних асоціацій для різних використань;
- надання зв'язку ОПР (ATSC - Air Traffic Services Communication) у відповідності з класом ATSC (див. табл. 8.1.), який визначається максимальною затримкою ΔT max наскрізного проходження повідомлення через ATN в одному напрямку (імовірність проходження 0,95).

Таблиця 8.1

Затримки проходження повідомлення через АТМ

Клас ATSC	A	B	C	D	E	F	G	H
Максимальна затримка ΔT max , с	Резерв	4,5	7,2	13,5	18,0	27,0	50,0	100,0

Мережа ATN враховує пріоритети передавання повідомлень, які подано у табл.1.2. При цьому до зв'язку з безпеки і регулярності польотів відносяться пріоритети, які лежать вище п'ятого мережного рівня ATN. В підмережі SSB Mode S пріоритети з 14 по 10 є високими, а з 9 по 6 - низькими. Серед інших категорій повідомлень ATN, тобто від 0 до 5, в підмережі режиму S допускається проходження тільки тих, які стосуються регулярності і безпеки польотів. Щодо підмережі VDL 1 і 2, то в них відсутні певні механізми забезпечення пріоритетів [1,2].

Таблиця 8.2

Пріоритети передавання повідомлень.

Категорія повідомлень		Пріоритет відповідного рівня		
		Транспор	Мережний	Під мережі
Керування мережею / системою		0	14	14
Надзвичайні (про лихо)		1	13	14
Термінові		2	12	14
З безпеки польотів	Вищого пріоритету	3	11	11
	Звичайного пріоритету	4	10	11

Метеорологічні	5	9	8
З регулярності польотів	6	8	7
Служби авіаційної інформації	7	7	6
Мережні / системні	8	6	5
Авіаційні, адміністративні	9	5	5
(не надано)	10	4	
Адміністративні термінові та пов'язані зі статусом ООН	11	3	3
Адміністративні вищого пріоритету та державні/урядові	12	2	2
Адміністративні звичайного	13	1	1
Адміністративні нижчого	14	0	0

Структура протоколів ATN, яка відповідає EMBBC ISO показана на рис. 8.3. Мережний рівень тут подано трьома підрівнями зі своїми протоколами:

- міжмережний протокол IP (Internet Protocol) зокрема, протокол мережного рівня без встановлення з'єднання CLNP (Connectionless Network Protocol);
- протокол обміну маршрутною інформацією RP (Routing Protocol);
- протокол залежної від підмережі функції конвергенції SNDCF (Subnetwork Dependent Convergence Function);
- протокол доступу до підмережі SNAcP (Subnetwork Access Protocol).
- протокол міжобласного обміну маршрутною інформацію IDRP (Inter Domain Routing Information Exchange Protocol)

При цьому порт 1 визначає точки доступу до транспортних послуг, порт 2 – порт користувача, порт 3 - порт провайдера мережі, порт 4 - порт приєднання підмереж.

Одним з основних видів використання ATN в зв'язку "Земля - Земля" (G/G) є обмін даними між органами ОПР (AIDC - Air traffic service Inter facility Data Communication). Мережа ATN забезпечує наступні функції AIDC: повідомлення про польоти, координація польотів, передавання керування, передавання зв'язку, передавання даних, спостереження, передавання даних загального характеру.

З метою ефективного і якісного виконання покладених на ATN задач інтеграція діючих систем АНЕЗ має враховувати позитивні риси та використовувати сучасні телекомунікаційні технології. Основними з них є технології, які базуються на стандартах ISDN, Frame Relay(FR), ATM (Asynchronous Transfer Mode), TCP/IP (Transmission Control Protocol / Internet Protocol).

Розглянемо призначення та особливості цих технологій з точки зору використання в ATN

8.1.2.3. Загальна характеристика сучасних телекомунікаційних технологій в ATN

Сучасний період науково-технічного прогресу характеризується стрімким розвитком телекомунікаційних систем і мереж. Характерною рисою цього розвитку є впровадження прогресивних телекомунікаційних технологій, які базуються на цифрових методах передавання, приймання та оброблення повідомлень. Еволюційний розвиток телекомунікаційних технологій добре віддзеркалює так звана "хвильова" теорія розвитку [8,9]. Суть її в тому, що будь-яка нова технологія поступово з'являється на ринку, досягає в залежності від попиту, максимального розповсюдження, після чого поступово залишає ринок. Схематично хід такої еволюції показано на рис. 8.4. Рисунок показує, що на сучасному етапі розвитку цифрових телекомунікаційних технологій пікового розвитку сягають технології ISDN і Frame Relay. Обсяги Q використання виділених цифрових ліній передавання поступово знижуються. Попит на асинхронну технологію ATM поступово збільшується. Для кожної країни чи окремого регіона хід кривих на рис. 8.4 може відрізнятися по термінам наставання піків та їх амплітудам. Але загальний характер сімейства таких кривих , як правило, зберігається.

Причиною зміни технологій звичайно є більша економічна конкурентоспроможність нових технологічних рішень в порівнянні з діючими технологіями. При цьому не виключається можливість співіснування різних технологій (наприклад, ISDN і FR). Першим етапом переходу від аналогової до цифрової первинної мережі був етап створення інтегрованих цифрових мереж IDN (Integrated Digital Networks) в галузі цифрової телефонії. В мережах передавання даних в цей період на дільницях "вузол - вузол" починається використання виділених цифрових каналів мережі PDN (- плезіохронна цифрова ієрархія). Це суттєво підвищило якість передавання і стимулювало розвиток пакетної комутації (наприклад, протокол X.25).

Подальший розвиток телекомунікаційних технологій вимагав зростання пропускної спроможності мереж і об'єднання телефонії та передавання даних на єдиній цифровій основі. Це дало поштовх до переходу від IDN до ISDN. Технологія ISDN забезпечила транспортне середовище для передавання цифрового потоку від користувача до користувача. Якість цифрових каналів виявилась настільки високою, що протокол X.25 став збитковим і з нього стало можливим видалити алгоритми відновлення та квітирування даних. Результатом цього була поява протоколу Frame Relay (FR). Структура протоколу FR, має багато спільного зі структурою протоколів ISDN тому, що основні технології базуються на протоколі ITU-T G921/G931. Третім етапом удосконалення сучасних телекомунікаційних технологій є запровадження широкосмугових послуг, інтеграція їх з ISDN і перехід до B-ISDN (Broadband ISDN – широкосмугова ISDN) з зростанням обсягів використання технології ATM. Технологія ATM в теперішній час дозволяє інтегрувати в єдиний трафік різні за характером потоки різних користувачів і тому є більш складною, ніж попередні технології.[2, 3]

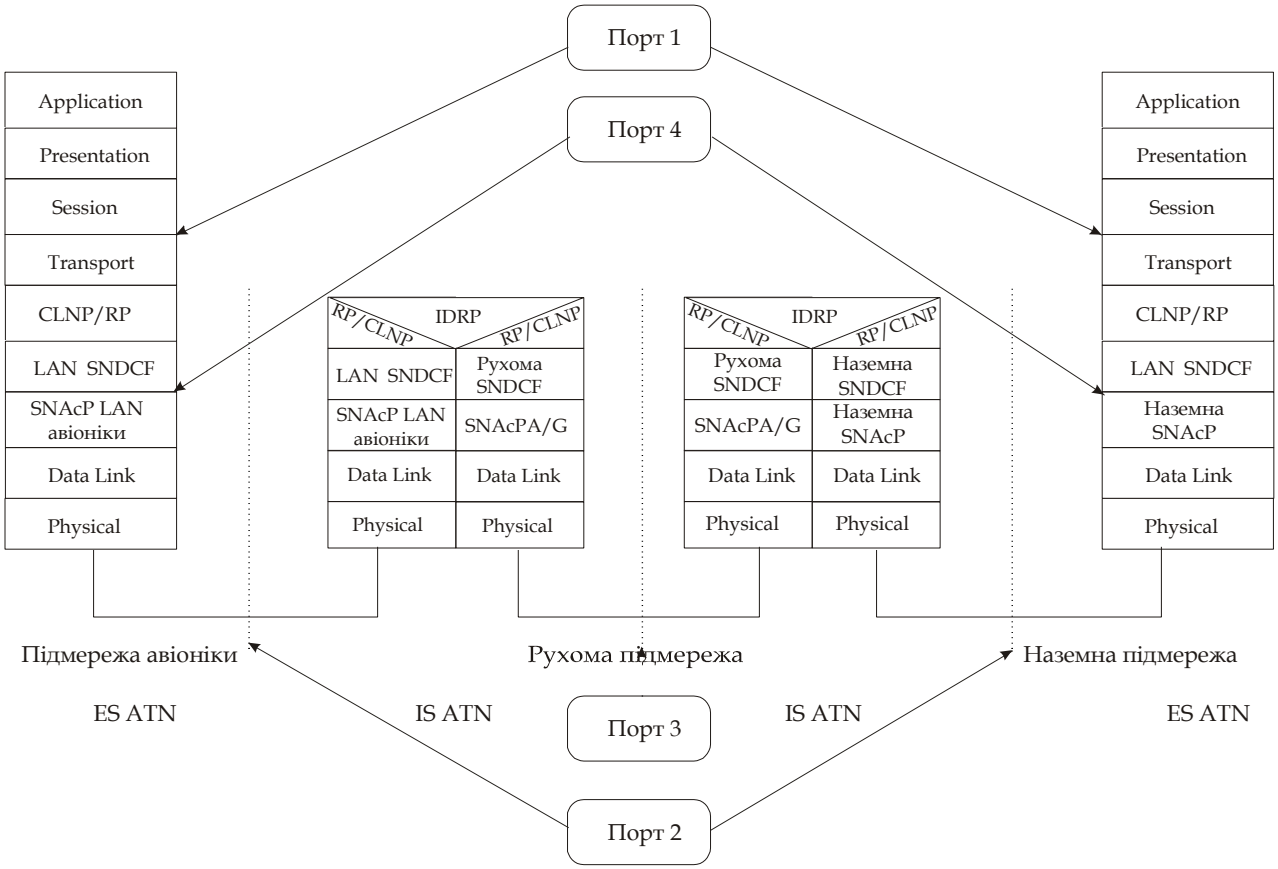


Рис. 8.3. Структура протоколів ATN

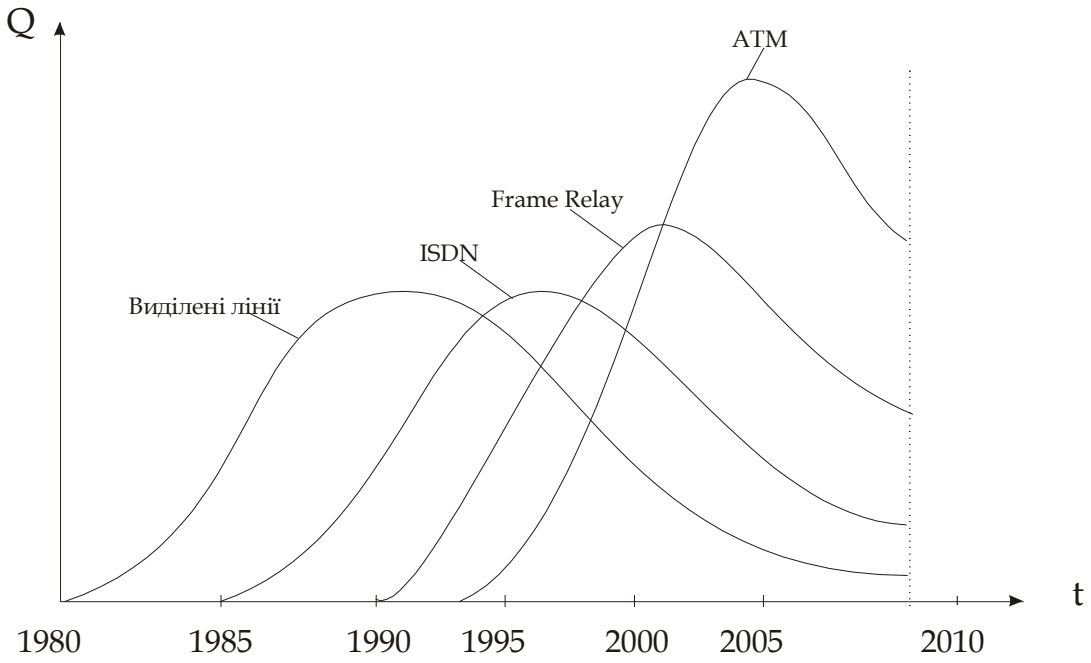


Рис. 8.4. Розвиток окремих цифрових телекомунікаційних технологій.

8.2. Аналіз особливостей використання в АНЕЗ ЦА ліній передачі мереж загального користування з сучасними технологіями

8.2.1. Особливості відомчої магістральної цифрової мережі зв'язку РЦ ЦА

У відповідності з рекомендаціями керівних документів ІСАО відомча мережа АНЕЗ ЦА будується, як правило, на базі орендованих магістральних ліній передачі мереж загального користування (МЗК), зокрема мереж передачі даних (МПД). Ця особливість зумовлює техніко – економічну доцільність та необхідність [1 – 3]:

- врахування і використання в АНЕЗ ЦА технологій мереж загального користування (МЗК), зокрема, ISDN (PDH та SDH), Frame Relay (FR) ATM, IP/TCP;
- шлюзування потоків повідомлень між АНЕЗ ЦА і МЗК;
- використання для транспорту даних сучасних технологій пакетної комутації.

Особливість використання систем транспорту даних (СТД) у ЦА полягає в тому, що внаслідок зрозумілих обставин (перш за все, необхідності додержування суворих заходів безпеки) роль стандартизації, регламентації та уніфікації, у т.ч. обладнання ПД та правил його використання, має визначне значення. Тому завдяки добре налагодженому міжнародному співробітництву по лінії ІСАО та ITU є можливим і доцільним для задоволення потреб зв'язку у сфері авіаційного транспорту будувати однорідні мережі передачі даних. Це дає змогу орієнтуватися на використання FR –обладнання. Особливо велике практичне значення для побудови авіаційних корпоративних СТД має те, що на найбільш поширених українських мережах ПД національного рівня(це мережі Укртелеком та Інфоком) в якості основного технологічного обладнання (в першу чергу, у мережах абонентського доступу) використовується обладнання FR. Отже, існує можливість оренди такого обладнання для утворення корпоративних та (або) віртуально корпоративних мереж ПД в галузі ЦА.[3]

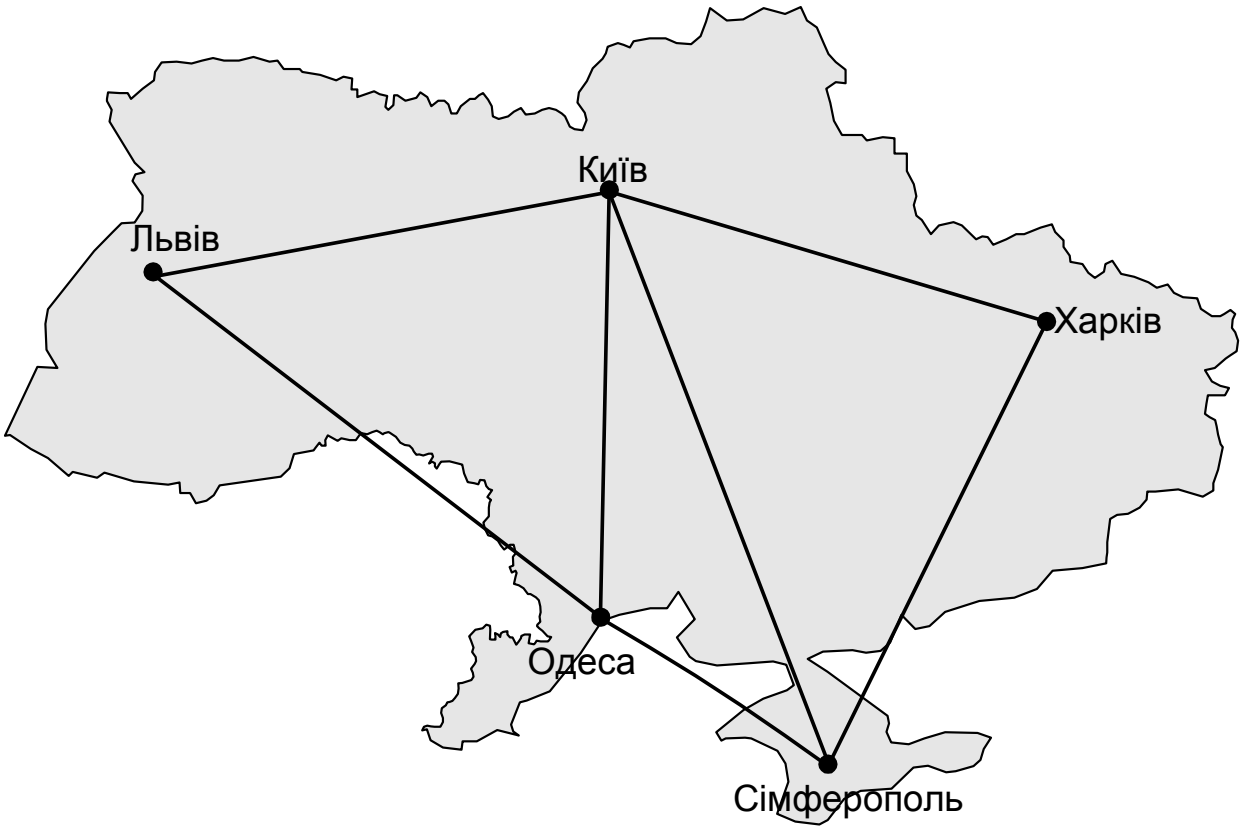


Рисунок 8.5. Топологічна структура транспортної мережі РЦ для АНЕЗ

Топологічна структура транспортної мережі НВДП РЦ для АНЕЗ показана на рис. 8.5. Вона являє собою полігональну мережу з головним комутаційним центром в м. Київ.

Варіант узагальненої архітектури транспортної мережі передачі даних (МПД) між підприємствами ЦА, відображено на рисунку 8.6. Вона являє собою двохшарову структуру. Внутрішній шар структурно представляє магістральну транспортну мережу, доступ до якої побудовано на базі технологій АТМ та IP, а зовнішній шар – мережі абонентського доступу FR та IP. Мережі абонентського обладнання FR використовуються в двох основних напрямках застосування:

- для забезпечення транспорту IP – пакетів від абонентських вузлів авіапідприємств до вузлів IP – мереж (як спеціалізованих, так і загального користування);
- для організації підключень до магістральної транспортної мережі (тобто, до ядра МПД) з використанням HDLC – подібних протоколів.

Ядро транспортної мережі (внутрішній шар в архітектурі МПД – див. Рисунок 8.5.) являє собою магістральну АТМ/ IP –мережу. Вузли її з'єднуються між собою високошвидкісними магістральними каналами ПД за схемою "із резервуванням напрямків". Міжвузлові з'єднання в магістральній мережі здійснюються за технологією АТМ. Пропускна спроможність кожного магістрального каналу передачі даних (ПД) в цій мережі – 155 Мбіт/с. Через неї циркулюють мультиплексовані потоки даних від магістральних АТМ –комутаторів та IP –маршрутизаторів, а також комутаторів/ маршрутизаторів мереж доступу.

Зовнішній (по відношенню до ядра) шар в структурі МПД розтинається на два прошарки. Перший прошарок – це FR –мережа абонентського доступу. Вузли цієї мережі приєднуються до АТМ-комутаторів магістральної мережі через високошвидкісні канали ПД. В цих вузлах розташовані крайові FR-комутатори, до портів котрих під'єднуються авіапідприємства через канали абонентського доступу. Пропускна спроможність кожного такого абонентського каналу доступу у FR -мережу – до 2,048 Мбіт/с. Через них циркулюють мультиплексовані потоки даних від пристроїв доступу до FR-вузлів, які називають пристроями FRAD (Frame Relay Access Device). Для передачі даних в мережі абонентського доступу використовується технологія постійних віртуальних каналів (PVC).

Другий прошарок зовнішнього шару в структурі МПД – це IP-мережа абонентського доступу, що призначена, головним чином, для надання послуг Інтернет та Інтранет. Вузли цієї мережі приєднуються до IP-маршрутизаторів магістральної ATM/IP-мережі із використанням цифрових потоків типу E1 (із швидкістю 2,048 Мбіт/с), що утворюються за допомогою обладнання первинної мережі. Ця мережа може бути власністю держави і надана у розпорядження Міністерству транспорта, або бути власністю АТ „Укртелеком" та (або) „Інфоком".

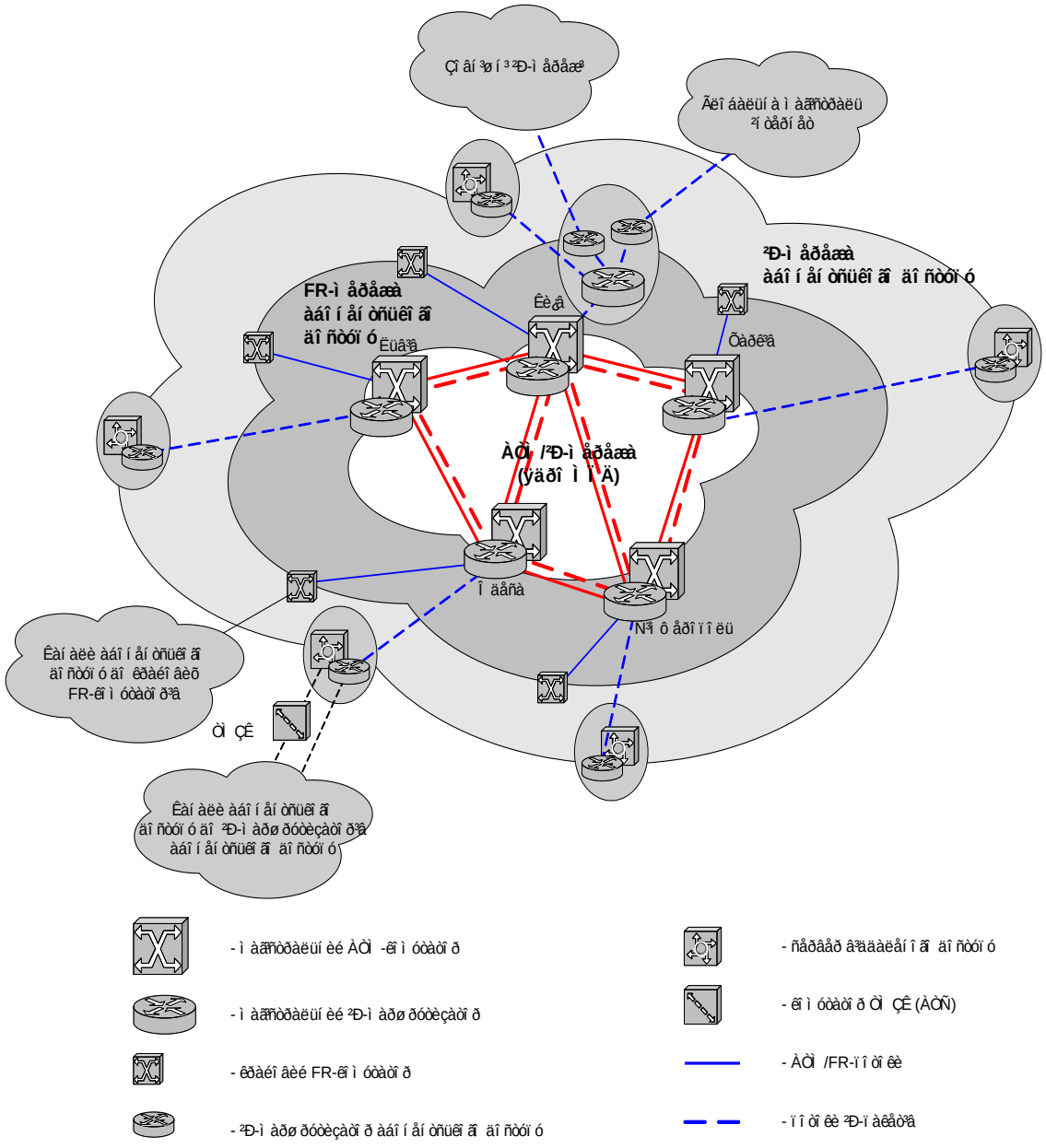


Рис. 8.6. Варіант архітектури транспортної мережі для АНЕЗ

Користувачі IP-мережі підключаються до вузлів доступу IP (до IP-маршрутизаторів абонентського доступу) за допомогою синхронних та (або) асинхронних некомутованих ліній, TDM-каналів, FR-каналів, а також комутованих каналів телефонних мереж загального користування (ТМЗК). Через IP-мережу авіапідприємства можуть мати доступ до глобальної мережі Інтернет.

Транспортна МПД повинна мати у своєму складі вузли взаємодії з іншими мережами. За допомогою обладнання пакетної маршрутизації вона повинна сполучатися з МПД інших українських операторів, а також підключатися до закордонних вузлів, зокрема з метою організації інформаційного взаємообміну з авіапідприємствами інших держав.

Для вирішення задач керування транспортною МПД та контролю її працездатності необхідно створити відповідну мережу управління. Бажано реалізувати управління типу

„out-of-band” [13,14]. Такий тип управління передбачає створення потоків сигналів управління та іншої технологічної інформації через фізично відокремлені канали зв’язку. Це сприятиме підвищенню живучості та надійності функціонування мереж, що дуже важливо в діяльності підприємств ЦА. Транспортна МПД має надавати ширший спектр мережних послуг практично на всіх семи рівнях EMBBC [8,10]. На фізичному і канальному рівнях цієї моделі мають надаватися послуги абонентського доступу до вузлів МПД. На канальному рівні-послуги транспорту фреймів (фрейм -це формат блоку даних у протоколах канального рівня) через FR та ATM -канали, а також організація підключень до МПД з використанням протоколу PPP та інших HDLC - подібних протоколів; на мережному послуги транспортування IP - пакетів на сеансовому рівні і вище - базовий набір інтернет – послуг, створення віртуальних приватних мереж, відеоконференцзв’язок тощо. Слід підкреслити, що на базі МПД з використанням каналів FR та ATM створена і діє національна транспортна мережа Укртелекому, послуги якої на засадах оренди доступні для авіапідприємств. Транспортна мережа Укртелекому забезпечує можливість корпоративним клієнтам об'єднувати свої локальні обчислювальні мережі (ЛОМ), що можуть бути розосереджені по всій території України і навіть за кордоном, в глобальні корпоративні мережі, здійснювати віддалений доступ до вузлів таких корпоративних мереж і т. ін. Номенклатура надаваних послуг та глибина охоплення цими послугами території України постійно розширюються. Це падає можливість Уктелекому. надавати послуги за доступними цінами майже в будь-якому населеному пункті України, що, враховуючи специфіку розташування українських авіапідприємств, може бути в деяких випадках безальтернативною можливістю отримання доступу до корпоративних даних.

Транспортну МПД що обслуговуватиме авіапідприємства, доцільно побудувати на базі обладнання IP - маршрутизації та ATM/FR-комутації а також серверів різного функціонального призначення.

Функціональна і організаційна структура МПД має бути ієрархічною та багаторівневою. Топологія – близька до радіально–вузлової. Для з’єднання вузлів МПД між собою доцільно використовувати цифрові канали первинної мережі із пропускною спроможністю від 2.048 до 155 Мбіт/с [1.13].

Звісно, що для забезпечення доступу користувачів до магістральної МПД існують відповідні мережі абонентського доступу. При цьому слід розрізняти мережі абонентського доступу, які забезпечують доступ до вузлів транспортної мережі канального рівня (тобто, до FR/ATM- комутаторів) з метою отримання послуг транспортних каналів, та мережі абонентського доступу до IP-вузлів зокрема з метою отримання інтернет послуг, а також для хостингу або побудови віртуальних приватних мереж. У якості абонентських каналів в обох типах вищеназваних мереж абонентською доступу використовуються будь-які доступні для

користувачів канали зв'язку - аналогові або цифрові, комутовані або виділені канали тональної частоти (ТЧ), фізичні лінії (двох проводові або чотирьох проводові), оптичні канали, канали радіодоступу тощо. Вибір каналів доступу здійснюється з урахуванням наявних можливостей щодо підключення та місць розташування абонентського обладнання та вузлів МПД [9.12].

Один із можливих варіантів фізичної топології МПД наданий на рисунку 8.7. [4-7] За цим варіантом з врахуванням існуючої МЗК регіонально-транзитні вузли (РТВ) у Харкові, Дніпропетровську, Донецьку. Одесі та Львові з'єднані з центральним вузлом (ЦВ) в м. Києві за допомогою цифрових каналів первиної мережі з пропускною здатністю 155 Мбіт/с. Для передачі даних між регіонально-транзитними вузлами та центральними вузлом у сучасних умовах найбільш придатною є технологія АТМ [10]

Регіональні вузли (РВ) в обласних центрах України доцільно з'єднати з регіонально-транзитними вузлами за допомогою цифрових каналів первинної мережі з пропускною здатністю n x 2,048 Мбіт/с. Кожний регіональний вузол, окрім підключення до свого РТВ, бажано підключити ще, як мінімум, до одного вузла свого або вищого ієрархічного рівня. Для передачі даних між регіональними та регіонально-транзитними вузлами слід використовувати технології АТМ, FR та IP [9,14].

Варіант схеми розміщення обладнання ATM/FR- комутації на міжобласний ділянці транспортної МПД який пропонується, представлено на рисунку 8.8.

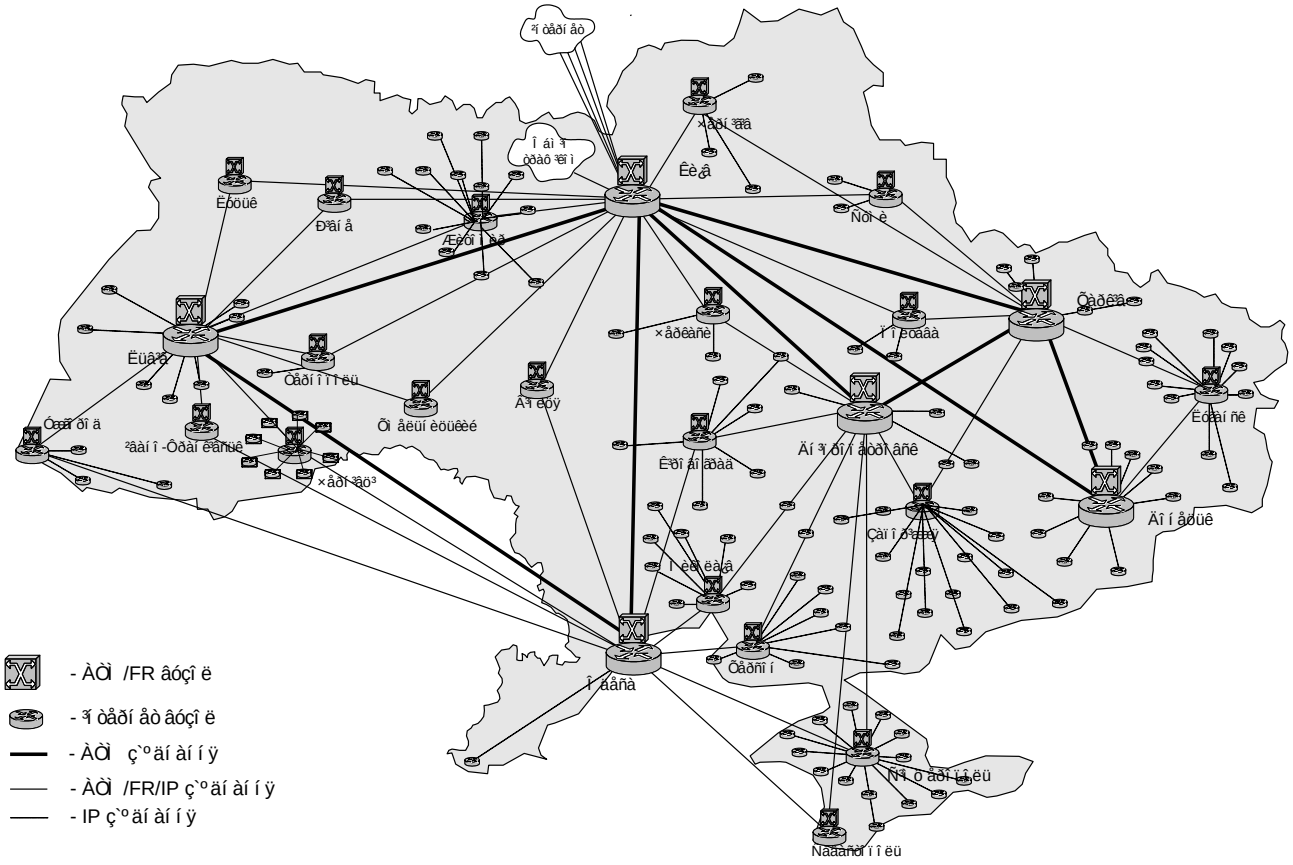


Рисунок 8.7. Варіант топології транспортної МПД для забезпечення зв’язку авіапідприємств в Україні

Крім обладнання ATM/FR –комутації в усіх вузлах МПД має бути встановлене також обладнання IP –маршрутизації, схема розміщена котрого, яка пропонується, представлена на рисунку 8.9.

До складу центрального вузла в м. Києві доцільно включити [13.14]:

1) магістральні маршрутизатори, маршрутизатори абонентського доступу, міжмережні шлюзи (національні й міжнародні);
2) магістральні ATM –комутатори та комутатори/мультиплексори абонентського ATM/FR –доступу.

До складу регіонально-транзитних вузлів МПД у містах Харків, Дніпропетровськ, Донецьк, Одеса та Львів бажано включити:

1) магістральні маршрутизатори , маршрутизатор абонентського доступу, а також можуть входити міжмережні шлюзи;
2) магістральний ATM –комутатор та комутатори/мультиплексори абонентського FR-доступу.

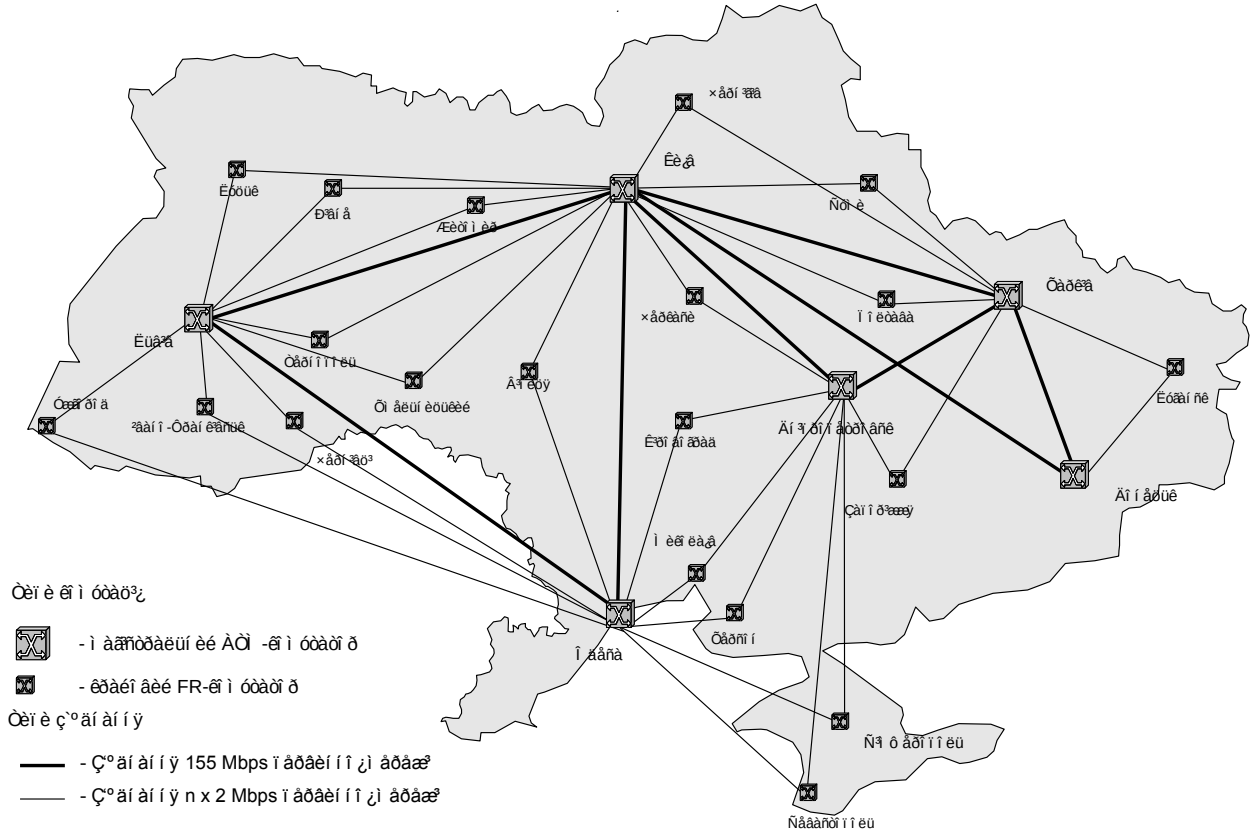


Рис. 8.8. Схема розміщення обладнання ATM/FR – комутації на міжобласній ділянці транспортної мережі передачі даних

Магістральні ATM – комутатори з’єднуються між собою через цифрові канали первинної мережі із швидкістю 155 Мбіт/с.

До складу регіональних вузлів МПД, які розміщуються в обласних центрах України, входять:

3) маршрутизатори абонентського доступу;
4) комутатори/мультиплексори абонентського FR доступу.

Кожен з регіональних маршрутизаторів має з'єднуватися з регіонально-транзитними магістралями маршрутизаторами через цифрові канали первинної мережі із швидкістю 2,048 Мбіт/с.

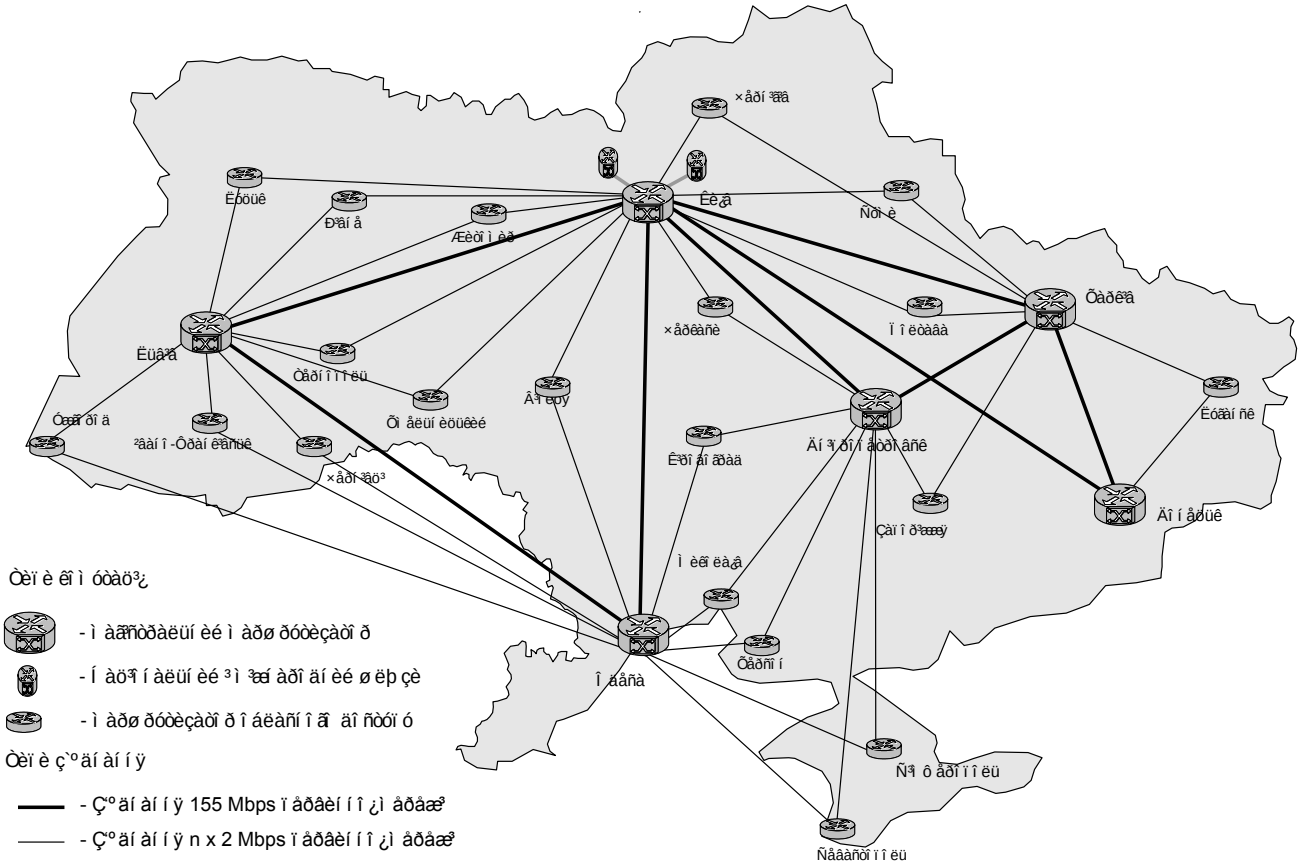


Рисунок 8.9. Схема розміщення обладнання IP – маршрутизації на міжобласній ділянці транспортної IP – мережі передачі даних.

В межах МПД, що обслуговуватиме авіапідприємства, доцільно створити і розвивати такі два види мереж абонентського доступу: IP –доступу FR –доступу.

8.2.2. Архітектура мереж абонентського IP –доступу

Мережі абонентського доступу підключаються до транспортної IP –мережі через вузли доступу (ВД). До складу основного обладнання типового ВД рівнів центрального (ЦВ) та регіональних (РВ) вузлів входять маршрутизотор абонентського доступу, сервери віддаленого доступу, сервери DNS RESOLVER та RADIUS PROXY. Обладнання ВД з'єднане між собою через локальну обчислювальну мережу (ЛОМ), поділену між мережним екраном на окремі зони захисту. Поділ об'єктів ЛОМ за зонами захисту здійснюється відповідно до прийнятої політики забезпечення захисту інформаційних ресурсів ВД [14].

Функції між мережного екрану може здійснювати маршрутизотор абонентського доступу або окремий програмно-апаратний засіб.

Типова конфігурація апаратних засобів ВД на мережних центральному та районних вузлах зображена на рисунку 8.10. [13].

На ЦВ та РТВ поряд з ВД до транспортної IP –мережі доцільно розмістити вузли доступу до прикладних служб Інтернету, типова конфігурація яких також показана на рисунку 8.10.

Типова конфігурація апаратних засобів ВД до IP –мережі на ЦВ практично не відрізняється від конфігурації ВД на РТВ, але існує суттєва різниця з точки зору функціональності та продуктивності встановленого обладнання на цих ВД.

Типова конфігурація ВД до IP –мережі, що розміщуються на РВ, не передбачає використання магістральних IP-маршрутизаторів та міжмережних шлюзів. IP-маршрутизатор абонентського доступу ВД на РВ має IP-канали, що побудовані на основі цифрових потоків E1, до визначеного (як правило, найближчого) ВД рівня РТВ або ЦВ. Крім того, на РВ з економічних міркувань не передбачається створення ВД до прикладних служб Інтернету. Користувачі, що підключені до ВД на РВ отримують послуги прикладних служб Інтернет в режимі віддаленого доступу до ресурсів РТВ або ЦВ.

Маючи на увазі відносно велику чисельність периферійних вузлів (ЦВ) авіапідприємств та їх значну розосередженість на території України, з метою мінімізації витрат на створення і утримання ВД до IP-мережі на ПВ обладнання цих вузлів слід намагатися зробити у мінімальній конфігурації. Зокрема, типова конфігурація ВД до IP-мережі на ПВ має складатися лише із обладнання, що дозволяє обмінюватися IP-трафіком між користувачами цього вузла і обладнанням самого вузла через наявні канали зв’язку (це – перш за все, пули модемів різних типів, аналогові, цифрові, через виділені канали тощо), а також із обладнання, що дозволяє мультиплексувати/демультиплексувати та (або) концентрувати отриманий трафік і далі транспортувати цей трафік через цифрові потоки типу E1 в каналі, що утворюється між ВД на ПВ і ВД наперед визначеного (як правило, найближчого) територіального вузла (ТВ) МПД. ВД на ТВ мультиплексують IP-трафік від приєднаних до них ПВ і далі спрямовують його на ВД регіонального вузла.

Мережі абонентського доступу підключаються до ВД через комутовані та (або) виділені канали зв’язку. Користувачі змушені, здебільшого, орієнтуватися на аналогові канали. Але поступово зростає можливість застосування цифрових комутованих каналів. Аналогові комутовані канали – це, як правило канали ЗАКТМ зі смугою пропускання 3,1 кГц. Цифрові комутовані канали, якщо вони використовуються, то це – канали BRI цифрової мережі з інтеграцією послуг (ЦМІО). Для організації каналів абонентського доступу через

канали ЗАКТМ/ЦМІП використовуються відповідно аналогові модеми/термінальні адаптери (ТА).

В якості шлюзів між мережами з комутацією каналів, через які здійснюють доступ користувачі послуг МПД, та транспортною IP-мережею використовуються сервери віддаленого доступу (СВД) (див. рисунок 8.10) СВД підключаються до ЗАКТМ через інтерфейси Е1. Обмін службовою інформацією з комутаторами ЗЛКТМ (тобто, з АТС) відбувається за допомогою систем сигналізації СКС7, R2D та інших. Для .підключення СВД до мережі ЦМІП використовуються інтерфейси PR1. Обмін службовою інформацією з комутаторами ЦМІП здійснюється за допомогою системи сигналізації DSS1.

Враховуючи специфіку діяльності авіапідприємств, перед отриманням доступу через комутовані канали до транспортної IP-мережі необхідно виконувати процедури ідентифікації ти автентифікації користувачів. Для нього використовується програмне забезпечення СВД та сервера RADIUS PROXY.

Обладнання та ПЗ, яке є необхідним для виконання безпосередніх функцій сервера RADIUS PROXY, входить до складу будь-якого ВД (крім ВД на ІІВ). Але спеціалізоване ПЗ та обладнання сервера RADIUS, яке виконує функції керування, входить до складу тільки вузла керування мережею, що розташований па ЦВ або на регіонально-транзитному вузлі, який виконує функції резервного вузла керування. До складу цих вузлів керування (тобто, основного і резервного) входить, крім того, спеціалізоване ПЗ та обладнання СВД з використанням замовних ліній типу ЗЗК, а також ПЗ, що здійснює функції управління ресурсами модемного пулу. ПЗ серверів СВД та RADIUS забезпечує облік обсягів наданих послуг комутованого доступу.

Крім комутованих аналогових і цифрових каналів для доступу до глобальної транспортної IP-мережі можуть використовуватися виділені канали. Виділені канали також можуть бути аналоговими та (або) цифровими

Крім того, для доступу до магістральної IP-мережі є можливим використання постійних віртуальних каналів транспортної мережі ATM/FR Укртелекому. Мережі абонентського доступу підключаються до мережі FR за допомогою спеціального обладнання доступу пристрою FRAD. Один із портів маршрутизатара ВД також підключений до мережі FR. При замовленні абонентом послуги доступу до магістральної IP-мережі між абонентським пристроєм FRAD та пристроєм FRAD, що підключений до порту IP-маршрутизатора, встановлюється постійний віртуальний FR-канал, через який абонентська мережа отримує доступ до транспортної IP-мережі.

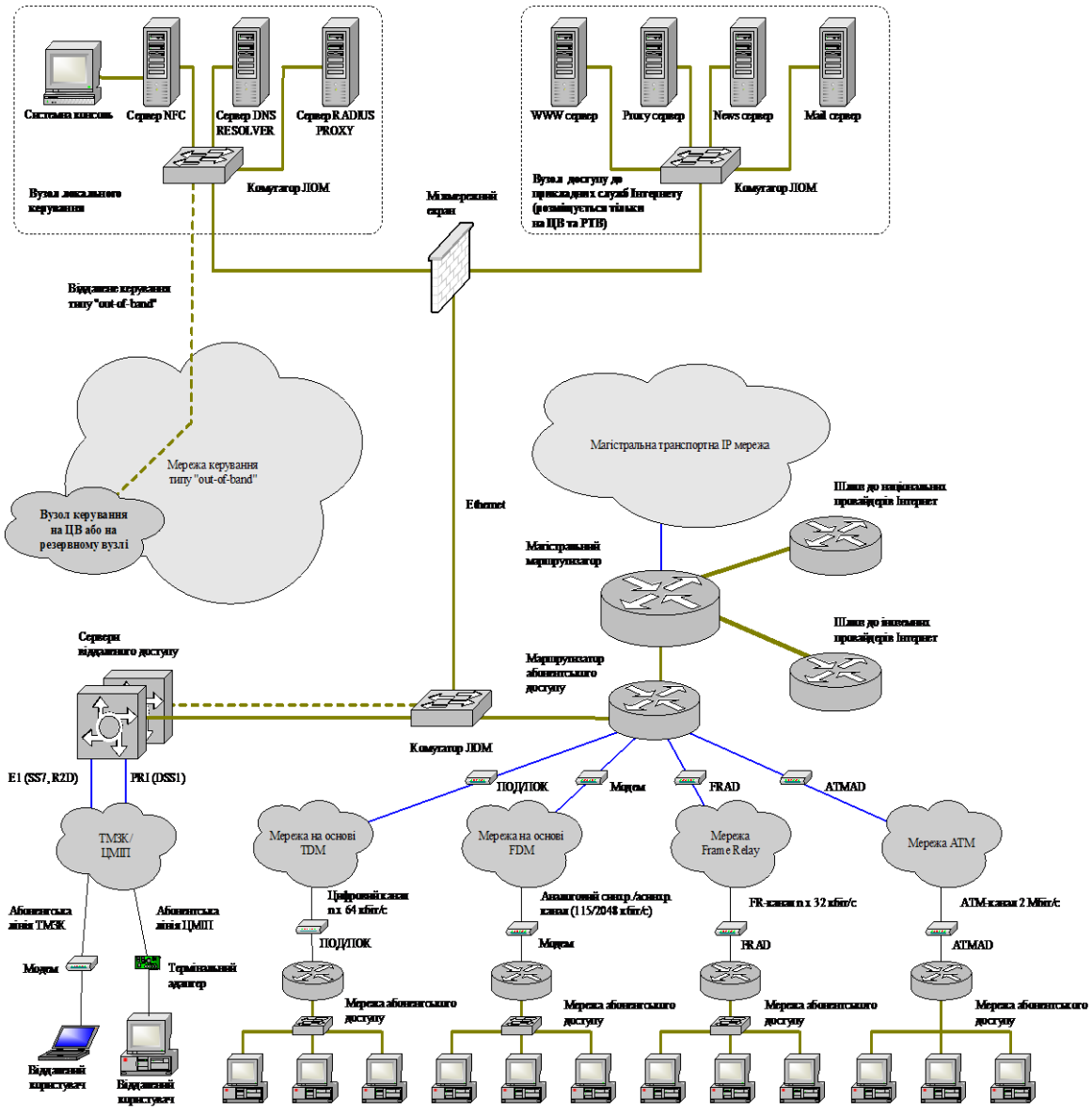
Облік обсягів наданих послуг за видами каналів доступу (тобто, облік трафіку} забезпечує ПЗ СВД або маршрутіпатора абонентського доступу, а також ПЗ сервера Net Flow

Collector (NFC) Обладнання та ПЗ сервера NFC має входити до складу вузла управління будь-якого ВД рівня ЦВ, РТВ та РВ.

Крім транспортних послуг МПД можуть надавати послуги прикладного рівня мережі Інтернет, такі як:

- послуги сервера доменних імен (DNS);
- послуги електронної пошти (Mail);
- послуги телеконференцій (News);
- послуги розміщення FTP серверів;
- послуги розміщення віртуальних WWW серверів (послуги хостингу).

Обладнання, необхідне для надання цих послуг, крім послуг DNS, входить до складу вузлів надання Інтернет-послуг та вузлів хостингу. Ці вузли мають знаходитися на ЦВ та РТВ і утворювати мережу надання послуг прикладних служб Інтернет (див, рисунок 8.10).



Примітка: ATMAD – пристрій доступу до мережі ATM; інші пояснення щодо прийнятих позначень та скорочень наведені в тексті документу

Рис. 8.10. – Типова конфігурація апаратних засобів вузла доступу до IP-мережі корпоративної МПД.

8.2.3. Мережі абонентського FR –доступу

Послуги мереж абонентського FR –доступу використовуються, здебільшого, для об'єднання корпоративних локальних мереж між собою. Ці мережі абонентського доступу підключаються до магістральної транспортної мережі через крайові FR –маршрутизатори /мультиплексори.

Якщо для підключення до магістральної транспортної мережі використовується технологія FR, то до складу обладнання мереж абонентського доступу повинен входити FRAD. Найчастіше пристрій FRAD є невід'ємною частиною IP-маршрутизаторів, але він також може бути конструктивно оформлений у вигляді окремого пристрою. В цьому випадку для його підключення до маршрутизатора, використовуються інтерфейси 10BaseT/100BaseTX, V.24, V.35, V.36, V.11. Для зв'язку FRAD з крайовими ATM/FR комутаторами/мультиплексорами використовуються цифрові та (або) аналогові виділені канали тощо. Каналоутворююче обладнання (ПОД/ПОК, синхронні/асинхронні аналогові модеми) може входити до складу FRAD (маршрутизатора) або бути конструктивно оформленим у вигляді окремих пристроїв.

В багатьох випадках крайові FR –комутатори можуть під`єднуватися до магістральних ATM –комутаторів за технологією FR, тобто через інтерфейс NNI FR із швидкістю 2,048 Мбіт/с. Пропонуєма схема абонентського доступу до магістральної транспортної мережі з використанням технології FR зображена на рисунку 8.11.

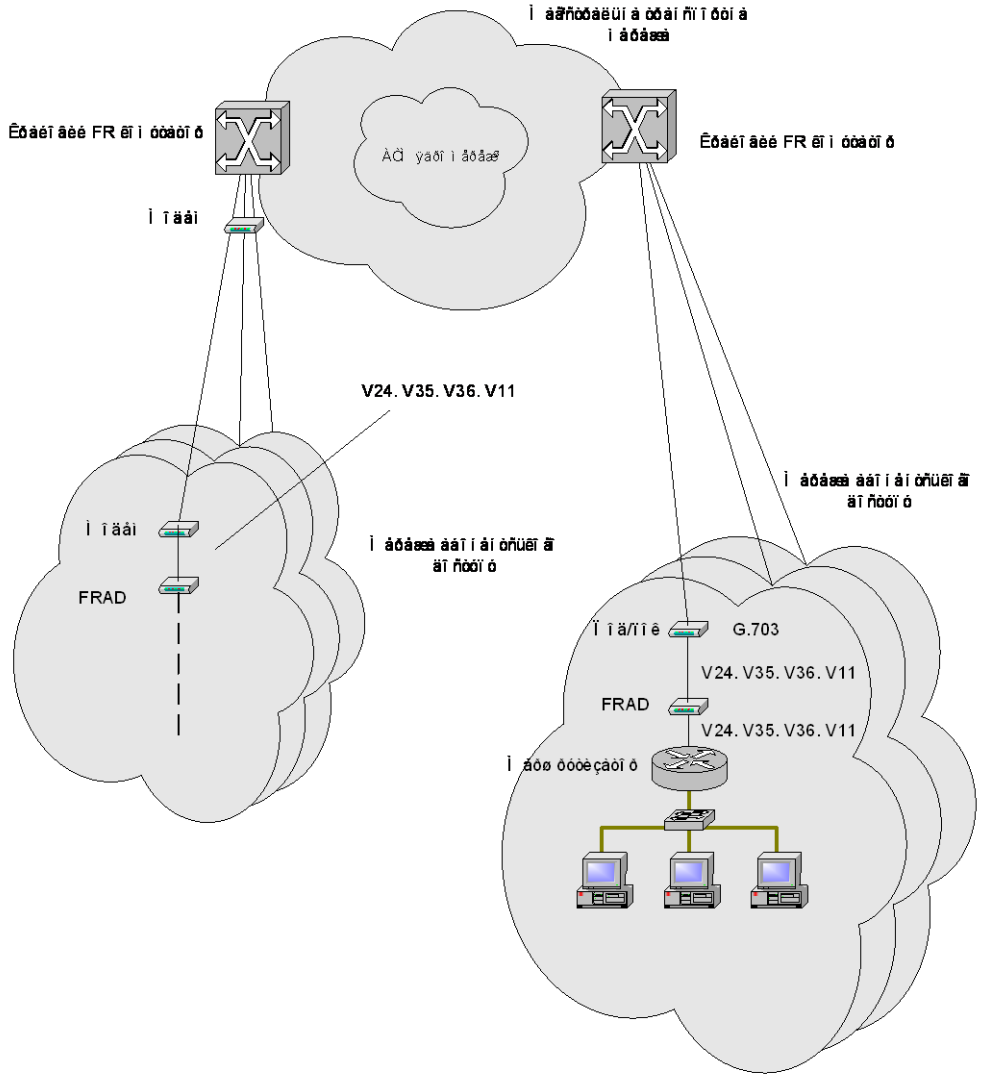


Рисунок 8.11 Пропонуєма схема абонентського доступу до магістральної транспортної мережі з використанням технології FR

Між абонентськими пристроями FRAD через комутатори транспортної мережі встановлюються постійні канали, оскільки послуги комутованих віртуальних каналів транспортними мережами практично ніде поки що не надаються. При встановлені постійного віртуального каналу задається його узгоджена швидкість (CIR) та додаткова максимальна швидкість (EIR).

Сумісне використання мережі FR і мережі МЗК характерне для служб ОПР цивільної авіації багатьох країн. На рис. 8.12 приведено схему організації фрагменту інтегрованої мережі ОПР “Aircontrol”. Мережа забезпечує цифрову передачу даних, телеграфних і телефоних повідомлень. Вона зв’язує віддалені диспетчерські пункти (ДП) ОПР з центральним вузлом FIR через канали МЗК, супутниковий канал і мережу FR.. Маршрутизатори долучаються до мережі FR і МЗК за допомогою модемів. Технологічний захист відомчої інформації забезпечуються заходами, регламентованими ICAO, які аналізуються нижче в п.п. 8.3. З метою зміцнення захисту відомчої інформації доцільно

використати міжмережні екрани (МЕ). Дослідженням ефективності використання МЕ та особливостей їх розміщення присвячені розділи 2-4 даної роботи.

Результати порівнювального експертного аналізу можливостей реалізації різних видів телекомунікаційних послуг на основі сучасних протоколів наведено в таблицях 8.3 і 8.4 та на рис. 8.13. [15]. Наведені дані показують певну перевагу технології ATM і FR у більшості послуг. Ця перевага особливо суттєва при передачах мови, відео і оперативних даних. Такий же висновок слід сформувати і для технології TCP/IP, але при передачі мови технологія TCP/IP поступається технологіям ATM і FR.

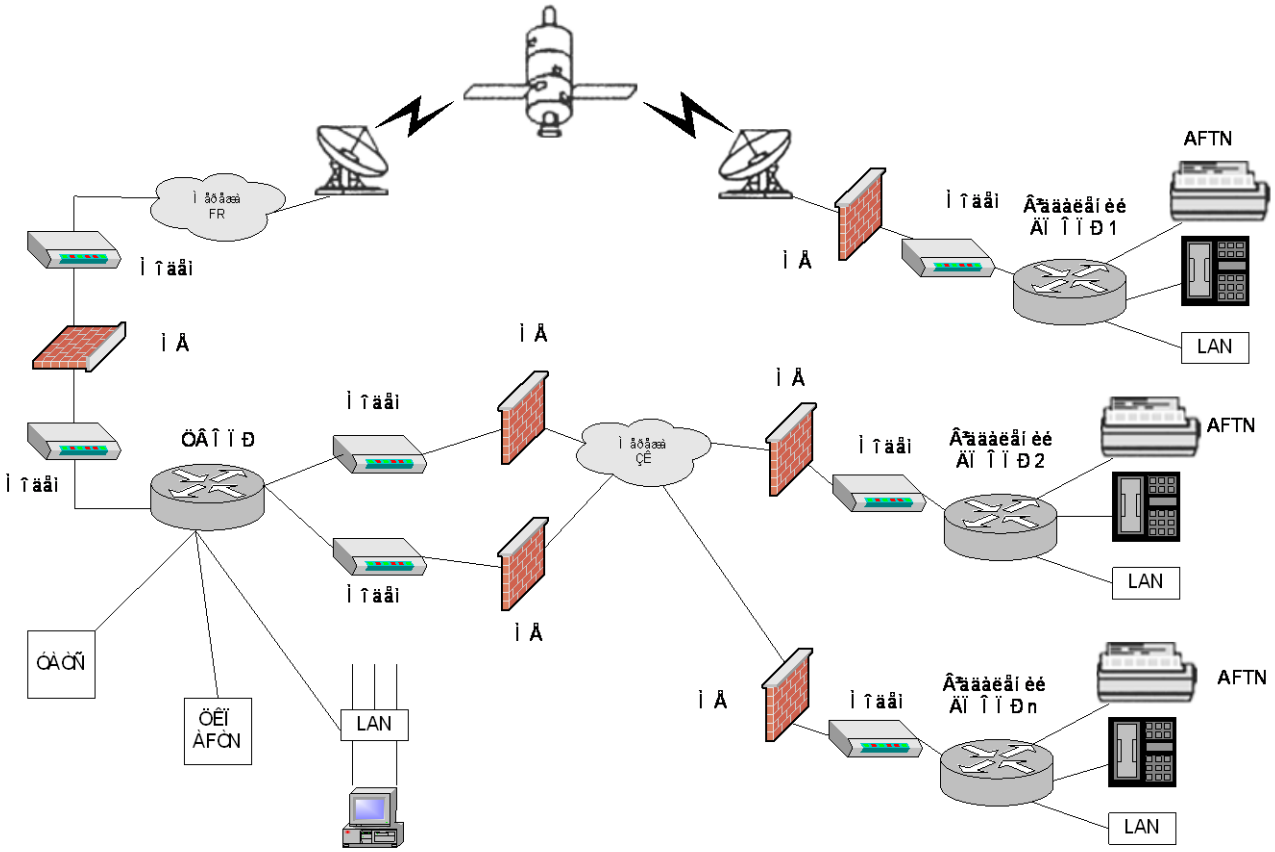


Рис 8.12. Схема організації фрагмента ЦМІО ОПР ЦА: МЕ - міжмережний екран; ДП – диспетчерський пункт.

Таблиця 8.3.

Можливості реалізації сучасних протоколів задля різних видів послуг

Тип протоколу	Тип передачі					
	Мова	Відео	Опер. дані	Файли даних	Відео файли	Аудіо файли
Ethernet	1	1	2	1	0	0
Token Ring	1	1	2	1	0	0
FDDI	3	3	3	1	1	1
HSSI	2	2	1	0	1	1
PPP	1	0	2	2	1	0
ISDN	4	2	2	1	2	1

X.25	2	1	3	2	1	0
Frame relay	4	3	3	1	2	1
ATM	5	4	4	1	2	1
Appletalk	1	0	1	1	1	0
DecNet	2	1	2	1	1	0
TCP/IP	2	1	3	2	1	0
IPX/SPX	2	1	2	1	1	0

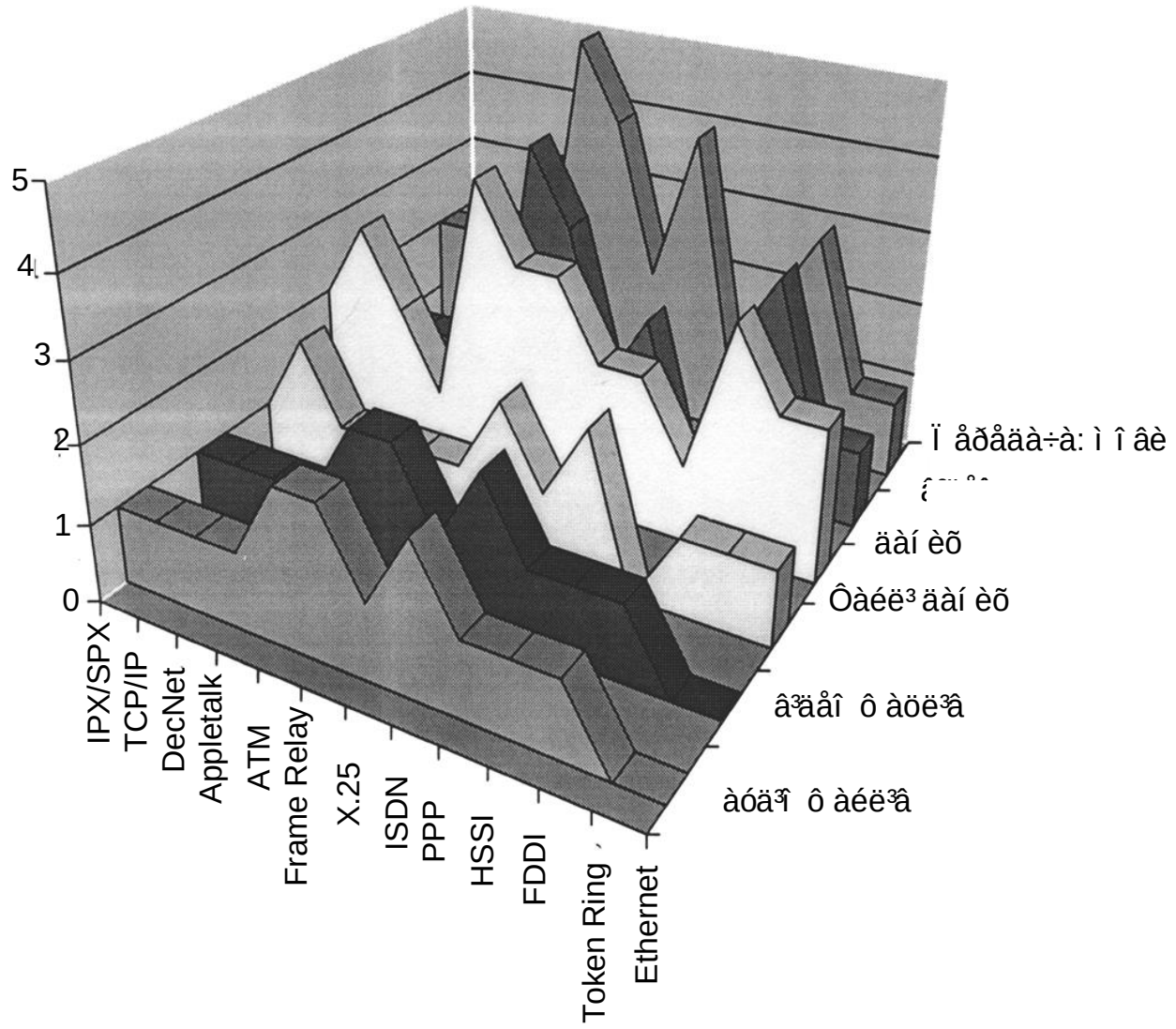


Рис. 8.13. Ефективність сучасних протоколів

Таблиця 8.4.

Відповідність протоколів сучасних технологій вимогам до послуг

Технічні показники обслуговування	Вимоги до протоколів	Ethernet	Token Ring	FDDI	HSSI	PPP	ISDN	X.25	Frame relay	ATM	Appletalk	DecNet	TCP/IP	IPX
Середній час доставки одиниці інформації	Можливість забезпечити доставку одиниці інформації за заданий час	+	+	+	+	-	+	-	+	+	-	-	-	-
Пропускна спроможність ТКС	Можливість забезпечити гарантовану пропускну спроможність з'єднання	-	-	+	+	-	+	-	+	+	-	-	-	-
Імовірність помилки при транспортуванні інформації	Можливість корекції помилок	+	+	+	-	+	-	+	-	-	-	-	+	-
Коефіцієнт готовності обслуговування	Можливість встановлення з'єднання по альтернативним маршрутам	-	-	+	-	-	-	+	-	+	-	+	+	+
Гарантований обсяг обслуговування	Можливість забезпечити задану пропускну спроможність з'єднання	-	-	+	-	-	-	+	-	+	-	+	+	+
Собівартість обслуговування	Визначається можливостями ЦМІО													
Рівень охоплення території обслуговування	Визначається можливостями ЦМІО													
Рівень захищеності передачі інформації (к-сть комбінацій ключа)	Вбудоване кодування інформації, що передається	-	-	-	-	+	+	+	-	+	+	+	+	+
Сумісність з різними видами обладнання і обслуговування	Визначається можливостями ЦМІО													

Впровадження ATN з використанням сучасних телекомунікаційних технологій обумовлює необхідність дотримання певних вимог щодо якості інформаційного обслуговування користувачів. В цифрових мережах МЗК і МПД та відомчих мережах ЦА якість обслуговування користувачів визначається узагальненими критеріями. Вони охоплюють по декілька параметрів системи зв'язку. Відповідно до рекомендацій ITU та ICAO для систем АЕЗ такими критеріями є [1,8]:

- - QoS (Quality of Service) — якість обслуговування;
- RCP (Required Communication Performance) — необхідні характеристики зв’язку

Розглянемо специфіку цих критеріїв стосовно ATN.

8.2.4. Вимоги до якості надання послуг в ATN

8.2.4.1. Критерії QoS

Поняття якості, відповідно до ITU-T, E.430 і E.800 формулюється як “сукупність показників, що характеризують задовільненість користувача телекомунікаційними послугами, які надаються”. Складовими частинами оцінки якості послуги є три основні стадії надання послуги: доступ до передачі даних, передача даних, завершення сеансу передачі (порушення з’єднання). Кожна з цих стадій характеризується трьома основними показниками: швидкість, достовірність, гарантованість. Наведене визначення показників якості в рекомендації E.430 є базовим для інших рекомендацій ITU-T щодо якості послуг для різних типів мереж.

В рекомендації X.140 для МПД (PDN – Public Data Network) загального користування параметри незалежні ні від додатку, ні від структури мережі, ні від послуги. Так, основним параметрами якості обслуговування мереж передачі даних PDN (зокрема мережі X.25) є наступні:

- затримка доступу; імовірність організації неправильного доступу; імовірність відмови у встановленні доступу;
- затримка передачі інформації користувача; швидкість передачі інформації користувача; імовірність помилок передачі інформації; імовірність передачі зайвої інформації; імовірність помилкової доставки інформації користувача; імовірність загублення інформації користувача;
- затримка у розрушенні з’єднання; імовірність відмови у роз’єднанні доступу;
- доступність послуги, імовірність відмови у передачі інформації користувача; час недоступності послуги.

Перелічені вище параметри організовані у відповідності з концепцією QoS, яка подана в рекомендації ITU-T E.430. Остання група параметрів є похідною від основних і тому вони у об’єднану табл.. 8.5. не ввійшли.

Таблиця 8.5.

Показники QoS

Фаза надання послуги	Показники якості		
	Швидкість	Точність	Гарантованність
Організація доступу	Затримка установлення доступу	Імовірність організації невірного доступу	Імовірність відмови в установлені доступу
Передача даних	Затримки передачі даних користувача Швидкість передачі даних користувача Пропускна спроможність	Імовірність помилки у інформації користувача Імовірність передачі зайвої інформації Імовірність помилкової доставки інформації	Імовірність втрати інформації користувача
Роз'єднання доступу	Затримка звільнення мережного з'єднання	Імовірність неуспішного звільнення мережного з'єднання	Імовірність неуспішного звільнення мережного з'єднання

Основними параметрами QoS, які важливі в ATN для кінцевих користувачів, є затримка передавання повідомлення T_3, пропускна спроможність системи зв'язку r0 і коефіцієнт помилок Кп. Ці параметри в ATN використовують для прогнозування рівня QoS у підмережах, через які проходить маршрут між кінцевими користувачами. Від рівня QoS безпосередньо залежать також арендні витрати Da на надання послуг користувачам протягом певного часу Та (надання каналу зв'язку на термін Та).

Затримка Т3 визначається, як час, що минає між моментом подання одиниці інформації на рівень MAC і моментом успішного її отримання відповідним обладнанням приймача. Наприклад, в СПД ACARS математичне очікування плюс середнє квадратичне відхилення затримки проходження складає близько п'яти секунд. В системі AMSS норми на T_3 залежать від пріоритету повідомлення Q швидкості передачі та напрямку - до ПС, чи від ПС (таблиця 8.6.).

Пропускна спроможність R_0 (біт/с) визначається типом лінії передачі (каналу передачі), які використовуються в системі зв'язку. Звичайно в реальних умовах при бінарному кодуванні швидкість передачі інформації Ri < R0. Ступінь цієї нерівності оцінюють продуктивністю системи. Продуктивність визначається як процент пропускної здатності каналу зв'язку, яка споживається для успішного передавання інформації на фізичному рівні: $\rho = R_i / R_0$. Величина ρ звичайно нормується з урахуванням припустимого значення Т3. Так, в системі ACARS (США) $\rho \le 0{,}45$. Для системи VDL/ CSMA $\rho \le 0{,}6$ в одноканальних лініях передачі AFTN відносна завантаженість $\rho \le 0{,}4$.

Коефіцієнт помилок Кп при передаванні дискретних повідомлень нормується в залежності від типу каналу зв'язку, типу інформаційної технології та методу підвищення завадостійкості системи зв'язку. Для прикінцевих користувачів мережі ATN в каналах з технологією ISDN і циклічним кодуванням рівень бітових помилок BER (Bite Error) оцінюється значенням 10^{-11}. При технології ATM в якості Кп використовують відносну кількість загублених чарунок $\gamma r = \leq 10^{-7}$. Розглянутий перелік основних параметрів QoS може бути розширеним в залежності від призначення системи зв'язку та характеру задач, які вирішуються. Наприклад, параметри QoS можуть бути використані для оцінки ефективності засобів захисту інформації.

8.2.4.2. Критерій RCP

Критерій RCP (Required Communication Performance) призначений для використання фахівцями ОПР, яким під час виконання функцій ОПР потрібний АЕЗ. Концепція RCP спрямована на використання малої кількості параметрів Для кожної функції ОПР мають бути так визначені та конкретизовані параметри характеристик АЕЗ, щоб забезпечити оцінку і контроль різних технологій зв'язку на різних етапах польоту та при різних експлуатаційних умовах Різним функціям ОПР можуть відповідати різні типи RCP. Одна і та ж функція ОПР може мати різні типи RCP для різних умов експлуатації.

RCP - це комплекс вимог до характеристик АЕЗ з метою забезпечення конкретних функцій ОПР. До визначальних параметрів RCP належать [1,8]: тривалість процесу зв'язку, цілісність, готовність і безперервність функціонування. Тип RCP позначається однією великою латинською літерою (табл. 8.7.)

Перед нею цифрою вказується параметр тривалості процесу зв'язку [1]. Наприклад, 100E означає, що тривалість зв'язку становить 100 секунд, а набір параметрів RCP відповідає типу E.

Таблиця 8.6

Затримка повідомлення в AMSS

Швидкість передачі , Кбіт/с	Максимальна затримка встановлення з'єднання, с	Транзитна затримка, с			Затримка передачі даних, с		
		до ПС		від ПС	до ПС		від ПС
		Q=15	Q=3	Q=15	Q=15	Q=3	Q=15
0,6	70	12	40	40	15	110	80
1,2	45	8	25	30	9	60	65
2,4	25	5	12	15	6	30	35
4,8	25	4	7	13	5	20	30
10,5	25	4	5	13	4	10	30

Таблиця 8.7

Типи RCP

Тип RCP	Цілісність	Готовність	Безперервність
A	10-9	0,99999	0,99999
B	10-7	0,99996	0,99996
C	10-6	0,9996	0,9996
D	10-5	0,999	0,999
E	10-5	0,99	0,99
F	10-3	0,99	0,99
G	10-3	вимоги відсутні	

Тривалість процесу зв'язку - це максимальний термін для завершення процесу зв’язку. Цілісність даних – це імовірність безпомилкової доставки даних протягом часу, не більшого за заданий.

Готовність являє долю часу, протягом якого надається обслуговування (T_0), від загального часу роботи Тр, тобто $k_r = T_0 / T_p$

Безперервність – це імовірність працездатності системи протягом часу виконання задачі.

Рекомендовані ІСАО значення параметрів RCP в залежності від типу RCP наведено в табл. 8.7. Узагальнені в середньому характеристики надійності засобів зв'язку подано в табл.1.8 [1,2,8]. Висока надійність автоматичних дубльованих засобів зв'язку дозволяє в моделях мереж брати до уваги тільки надійність каналів зв'язку та кінцевого обладнання.

Таблиця 8.8

Характеристики надійності засобів зв'язку

№ п/п	Типи засобу зв'язку	Коефіцієнт готовності, k?	Середній час відновлення Тв, г
1	Канал лінії зв'язку довжиною 1 000 км:		
2	магістральної кабельної	0,99	1,0
3	зонової кабельної	0,95	1,0
4	радіорелейної	0,95	1,0
5	Канал радіолінії МХ прямої бачимості	0,95	0,5
6	Канал радіолінії ДКМХ з передавачами середньої та великої потужності	0,9-0,95	0,5
7	Канал зв'язку через ШСЗ (до 80 тис.км)	0,95	0,5
8	Кінцеві ТЛФ апарати (абонентські)	0,9999	1,0
9	Кінцеві ТЛГ апарати (абонентські)	0,9995	1,0
10	Кінцеве обладнання даних (КОД)	0,9999	10,0
11	Вузлові прийомо-передавачі	0,9999-0,99999	0,1-0,5
12	Автоматичні вузли комутації каналів	0,9999-0,99999	0,1-0,5
13	Автоматичні центри комутації (ЦКП)	0,99999	0,1-0,2
14	Автоматичні концентратори	0,9999	0,1
15	Дубльовані ЦКП	0,9999997	0,5 - 0,2

Один із основних параметрів QoS та RCP – затримка $T_З$ проходження повідомлень через ATN. Цей параметр нормований ІСАО по класу ATSC (Air Traffic Series

Communication) і наведений у табл. 8.1. [1.2]. Зрозуміло, що затримка пов’язана з пропускною спроможністю системи зв’язку. Застосування певних засобів захисту інформації може зменшувати R_0 і збільшувати T_3. Таким чином, ефективність тих засобів ТЗІ, застосування яких веде до того, що якість обмінюється на швидкість, можна оцінювати по критерію збільшення T_3 або по критерію зменшення R_0. Ці питання досліджуються в розділах 2 і 3.

8. 3 Класифікація атак на ресурси інформаційно-комунікаційних систем

Проблема розробки й вибору ефективних методів і засобів захисту ІКС від атак у значній мірі залежить від ресурсів, на які спрямовані атаки, зовнішніх проявів, можливостей порушень характеристик безпеки й інших факторів. Ефективність її рішення в першу чергу пов'язана з визначенням того, на які класи атак розраховані ті або інші методи й засоби протидії.

У роботах [22-32] різними авторами розглядаються методи й засоби реалізації атак, а також наведено кілька варіантів їхніх класифікацій, які не охоплюють широкий спектр ознак і не характеризуються досить повним системним узагальнюючим підходом. Частина відомих класифікацій трохи звужена (наприклад, до таких об'єктів як глобальні комп'ютерні мережі) і вони не можуть бути використані як узагальнений інструмент для широкого спектра ресурсів ІКС , наприклад, таких, як локальні обчислювальні мережі, робочі станції, файл або носії даних, комп'ютери не підключені до тієї ж мережі й т.п.

На основі проведеного аналізу відомих класифікацій, методів і засобів реалізації атак пропонується узагальнена класифікація, що може бути використана для широкого спектра ресурсів ІКС .

Для того, щоб уникнути неоднозначності в тлумаченнях відзначимо, що атака - заходи, які приймаються для підриву безпеки КС (відмова в обслуговуванні, порушення характеристик безпеки й ін.).

З урахуванням того, що спектр атак досить різнорідний, то основним принципом по якому можна найбільше ефективно (відповідно до поставленій проблемі) здійснити класифікацію буде ознаковий. Пропонується класифікувати атаки на ресурси ІКС по наступних базових ознаках: автоматизації; взаємодії з політикою безпеки; дистанційності; дії, породженої несанкціонованим доступом (НСД); зовнішньому прояву; ініціалізаційній умові; інструментальним засобам; наявності зворотного зв'язку; порушенню характеристик безпеки; природі взаємодії; реляційним ознакам; специфіці реалізації; спрямованості результату; ступеня складності; типу базового ресурсу; семирівневій еталонної моделі.

По автоматизації атаки можна розділити на: мануальні; автоматизовані; автоматичні (вірусні).

Мануальні атаки (підглядання, збір сміття [21], вилучення інформаційних носіїв, підміна положень вмикачів режимів і т.п.) реалізуються безпосередньо за участю людини без використання будь-яких спеціальних засобів. Автоматизовані атаки здійснюються з постійною участю оператора з використанням широкого спектра програмних й апаратних ресурсів і пов'язані із супперзапингом, снупингом, снифингом [21], підключенням додаткових терміналів, використанням мережних аналізаторів й ін. Автоматичні атаки реалізуються без участі людини і як правило з використанням спеціалізованих програмних засобів, функціонування яких ґрунтується на вірусних технологіях.

По взаємодії з політикою безпеки атаки діляться на: постполітизаційні; деполітизаційні.

Постполітизаційні атаки засновані на використанні недоліків у вже реалізованій політиці безпеки [21]. Такими недоліками можуть бути неправильно побудовані правила розмежування доступу, використання програмних й апаратних засобів з недостатнім рівнем захищеності, прорахунки при блокуванні каналів витоку інформації з обмеженим доступом й ін. Деполітизаційні атаки пов'язані з помилками й недбалістю [22, 33], які мають місце при реалізації заходів із забезпеченням уже існуючої політики безпеки. Це в першу чергу пов'язане з людським фактором і залежить від недостатньої адміністративної підтримки, коректності виконання функцій захисту, своєчасності реагування на позаштатні ситуації й ін.

За дистанційністю атаки діляться на: локальні; вилучені.

Якщо атаки на ресурс здійснюються в локалізованій області його розташування (локальна обчислювальна мережа, робоча станція, принтер, носій інформації, операційна система, додатки й т.п.), то вони називаються локальними, а в противному випадку - вилученими. Наприклад, локальна атака може бути реалізована усередині сегмента (фізичного об'єднання станцій за допомогою комутаційних пристроїв не вище канального рівня) при цьому джерело атаки яка атакує ресурс, буде перебувати в границях одного сегмента, а межсегментная атака може бути прикладом вилученої атаки, якщо джерело й ресурс перебувають у різних сегментах комп'ютерної мережі, наприклад, кампусній. У першому випадку ініціатором атаки звичайно буває легальний користувач, що, наприклад, з файлу-сервера через робочу станцію здійснює копіювання конфіденційних даних на зовнішній носій інформації.

У процесі здійснення атак може бути реалізований НСД (як засіб досягнення мети) до різних ресурсів ІКС. У цьому випадку по дії, породженій НСД до зазначених ресурсів, атаки з обліком [20] діляться на: интераптаційні; интерсептаційні; модифікаційні; фальсифікаційні; вільні.

Интераптаційні атаки реалізуються шляхом переривання функціонування ресурсів, тобто вони гублять функціональність або стають недоступними, наприклад, за допомогою

різного роду блокувань, крадіжок і т.п. Интерсептаційні атаки здійснюються шляхом перехоплення різнорідної інформації щодо ресурсів. Перехоплення буває активним і пасивним. При активному перехопленні здійснюється незаконне підключення до каналів зв'язку, застосовуються мережні аналізатори, впроваджуються спеціальні програми й виконуються інші дії з метою, наприклад, копіювання або читання файлів, одержання імен користувачів і т.п. При пасивному перехопленні здійснюється візуальне, або, за допомогою засобів радіоперехоплення, зняття інформації з екрана відеотермінала, уловлювання випромінювань від принтера, дисководів й ін. Активне перехоплення (на відміну від пасивного) можна виявити, для чого, наприклад, здійснюється перегляд кабельних з'єднань, аналізуються невраховані процеси в операційній системі, контролюються запити на обслуговування й ін. Модифікаційні атаки в процесі доступу до ресурсів здійснюють їхнє перетворення, наприклад, шляхом реконфигурації апаратних засобів, впровадженням додаткових програм (закладок, вірусів і т.і.) або зміною існуючих з метою реалізації функцій атаки, наприклад, таких, які знищують бази даних, сповільнюють або імітують виконання програм, розширюють повноваження, записують таємну інформацію в схований простір диска й т.і. Фальсифікаційні атаки ґрунтуються на впровадженні в ресурси неврахованих компонентів, наприклад, процесів, які здійснюють підробку повідомлень, записів, файлів й ін. Вільні атаки не спрямовані на пряму реалізацію НСД до ресурсів ІКС (відповідно до вищеописаних підкласів) і не орієнтовані на порушення прийнятої політики безпеки. Такі атаки в основному спрямовані на збір інформації, наприклад, визначення карти обчислювальної мережі, адреси активних комп'ютерів і наявність сервисов, одержання даних шляхом аналізу періодичних видань, відомчих бюлетенів, документації й ін.

По зовнішньому прояву атаки діляться на: пасивні та активні.

У результаті своєї дії (наприклад, візуального перегляду даних з термінала) пасивні атаки не здійснюють безпосередній вплив на ресурси й можуть не порушити їхньої характеристики безпеки, наприклад, при перехопленні зашифрованих даних. У результаті активних атак на ресурси здійснюється безпосередній вплив (зміна конфігурації, порушення функціональності й ін.) і порушуються їхні характеристики безпеки. Практично всі типи вилучених атак є активними. Особливість активних атак (у порівнянні з пасивними) у тім, що є принципова можливість їхнього виявлення, тому, що в результаті безпосереднього впливу здійснюються певні зміни. На відміну від активних, пасивні атаки практично не залишають слідів втручання.

По ініціалізаційній умові атаки діляться на: умовні та безумовні.

Умовні атаки ініціалізуюьтся у випадку виникнення певної події (механізм логічної бомби [33]) і у свою чергу можуть ділитися на пасивні й активні. Прикладом ініціалізації пасивної умовної атаки може бути передача від потенційної мети запиту певного типу, що і

буде умовою початку атаки. У цьому випадку, наприклад, такою умовою можуть бути DNS- і ARP-запити в стеці TCP/IP. Активні умовні атаки здійснюють постійний моніторинг стану окремих ресурсів і при його певній зміні формується сигнал ініціалізації. Прикладом такого стану може бути подія, пов'язана з перериванням сеансу роботи користувача із сервером без стандартної команди, наприклад, LOGOFF. Момент ініціалізації безумовних атак не супроводжується певною зміною стану ресурсів і визначається джерелом атаки.

По використовуваних інструментальних засобах атаки діляться на: програмні; апаратні; нетипові.

Програмні атаки ґрунтуються на спеціальних мікро- або макрокодованих засобах (наприклад, суперзапінгових утилітах [21], внутрішніх командах, сценаріях автоматизації й т.п.), які функціонують у границях ІКС для реалізації своїх функцій. Апаратні атаки ґрунтуються на різноманітних механічних, електричних, електромеханічних, електронних, електронно-механічних й інших пристроях, які використаються автономно або разом з іншими апаратурами для виконання відповідних функцій. Нетипові атаки реалізуються на основі таких засобів, які не відносяться до апаратно або програмних, наприклад, вибухівка, радіоактивні матеріали, кислоти, луги, комахи, гризуни й т.п.

По наявності зворотного зв'язку з атакованим ресурсом, атаки бувають із: зворотним зв'язком; без зворотного зв'язку.

У процесі реалізації атаки зі зворотним зв'язком здійснюється одержання від атакованого ресурсу відповіді на певні дії, які необхідні, наприклад, для подальшого продовження зазначеного процесу на більш ефективному рівні, що досягається завдяки аналізу реакцій об'єкта атаки на певні зміни. Атака без зворотного зв'язку реалізує свої дії незалежно від реакції атакованого ресурсу. Найбільш яскравим прикладом таких атак є відмова в обслуговуванні.

При реалізації атак здійснюється порушення основних характеристик безпеки ресурсів ІКС (конфіденційності, цілісності й доступності). У цьому контексті по типу порушення характеристик безпеки атаки бувають: К-дії (порушення конфіденційності ресурсів); Ц-действия (порушення цілісності ресурсів); Д-действия (порушення доступності ресурсів).

Якщо в процесі атаки порушуються різні характеристики безпеки, то результуючий тип буде комбінований з основних, наприклад, Кцд-дії - атака, що порушує конфіденційність, цілісність і доступність ресурсів.

По природі взаємодії з ресурсами ІКС атаки діляться на: фізичні та логічні.

Для перших характерна фізична форма взаємодії, що проявляється у вигляді різного роду прямих блокувань, ушкоджень, проникнень, крадіжок і т.п., наприклад, розмикання електричних з'єднань, ушкодження носіїв інформації, розукомплектовування, подолання

фізичної границі захисту, підслуховування, перехоплення побічних електромагнітних випромінювань і наведень і т.п. Для других не властиве пряма фізична взаємодія з ресурсами й вони (в основному) пов'язані з логікою подій, наприклад, аналізом протоколів, перевантаженням, підбором паролів, захопленням сеансів й ін.

По реляційних ознаках джерела атаки й атакованого ресурсу атаки діляться на: мономономні; полімономні; монополічні; поліполічні.

Мономономні атаки реалізуються з одного джерела на один конкретний ресурс. Часто такі атаки називають нерозподіленими. Полімономні атаки здійснюються одночасно з декількох джерел (два й більше) на один ресурс і націлені на досягнення однієї конкретної мети. Такі атаки часто називають розподіленими. Монополічні атаки реалізуються з одного джерела одночасно на безліч ресурсів (два й більше) і спрямовані на досягнення конкретної мети. Наприклад, такого типу атаки можуть бути засновані на широкомовній передачі повідомлення від джерела на всі комп'ютери сегмента, адреси яких перебувають під однією маскою підмережі. Поліполічні атаки поєднують у собі полімономні й монополічні технології по яких безліч джерел здійснює атаки на безліч ресурсів з метою досягнення поставленої мети.

По специфіці реалізації атаки діляться на: фрагментировані; без умовчань; сховані; пигібекінгові; маскарадні; непрямі; соціотехнічні; криптоаналітичні; неспецифічні.

Фрагментовані атаки базуються на принципі декомпозиції й поетапної реалізації, наприклад, на основі використання механізму розбивки IP-пакетів (на безліч більше дрібних) і подальшої їхньої передачі. Такий підхід дозволяє обходити системи виявлення атак, які не розраховані на протидію декомпозиційним технологіям. Атаки, які реалізуються без використання значень за замовчуванням (наприклад, програмна закладка BackOrifice за замовчуванням використає порт 31337, але це значення може бути змінено, наприклад, на 31336), орієнтовані на подолання систем виявлення атак, які ґрунтуються на сигнатурні (шаблонових) технологіях за аналогією з антивірусними програмами, призначеними для захисту від сигнатурних вірусів [33]. Сховані атаки використають різноманітні засоби (підміна контрольних сум, перехоплення різноманітних даних, модифікація ядра операційної системи, використання стандартних або схожих на стандартні імена й т.п.), які дозволяють залишатися невиявленими в локалізованій області атакованого ресурсу. Технологія схованих атак по своїй ідеології подібна до технології стелс-вирусов [33]. Пигібекінгові [21] атаки засновані на несанкціонованому одержанні доступу до тимчасово неконтрольованого ресурсу, наприклад, шляхом проникнення до ІКС у результаті тимчасової відсутності або після некоректного завершення сеансу роботи легального користувача. В [24] наведені конкретні приклади таких атак у варіанті захоплення сеансу й додатків. Маскарадні [21] атаки засновані на формуванні такого поводження порушника, що дозволяє йому видати

себе за легальне джерело, наприклад, шляхом обману [21] (spoofing) атакувати обчислювальну мережу (із протоколом TCP/IP) привласнюючи IP-адресу за допомогою якого можна обходити систему захисту. Непрямі атаки засновані на тім, що напад здійснюється через третю особу (посередника), а дійсне джерело нападу залишається невідомим, при цьому часто використаються маскарадні [21] технології. Наприклад, скориставшись варіантом нападу з перенапрямком атаки [24], для виключення можливості виявлення реального джерела, порушник проводить або перенаправляє свій трафик через чужий комп'ютер, що для атакованого ресурсу й буде вихідним джерелом. Соціотехнічні [21] (соціальний інжиніринг) атаки пов'язані з одержанням даних (наприклад, імен користувачів, паролів, телефонних номерів вилученого доступу й т.п.) від атакованих людей у процесі інформаційного обміну. Криптоаналітичні атаки засновані на використанні широкого спектра криптоаналітичних методів [21] і засобів для злому ресурсів, захищених різними криптографічними засобами. До неспецифічних категорій атак ставляться ті, які не мають вищезгаданих особливостей реалізації, при цьому варто враховувати, що технології атак постійно розвиваються й дані ознаки можуть бути розширені.

По спрямованості результату атаки діляться на: розширювальні; такі що викривляють; такі що поширюють; розкрадаючі; перевантажувальні; інформаційні; утримуючі; нищівні.

Розширювальні атаки орієнтовані на одержання більших повноважень на права доступу до ресурсу, наприклад, на вхід у локальну обчислювальну мережу із правами адміністратора, одержання доступу на запис до полів баз даних, зміни атрибутів файлів і т.п. Атаки, що викривляють, пов'язані зі здійсненням будь-яких прямих змін у цільовому ресурсі, наприклад, підробка полів баз даних, підміна інформаційних носіїв, зміна часу й дати й ін. Атаки, що поширюють, спрямовані на одержання доступу до ресурсу і його розкриття без відповідних на це повноважень, наприклад, несанкціоноване одержання файлу даних з паролями і їхньою публікацією на хакерских сайтах або розсилання серед абонентів обчислювальної мережі. Розкрадаючі атаки спрямовані на несанкціоноване використання ресурсу без нанесення прямого збитку, наприклад, без зниження якості обслуговування користувачів здійснюється тимчасове вилучення частини пам'яті (для розширення можливостей іншої системи), завантаження телекомунікаційних каналів, використання робочої станції або мережного сервісу й ін. Перевантажувальні атаки спрямовані на завантаження ресурсу до такого рівня, що він губить свої функціональні властивості щодо його використання. Результатом таких атак можуть бути описані в [20] “неможливість використання ”, “перевантаження”, “перешкоджання використанню” (відмова в обслуговуванні [21]) і т.п. Інформаційні атаки пов'язані зі збиранням необхідних даних (як правило для реалізації подальших дій) і не передбачають здійснення прямого НСД до ресурсу, наприклад, одержання інформації в результаті аналізу публікацій, використання

системних утиліт для виявлення активних робочих станцій, сервісів й т.п. Утримуючі атаки призначені для тимчасової затримки ресурсу з метою зниження його актуальності, наприклад, притримування шифрограми на проміжному вузлі при її передачі телекомунікаційними каналами загального користування. Нищівні атаки орієнтовані на безповоротну ліквідацію ресурсу, наприклад, видалення файлу, дроблення інформаційного носія, низькорівневе форматування жорсткого диска з метою знищення даних і т.п.

По ступені складності атаки можна розділити на: прості; складні; системні.

Прості атаки являють собою нескладні в реалізації послідовності дій, спрямовані на виконання окремих процедур, наприклад, сканування портів, аналіз трафика, пошук активних робочих станцій, вилучене керування й т.п. Складні атаки є комбінацією простих, призначених для реалізації ряду необхідних функцій, наприклад, виявлення активної робочої станції й здійснення вилученого керування нею. Системні атаки будуються на основі сформованого системного підходу з багатокроковою комбінацією дій і використанням простих атак для ефективної реалізації спеціально спрямованого комплексу функцій, наприклад, пошук активних робочих станцій, моніторинг трафика, сканування, злом операційної системи й робочих додатків, несанкціоноване копіювання даних і замітання слідів.

По типу базового ресурсу, на який орієнтовані атаки, останні діляться на: ВОМ-ресурсные (атаки на вузли обчислювальної мережі); ЛОМ-ресурсные (атаки на локальні обчислювальні мережі); Ін^-ресурсні (атаки на інформаційні носії); Оса^-ресурсні (атаки на операційні системи); Пв-ресурсні (атаки на протоколи взаємодії); Пкс-ресурсні (атаки на персонал ІКС); Рп-ресурсні (атаки на робочі додатки); Са-ресурсні (атаки на сценарії автоматизації); Фд-ресурсні (атаки на файли даних) і ін.

Якщо атаки орієнтовані на інші типи ресурсів, то при їхній класифікації вводиться відповідне додаткове скорочення, а у випадку множинної дії тип визначається комбінацією базових ресурсів, наприклад, Рп-фд-ресурсні - атаки на робочі додатки й файли даних.

Міжнародна організація стандартизації (ISO) запропонувала семирівневу еталонну модель із метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Таких класів функцій виділено сім. Вони одержали назву рівнів, кожний з яких виконує певні завдання в процесі передачі блоку інформації, причому відповідний рівень із боку-приймача робить перетворення, зворотні тим, які зроблені на тім же рівні на передавальній стороні (джерелі). У цьому зв'язку атаки по семирівневій еталонній моделі можна визначити на: фізичному рівні, такі що кодуються параметром K0(2) = 20; канальному рівні, кодуються параметром K1(2) = 21; мережному рівні, кодуються параметром K2(2) = 22; транспортному рівні, кодуються параметром K3(2) = 23; сеансовом

рівні, кодуються параметром K4(2) = 24; рівні подання даних, кодуються параметром K5(2) = 25; прикладному рівні, кодуються параметром K6(2) = 26.

На фізичному рівні забезпечуються необхідні механічні, електричні, функціональні й процедурні характеристики для встановлення, підтримки й розмикання фізичного з'єднання.

На канальному рівні забезпечуються функціональні й процедурні засоби для встановлення, підтримки й звільнення ліній передачі даних між абонентами мережі (наприклад, терміналами й вузлами мережі).

На мережному рівні забезпечуються функціональні й процедурні засоби для обміну службовою інформацією між двома об'єктами транспортного рівня мережі (тобто пристроями, які підтримують протоколи на транспортному рівні за допомогою мережного з'єднання). Гарантує незалежність поводження об'єктів транспортного рівня від схеми маршрутизації й комутації.

На транспортному рівні забезпечується оптимізація комутаційного обслуговування (підтримуваного реалізацією більше низьких рівнів зв'язку) шляхом забезпечення прозорих передач даних між абонентами в рамках сеансу.

На сеансовом рівні здійснюється забезпечення на логічному рівні обслуговування двох «зв'язаних» на рівні подання даних об'єктів мережі й керування ведення діалогу між ними шляхом синхронізації повідомлень.

На рівні подання даних забезпечується сукупність службових операцій, які можна вибрати на прикладному рівні для інтерпретації переданих й одержуваних даних. Ці службові операції містять у собі керування інформаційним обміном, відображення даних і керування структурованими даними. Службові операції цього рівня являють собою основу всієї семиуровневой моделі й дозволяють зв'язувати воєдино термінали й засоби обчислювальної техніки всіляких типів.

На прикладному рівні забезпечується безпосередня підтримка прикладних процесів і програм кінцевого користувача й управління взаємодії цих програм з різними об'єктами мережі передачі даних. Визначення класу атаки по даній ознаці наступне - ISO-K, де K= K(2)0 + K(2)1 + K(2)2 + K(2)3 + K(2)4 + K(2)5 + K(2)6 - двійковий код. Для зручності K будемо представляти в шестнадцятеричному коді (K (16)). Наприклад, якщо по цій класифікації атака записана як ISO-3A (де 3A(2)= 0111010 = 25 + 24 +23 +21 = K5 + K4 + K3 + K1), те вона інтерпретує реалізацію на рівні канальному, транспортному, сеансовом і подання даних, а наприклад, запис ISO-00 означає, що клас атак не підтримується семирівневою еталонною моделлю.

Не важко помітити, що атаки, які класифікуються за признаковим принципом, можуть у кожному конкретному випадку при визначенні загального класу містити не тільки одну,

але й більше компонент кожної з ознак. Слід зазначити, що з появою нових методів і засобів реалізації атак, ознаки запропонованої класифікації можуть бути розширені.

При практичному використанні класифікації, наприклад, таку атаку, як сканування портів, за допомогою утиліт ScanPort, Nmap або Essential NetTools можна визначити як: автоматизована, постполітизаційнна, вилучена, вільна, пасивна, безумовна, програмна, зі зворотним зв'язком, До-дії, логічна, мономономна, неспецифічна, інформаційна, проста, Увс-ресурсная, ISO-39.

За допомогою даної класифікації можна здійснювати (відповідну їй) формалізацію можливостей систем протидії для підвищення ефективності їхнього вибору й формуванні вимог при їхній розробці.

8.4. Вимоги до комплексної системи захисту інформації в авіаційних інформаційно-комунікаційних системах

Принципи побудови КСЗІ, виходячи з архітектури ІКС і тенденцій її подальшого розвитку, повинні враховувати особливості архітектури мережі аеропорту й базуватися на положеннях, які містяться в нормативних документах з технічного захисту інформації (НД ТЗІ) і в міжнародних стандартах ISO й МСЕ-Т. При побудові КСЗІ необхідно реалізувати механізми захисту інформації на різних рівнях базової моделі OSI. Варто забезпечити реалізацію таких принципів архітектури безпеки:

КСЗІ будується на основі штатних вбудованих механізмів захисту інформації базового програмного забезпечення (ПЗ), операційної системи (ОС) мережного обладнання, серверів мережних служб і робочих станцій;

- - підвищення рівня захищеності базового ПЗ досягається завдяки модульній побудові КСЗІ, що дозволяє включати до її складу додаткові програмно-апаратні засоби захисту, поетапно розширювати й модернізувати систему із забезпеченням необхідного рівня захищеності інформаційних ресурсів ІКС;
- - централізоване адміністрування й керування засобами КСЗІ;
- узгодження архітектури КСЗІ з архітектурою й принципами побудови ІКС.

КСЗІ ІКС повинна будуватися у вигляді відносно незалежних логічних модулів, які можуть розглядатися як КСЗІ окремих фрагментів й (або) вузлів ІКС (ЛОМ, її доменів, технологій обробки інформації й т.п.) на всіх етапах створення, тобто має забезпечуватися можливість незалежного проектування, впровадження, експертизи й введення в експлуатацію цих компонентів.

Розподіл КСЗІ ІКС на окремі компоненти здійснюється для кожної складової частини ІКС, що має тільки їй властиві переліки конкретних погроз для інформації, критичні інформаційні ресурси або сервери, які надаються абонентам, програмно-апаратні засоби

обробки, відображення, копіювання й друку даних, особливості розташування й характеристики середовища користувачів і технології обробки інформації.

Кожен домен безпеки повинен мати свої правила розмежування доступу, і вимоги до функціонального профілю захищеності інформації.

Вимоги до реалізації послуг безпеки повинні бути реалізовані по єдиним принципами й взаємодіяти між собою в рамках єдиної політики безпеки інформаційних ресурсів ІКС.

Типові компоненти КСЗі в рамках всієї ІКС повинні мати однотипні й функціонально однакові механізми, заходи й засоби захисту інформації.

Вихідні дані баз даних захисту (імена, ідентифікатори ресурсів, атрибути доступу користувачів й ін.) у кожному домені формуються окремо. Ці дані уточнюються на етапі технічного проектування КСЗІ.

КСЗІ ІКС повинна проектуватися таким чином, щоб була можливість оцінити (для будь-яких видів випробувань, у тому числі й державній експертизі) проектні рішення щодо кожного окремого компоненту КСЗІ.

Примітка. Оцінка коректності побудови КСЗІ ІКС у цілому може включати опції з перевірки взаємодії (адміністрування, керування, обмін даними бази даних захисту й т.п.) уже оцінених окремих компонентів КСЗІ.

КСЗІ ІКС необхідно розглядати як інтегровану систему, що утворена сукупністю КСЗІ кожного з доменів безпеки.

8.4.2 Загальні вимоги до КСЗІ

КСЗІ ІКС повинна забезпечувати цілісність інформації, що передається мережею, шляхом забезпечення доступу до неї тільки санкціонованих користувачів і тільки відповідно до встановлених правил розмежування доступу, а також шляхом впровадження механізмів і процедур виявлення фактів порушення цілісності зазначеної інформації, її видалення або копіювання.

КСЗІ ІКС повинна вести облік і здійснювати реєстрацію подій, які пов'язані з безпосереднім доступом (спробами доступу) до інформації, здійснювати безперервний контроль за такими подіями й забезпечувати захист реєстраційної інформації від несанкціонованої модифікації, руйнування або знищення. Обсяг реєстраційної інформації повинен бути достатнім для встановлення причин і джерела виникнення зареєстрованої події.

Послуги ІКС повинні надаватися тільки зареєстрованим користувачам за умови їхнього достовірного розпізнавання.

КСЗІ повинна мати можливість контролювати цілісність власного складу й окремих програмно-технічних компонентів ІКС.

Повинна забезпечуватися можливість однозначного встановлення приналежності інформації, що передається ІКС, певному користувачеві, і встановлення факту передачі або одержання користувачем певної інформації.

Повинне бути виключене з боку користувачів несанкціоноване або неконтрольоване використання ресурсів ІКС.

Критичні з погляду безпеки компоненти КСЗІ повинні контролюватися й (або) резервуватися, для того щоб їхня відмова не приводила до переривання процесу надання послуг.

У випадку виникнення відмов, які порушують функціонування КСЗІ, порядок надання послуг користувачам або абонентам визначається даним вимогами.

КСЗІ повинна підтримувати безпечну інформаційну технологію, в рамках якої доступ до різних видів інформаційних ресурсів, які вимагають захисту, організується таким чином, що тільки вповноваженим користувачам або процесам надається можливість роботи із цією інформацією й гарантується цілісність і доступність інформації при її транспортуванні каналами ІКС.

У випадку відмови КСЗІ (або окремого її модуля) повинен передбачатися режим аварійного блокування доступу користувачів до мережі (або окремого її модуля). Порядок дій користувачів й обслуговуючого персоналу в цих випадках визначається Планом захисту інформації в ІКС, затвердженого Адміністрацією.

ІКС є система, що передбачає можливість розробки й впровадження в її складі нових підсистем (як функціональних, так і систем забезпечення). Принципи й підходи покладені в основу створення КСЗІ повинні забезпечити можливість збільшення кількості виконуваних функцій ІКС або сервісів, які надаються абонентам, забезпечивши при цьому можливість реалізації захисту інформації в нових підсистемах з необхідним рівнем ефективності й гарантій.

Додаткові (закупівельні) технічні, апаратно-програмні й програмні засоби захисту інформації від НСД, які вводяться до складу комплексу засобів захисту (КЗЗ), повинні мати сертифікати або експертні висновки щодо їхньої відповідності вимогам нормативної документації ТЗІ.

8.4.3 Основні вимоги до реалізації політики безпеки

Політика безпеки розглядає інформацію, технології її обробки й користувачів, які ці технології використають, основні погрози для інформації й потенційних порушників, які ці погрози можуть створити, формулює моделі погроз і порушників, визначає інформаційні ресурси, які потребують захисту, і вимоги до захисту інформації.

КСЗІ повинна підтримувати коректно певну політику безпеки - множину правил, які при заданій класифікації суб'єктів доступу й об'єктів захисту, використаються для визначення можливості надання дозволу на доступ конкретного суб'єкта до конкретного об'єкта, надання й зміни повноважень, моніторингу всіх подій, які впливають на безпеку, і їхню реєстрацію.

В основу політики безпеки ІКС повинен бути покладений адміністративний принцип розмежування доступу, відповідно до принципу мінімуму повноважень, а саме право доступу може бути надано лише за фактом службової необхідності. Для втілення принципу мінімуму повноважень повинні бути розроблені відповідні організаційно-розпорядницькі документи аеропорту, інструкції, інші документи, які регламентують діяльність працівників аеропорту в сфері захисту інформації.

Об'єкти захисту в ІКС.

Об'єктами захисту в ІКС є структурні й програмно-інформаційні компоненти кожного з телекомунікаційних вузлів, у яких перебуває або може перебувати інформація, що підлягає захисту, та інформація в каналах транспорту даних у межах контрольованої зони.

Всі вузли нижнього рівня (ВНР) - однотипні, які складаються з локальної обчислювальної мережі (ЛОМ) й локального маршрутизатора. Вони утворюють локальний домен безпеки.

До програмно-інформаційних компонентів, які підлягають захисту, відносять:

- сукупність даних, що мають структури, які відповідають технологіям їхньої обробки й збереження у ЛОМ кожний з вузлів ІКС або в окремих її структурних компонентах;
- програмне забезпечення, що ці технології реалізує;
- потоки даних (дейтаграми), маршрутизацію яких за межі мережі передачі даних (МПД) здійснює локальний маршрутизатор.

До таких об'єктів захисту належать:

- потоки дейтаграм, які передаються каналами передачі даних до/від інших користувачів або до процесів, які цим користувачам належать;
- інформація адміністраторів і користувачів - суб'єкти доступу - і процеси, які функціонують від їхнього імені;
- об'єкти файлової системи - логічні диски, каталоги, підкаталоги, файли на дискетах і жорстких дисках серверів і робочих станцій, які містять інформацію, що підлягає захисту;
- таблиці баз даних, записи, поля баз даних, які містять інформацію, що підлягає захисту;
- інформація керування КСЗІ (дані щодо персональних ідентифікаторів і паролів користувачів, їхніх повноважень і прав доступу до об'єктів, установлених робочих

параметрів окремих механізмів або засобів захисту, інша інформація баз даних захисти, інформація журналів реєстрації дій користувачів і т.п.);

- інформаційні об'єкти, які містять загальнодоступну інформацію (сайту, довідкову, і т.п.);
- активне мережне й серверне обладнання ЛОМ;
- системне й функціональне програмне забезпечення, яке використається для обробки інформації, що підлягає захисту, для забезпечення функцій комплексу засобів захисту (КЗЗ);
- засоби адміністрування обладнання телекомунікаційного вузла (ТВ) і технологічна інформація, що при цьому використається;
- окремі периферійні пристрої, які задіяні в технологічному процесі обробки інформації, що підлягає захисту (друку, накопичувачі інформації, введення даних у ЛОМ).
- інформація, що зберігається на змінних носіях інформації засобів обчислювальної техніки ЛОМ ТВ;
- обчислювальні ресурси (наприклад, дисковий простір, тривалість сеансу роботи користувача із засобами обробки інформації, час використання центрального процесора й т.д.), безконтрольне використання або захоплення яких окремим користувачем може привести до блокування роботи інших користувачів, компонентів ЛОМ ТВ, ЛОМ ТВ в цілому, або магістрального маршрутизатора;
- фізичні й логічні з'єднання;
- спеціалізоване програмне забезпечення для обробки статистичної інформації з обліку часу надання послуг й обсягів трафіку користувачів.

Класифікація об'єктів захисту

Кожен об'єкт (ресурс системи), що контролюється КЗЗ, повинен бути класифікований за наступними реквізитами:

- унікальний ідентифікатор - однозначно ідентифікує об'єкт серед інших об'єктів, повинен генеруватися при реєстрації об'єкта, може змінюватися протягом часу існування об'єкту;
- тип об'єкта - необхідний для визначення КЗЗ способу захисту об'єкта керування (наприклад, каталог, файл, база даних, таблиця бази даних, запис бази даних і т.ін.);
- ідентифікатор пов'язаного з ним ієрархічно вищого об'єкта - указує положення об'єкта в ієрархічній структурі ІКС (компонент ІКС). Указується при реєстрації об'єкта, може змінюватися протягом існування об'єкта при модифікації його положення в ієрархічній структурі;
- ім'я об'єкта - визначає послідовність букв, що ідентифікує об'єкт, зрозумілого для

адміністратора безпеки змісту. Указується при реєстрації об'єкта й не може змінюватися протягом його існування;

- рівень доступу до об'єкта - указує перелік режимів, за якими може здійснюватися доступ до об'єкта (модифікація, вилучення, створення, читання). Конкретний перелік визначається типом об'єкта;
- інформація керування доступом - визначає загальні параметри керування доступом для об'єктів, а також параметри доступу до об'єктів, параметри адміністрування об'єкта (пов'язана з об'єктом інформація бази даних захисту).

Додатково для мережних об'єктів можуть визначатися реквізити:

- унікальна адреса в мережі в числовій, доменній або бездоменній формі;
- унікальний номер процесу по даній мережній адресі (номер порту).

Інформація керування доступом повинна вказуватися при реєстрації об'єкта й може змінюватися протягом часу його існування. Внесення інформації про об'єкти в базу даних захисту КЗЗ повинне здійснюватися адміністратором безпеки відповідно до правил, установленими розпорядницькими документами, які регламентують експлуатацію КСЗІ.

Класифікація суб'єктів

Кожен суб'єкт, що може мати доступ до об'єктів (ресурсів) ІКС, повинен класифікуватися наступними реквізитами:

- унікальний ідентифікатор - повинен однозначно ідентифікувати суб'єкт серед інших суб'єктів, повинен генеруватися при реєстрації суб'єкта й не змінюватися протягом часу його існування;
- тип суб'єкта - може мати значення - "суб'єкт" при описі окремого суб'єкта, "група суб'єктів" при описі групи суб'єктів з однаковими повноваженнями, "суб'єкт - процес", коли описується процес, що активізує інші процеси й відноситься до зовнішніх користувачів, адміністраторів будь-якої категорії й т.д.
- ідентифікатор ієрархічно вищої групи - повинен указувати положення суб'єкта в ієрархічній структурі ІКС . Цей ідентифікатор визначає відносини суміжності ієрархічно вищого суб'єкта стосовно даного. Указується при реєстрації суб'єкта, може змінюватися протягом існування суб'єкта при зміні його положення в ієрархічній структурі;
- ім'я - визначає послідовність букв, що ідентифікує об'єкт. Указується при реєстрації об'єкта й може змінюватися протягом його професійної діяльності:
- рівень повноважень - призначений для реалізації механізмів керування доступом. Повинен разом з рівнем доступу до об'єкта використатися в процесі прийняття рішень про санкціонування або блокування доступу відповідно до адміністративного принципу;

– інформація керування доступом - визначає загальні параметри керування доступом для суб'єктів, а також параметри доступу до об'єктів. Інформація керування доступом повинна вказуватися при реєстрації суб'єкта (групи суб'єктів і може змінюватися протягом часу його діяльності відповідно модифікації його повноважень. Внесення інформації про суб'єкти в базу даних захисту ІКС повинно здійснюватися адміністратором відповідного рівня відповідно до встановлених правил.

Реквізити суб'єктів й об'єктів ІКС відповідно до наведеної класифікації становлять зміст бази даних захисту й утворюють основу формалізованої моделі розмежування доступу ІКС. База дані захисти КЗЗ, інформація керування КСЗІ, конфігураційні файли активного мережного обладнання, серверів мережних служб, таблиці маршрутизації (комутації) активного мережного обладнання; бази даних мережних служб автентифікації віддалених Remote Access Dial-In User Service (RADIUS) і протоколу контролю доступу користувачів Terminal Access Controller Access Control System (Tacacs+) утворюють службову інформацію КСЗІ.

Структура службової інформації й компоненти, які її утворюють визначається розроблювачем на етапі технічного проектування й визначається комплексом засобів обчислювальної техніки, які утворюють ЛОМ ТВ й програмними засобами відповідності до наведених критеріїв.

Конкретна структура реквізитів об'єктів і суб'єктів та їх множина, що дозволяє характеризувати об'єкт і суб'єкт у спосіб, що забезпечить реалізацію прав розмежування доступу відповідно до політики безпеки й формування бази даних захисту, визначається розроблювачем на етапі розробки технічного проекту.

Правила розмежування доступу

Правила розмежування доступу користувачів до ресурсів ІКС визначаються окремо для кожного з компонентів - ЛОМ вузла ІКС і магістрального маршрутизатора - стосовно яких висуваються вимоги щодо реалізації політики безпеки.

8.4.4 Вимоги до засобів захисту від несанкціонованого доступу (НСД)

Загальні вимоги й основні функції.

У кожній підмережі ЛОМ має бути структурована за своїми функціями на окремі сегменти.

Принципи реалізації, основні вимоги й склад функціональних послуг безпеки для сегментів повинні бути однаковими. Їхня відмінність має полягати лише в складі виконуваних ними функцій, задіяних інформаційних ресурсів, списку користувачів і правил розмежування доступу.

Політика безпеки повинна базуватися на адміністративному принципі розмежування доступу.

Організація робіт супроводу КСЗІ, включаючи керування засобами захисту інформації, контроль за дотриманням положень політики безпеки здійснюється службою захисту інформації. Організаційні й правові основи функціонування служби захисту інформації визначаються відповідальними посадовими особами аеропорту у встановленому порядку.

Політика безпеки інформації повинна поширюватися на об'єкти, які безпосередньо або побічно впливають на безпеку інформації.

Правила розмежування доступу й надання атрибутів доступу

Розмежування доступу різних категорій користувачів до різних типів ресурсів вузла доступу встановлюється в границях завдань, які вирішуються підрозділам аеропорту, виходячи з наступних правил:

- адміністратор безпеки має доступ до інформаційних об'єктів, які містять загальнодоступну інформацію, до службової інформації КСЗІ, до засобів захисту інформації, операційних систем і прикладного ПЗ, до технічних засобів, які задіяні в технологічному процесі керування КСЗІ, до інших об'єктів із правами доступу іншого адміністратора (для резервування цих функцій);
- адміністратор активного мережного обладнання має доступ до інформаційних об'єктів, які містять загальнодоступну інформацію, до активного мережного оснащення ЛОМ і магістрального маршрутизатора (або їхньої сукупності), до системного й функціональному ПЗ, що використається для адміністрування й керування ЛОМ і магістральним маршрутизатором, до службової інформації, що при цьому використається, до окремих периферійних пристроїв, які задіяні в технологічному процесі керування ЛОМ і магістральним маршрутизатором;
- адміністратор мережних служб має доступ до інформаційних об'єктів, які містять загальнодоступну інформацію, до об'єктів файлових систем і баз даних з технологічною інформацією вузла, до даних для автентифікації інших вузлів ІКС, до системного й функціональному ПЗ, що використається для забезпечення відповідних функцій КЗЗ, до логічної структури файлової системи, до окремих периферійних пристроїв, які задіяні в технологічному процесі відповідної задачі, до обчислювальних ресурсів відповідної задачі;
- адміністратор електронної пошти має доступ до інформаційних об'єктів, які містять загальнодоступну інформацію, до об'єктів файлової системи й бази даних з технологічною інформацією сервера електронної пошти, до системного й функціональному ПЗ, що використається для забезпечення відповідних функцій КЗЗ,

до логічної структури файлової системи, до окремих периферійних пристроїв, які задіяні в технологічному процесі відповідної задачі, до обчислювальних ресурсів відповідної задачі;

- абонент мережі має доступ до завдань, які вирішуються в границях домена, до інформаційних об'єктів, які містять загальнодоступну інформацію, до об'єктів файлової системи й баз даних, які стосуються його перебування в ІКС, до необхідного для цього системного й функціонального ПО, до технічних засобів, які задіяні в технологічному процесі відповідної задачі, до обчислювальних ресурсів відповідної задачі;
- технічний обслуговуючий персонал має доступ до інформаційних об'єктів, які містять загальнодоступну інформацію, до інформаційних об'єктів, які містять технічну, проектну, експлуатаційну документацію, до відповідних технічних засобів ТВ й ПЗ для проведення робіт з їхнього обслуговування.

Взаємодія зазначених об'єктів, повноваження й права абонентів і правила розмежування доступу для цього типу користувачів установлюються та регламентується положеннями політики безпеки.

Надання користувачеві певної ролі, атрибутів доступу до певного ресурсу і його прав доступу здійснюється тільки у випадках виконання таких умов:

- категорія користувача відповідає типу об'єкта захисту, як це визначено в загальних правилах розмежування доступу;
- доступ до даного об'єкта захисту визначений службовими обов'язками користувача;
- вид взаємодії користувача з об'єктом захисту (перелік дій над об'єктом) установлений специфікаціями послуг безпеки як дозволений;
- вид взаємодії користувача з об'єктом захисту визначений службовими обов'язками користувача.

Вимоги до комплексу засобів захисту

Комплекс засобів захисту повинен складатися з ідентифікованих й оцінених програмних модулів, сукупність яких забезпечує необхідний рівень захищеності інформації.

Вимоги до КЗЗ ЛОМ і до КЗЗ центрального й проміжного вузлів ІКС розрізняються.

У КЗЗ повинна бути включена сукупність всіх програмно-апаратних засобів задіяних для реалізації політики безпеки.

КЗЗ повинен гарантувати користувачам стійкість ІКС до відмов і можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до інших компонентів ІКС.

Під час зберігання, обробки й передачі інформації КЗЗ має забезпечувати реєстрацію дій абонентів і користувачів мережі (ідентифікатор користувача, пароль, Ір-адреса, МАС-

адреса, номер телефону (якщо доступ отриманий через комутовані канали телефонної мережі загального користування), адреси до яких користувач одержувала доступ, час дії й т.п.) способом, що дозволяє однозначно ідентифікувати користувача, адресу робочого місця (місце з якого користувач одержувала доступ до ІКС), з якого здійснений доступ до ресурсів WEB, FTP, e-mail і т.п.) і час, протягом якого здійснювався доступ. Реквізити користувачів, які підлягають реєстрації за допомогою КЗЗ, визначаються на етапі технічного проектування.

КЗЗ повинен забезпечити ідентифікацію користувача з визначенням крапки його входу в ІКС, однозначно аутентифікувати його й зареєструвати результат (успішних або неуспішний) цих подій у системному журналі. У випадку виявлення неавторизованого користувача повинна блокуватися можливість його роботи в ІКС.

КЗЗ повинен забезпечити необхідний рівень цілісності інформації щодо дій користувачів і персоналу в журналах реєстрації компонентів ЛОМ вузлів доступу ІКС із можливим виділенням одного або декількох серверів аудиту. Статистика роботи користувачів повинна бути спостереженою й доступною для адміністратора безпеки й за структурою та обсягом відповідати централізованій моделі керування ІКС.

Журнали реєстрації подій повинні мати захист від несанкціонованого доступу, модифікації або руйнування.

В ІКС або в окремих її компонентах повинна існувати можливість із використанням засобів адміністрування формувати робочі групи (групи обслуговуючого персоналу, користувачів), які мають додаткові можливості щодо одержання окремих послуг:

- за ознакою приналежності до того або іншого сегменту ЛОМ (домену) ТВ ІКС;
- відповідно функціям, які необхідно виконувати конкретному користувачеві або групі користувачів.

При цьому КЗЗ вузла ІКС повинен забезпечувати контроль за можливостями встановлення, перегляду, модифікації стратегій керування (наприклад, реалізація керування віртуальними мережами), а також гарантувати забезпечення контролю за цілісністю засобів адміністрування ІКС.

У КЗЗ повинна бути реалізована можливість виявлення фактів несанкціонованого доступу до об'єктів й (або) процесів, які можуть привести до виникнення погроз для системи відповідно "Моделі погроз в ІКС", і забезпечена фіксація в журналі системи: імені користувача, об'єкта й (або) процесу, до якого була спроба доступу, місця й часу, коли виникла погроза. Допускається фіксація додаткової інформації, що дозволяє однозначно ідентифікувати процеси, які створили погрозу. КЗЗ повинен забезпечити блокування роботи робочих станцій, каналів, адреса, з яких була створена загроза інформації.

КЗЗ повинен:

- починати своє функціонування одночасно із завантаженням ядра операційної системи,

контролювати завантаження ОС, попереджати про небезпечні дії із пристроями збереження інформації;

- працювати безперервно протягом усього часу функціонування ТВ ІКС;
- забезпечувати можливість установлення не менш 16 рівнів обмеження доступу до ресурсів і не менш 8 ролям адміністраторів й 8 ролей звичайних користувачів;
- класифікувати дії користувачів, виявляти спроби несанкціонованих дій і блокувати їх, реєструвати події, які можуть привести до порушення політики безпеки;
- реєструвати події, пов'язані з використанням механізмів ідентифікації іаутентифікації, взаємодією із ЛОМ іншого ТВ ІКС, виконанням команд на визначених мережних пристроях;
- забезпечувати взаємодію із КЗЗ ЛОМ іншого ТВ ІКС;
- автоматично передавати попередження заданих типів на консоль адміністратора безпеки (інших адміністраторів).

КЗЗ повинен забезпечувати такі рівні повноважень для доступу до ресурсів ІКС:

- адміністратора безпеки вузла доступу ІКС;
- адміністратора активного мережного оснащення вузла ІКС;
- адміністратора мережних служб (для здійснення керування сервисами вузла, які надаються (можуть надаватися) абонентам) вузла ІКС ;
- технічного обслуговуючого персоналу вузла ІКС;
- користувачам ІКС.

Список літератури

1. Стеклов В.К., Беркман Л.Н. Телекоммуникационные сети.-Киев.,-2000,-396с.
2. Современные телекоммуникации./ Под ред. Довгого С.А.-М.: Экотрендз,2003-320с.
3. Паук С.М. Сети авиационной электросвязи.-М.,:Транспорт,1986-272с.
4. Андрусяк А.І., Дем‘янчук В.С., Юр‘єв Ю.Н. Мережа авіаційного електрозв’язку. — К.: НАУ, 2001. – 448 с.
5. Беккер П. ISDN. Цифровая сеть и интеграция служб. Пер. с англ. – М.: Радио и связь,1992. – 208 с.
6. Баклеанов И.Г. ISDN и Frame Relay. Технология и практика измерений. – М.: Экто-Трендз, 1999. –и 264 с.
7. Соколов А.В., Шоньгин В.Ф. Защита информации в распредиолительных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 636 с.
8. Романец Ю.В., Тимофеев П.А., Шоньгин В.Ф., Защита информации в копьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перраб. и доп. — М.: Радио и связь, 2001. – 376 с.
9. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. Пер. с англ. — М.: ДМК Пресс, 2001. – 400 с.
10. Герасименко В. А., Малюк А. А. Основы защиты информации. — М.: МГИФИ, 1997. – 538 с.
11. Конахович Г.Ф. Системи радіозв*язку.- К.: НАУ,2004,-312с.
12. Большая энциклопедия шпионажа.…
13. Петраков А. В., Лагутин В. С. Защита абонентского телетрафика. — М.: Радио и связь, 2002. – 504 с.
14. Андрианов В. И., Бородин В. А., Соколов А. В. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие. — Лань, Спб, 1996 – 272 с.
15. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации — К.: Издательство Юниор, 2003. – 504 с.
16. Максименко Г. А., Хорошко В. А. Методы выявления, обработки и идентификации сигналов радио закладных устройств. — К.: ООО «Полиграф консалтинг», 2004. – 317
17. Конеев Н. Р., Беляев А. В. Информационная безопасность предприятия. — СПБ: БХВ – Петербург, 2003 – 725 с.