621.395(075)
Д81

# ЗАХИСТ ЗАСОБІВ І КАНАЛІВ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

В. Б. Дудикевич
В. В. Хома
Л. Т. Пархуць

Видавництво Л

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

**В.Б. Дудикевич,**
**В.В. Хома,**
**Л.Т. Пархуць**

# ЗАХИСТ ЗАСОБІВ І КАНАЛІВ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Навчальний посібник

*Рекомендувало Міністерство освіти і науки, молоді та спорту України*

Львів
Видавництво Львівської політехніки
2012

УДК 621.395.66+004.056.5](0.75.8)
ББК 32.882
Д 812

**Автори:**
**В.Б. Дудикевич,** доктор технічних наук, професор;
**В.В. Хома,** доктор технічних наук, професор;
**Л.Т. Пархуць,** доктор технічних наук, професор

**Рецензенти:**
**Шелест М.Є.,** доктор технічних наук, професор, професор кафедри систем захисту інформації Державного університету інформаційно-комунікаційних технологій;
**Чекурін В.Ф.,** доктор фізико-математичних наук, професор, завідувач відділу Інституту прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України;
**Овсяк В.К.,** доктор технічних наук, професор, професор кафедри автоматизації та комп'ютерних технологій Української академії друкарства

*Рекомендувало Міністерство освіти і науки, молоді та спорту України як навчальний посібник для студентів напряму "Інформаційна безпека" (Лист № 1/11-4635 від 07.06.2011 р.)*

**Дудикевич В.Б.**

Д 812 Захист засобів і каналів телефонного зв'язку: навч. посібник / В.Б. Дудикевич, В.В. Хома, Л.Т. Пархуць. – Львів: Видавництво Львівської політехніки, 2012. – 212 с.

ISBN 978-617-607-283-6

Викладено основи функціонування телефонних мереж загального користування, проаналізовано загрози інформаційній безпеці на об'єктах із телефонним зв'язком, детально описано методи і засоби захисту від витоку інформації абонентськими телефонними лініями, закриття мовних повідомлень під час їхньої передачі каналами зв'язку, запобігання несанкціонованому використанню засобів телефонії.

Призначено для студентів напряму "Інформаційна безпека".

**УДК 621.395.66+004.056.5](0.75.8)**
**ББК 32.882**

© Дудикевич В.Б., Хома В.В., Пархуць Л.Т., 2012
© Національний університет "Львівська політехніка", 2012

ISBN 978-617-607-283-6

# ВСТУП

В останні десятиріччя відбувся бурхливий розвиток і впровадження комп'ютерних мереж та медіатехнологій не лише у різні сфери професійної діяльності, але значною мірою й у побут. Проте й сьогодні в телекомунікаційних мережах телефонні повідомлення за своїм обсягом продовжують переважати трафік усіх інших видів зв'язку, причому така ситуація зберігатиметься ще кілька років. Це означає, що попри усе, люди воліють спілкуватися у натуральний спосіб – наживо, в режимі діалогу, тобто обміну телефонними повідомленнями. Ані електронна пошта, ані чат не можуть передати емоційний стан людини, її манеру розмови, відтворити тембр голосу. Іншою безперечною перевагою телефонного зв'язку є його доступність та поширеність. Кількість абонентів телефонних мереж уже давно перевищила мільярд, а сукупна протяжність "старої доброї мідної пари" на ділянках абонентських та з'єднувальних ліній еквівалентна кільком віддалям від Землі до Місяця.

В умовах лібералізації та інтенсифікації економічних відносин збільшується частка оперативної інформації, а відтак зростає значущість мовного обміну, що безпосередньо пов'язує самостійних у прийнятті рішень людей. Водночас загострюється потреба у забезпеченні конфіденційності мовного обміну. Зазвичай комерційні організації віддають перевагу створенню корпоративної захищеної мережі на основі мереж зв'язку загального користування. Цей шлях передбачає забезпечення власними силами захисту інформації як у каналах зв'язку, так і у місці розташування абонента.

Завдання захисту переговорів, які ведуться у приміщенні на контрольованій території, може бути виконане ціною певних витрат та незручностей для осіб, які беруть участь у переговорах. Значно складніше забезпечити захист мовної інформації у каналах зв'язку, які за своєю суттю завжди більше піддані зовнішнім загрозам. Отже, в сучасних умовах інформаційна безпека абонентів телефонного зв'язку – це актуальне і невідкладне завдання.

Враховуючи те, що ефективний захист певного об'єкта, у тім і телефонних каналів, може бути успішно зреалізований лише за умови досконалого вивчення його функціонування, автори побудували навчальний посібник, починаючи із викладення основ телефонного зв'язку, засад і структурних

елементів цифрової телефонії, структури та функціонування стаціонарних телефонних мереж загального користування. Обговорюються також питання, пов'язані із технологією функціонування системи стільникового зв'язку та пакетної телефонії у комп'ютерних мережах, які завдяки деяким перевагам активно конкурують на ринку надання послуг телефонного зв'язку. Далі розглядаються концептуальні питання інформаційної безпеки на об'єктах із телефонним зв'язком, методи і засоби несанкціонованого одержання інформації із абонентських телефонних ліній, які є найвразливішим та найнезахищенішим елементом телефонної мережі, що зумовлено передусім техніко-економічними аспектами.

Окремі розділи детально описують арсенал засобів, що можуть бути використані для контролю праметрів абонентського шлейфу з метою виявлення та локалізації нелегальних підключень, вивчення будови і способів застосування засобів технічного захисту від прослуховування абонентських телефонних ліній. Особливу увагу приділено висвітленню сучасних підходів до забезпечення конфіденційності обміну телефонними повідомленнями упродовж усього телефонного тракту, а також ознайомленню із методами і засобами запобігання телефонному шахрайству.

# Розділ 1
# ОСНОВИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

В історії техніки телефонний зв'язок посідає особливе місце. За впливом на розвиток цивілізації телефон поза сумнівом можна зарахувати до найвидатніших винаходів людства поряд із колесом, книгодрукуванням, паровою машиною. Із винайденням телефону та становленням телефонного зв'язку пов'язано чимало цікавих і навіть курйозних подій. Вислів "усе геніальне – просте" напряму стосується телефонії. Саме простота телефонного апарата і елементів телефонної мережі сприяла швидкому і широкому розповсюдженню телефонного зв'язку.

У цьому розділі коротко описані основні віхи розвитку телефонії, принцип роботи телефонного апарата, найважливіші структурні елементи телефонних мереж, а також проблеми, пов'язані із забезпеченням надійності та якості обміну телефонними повідомленнями.

У результаті вивчення цього розділу студент повинен знати:

- основні віхи розвитку телефонного зв'язку;
- принципи формування і передачі телефонних повідомлень, а також відтворення акустичних сигналів;
- будову і функції телефонного апарата, зокрема способи абонентської сигналізації;
- призначення і характеристики ліній зв'язку, систем передачі і комутації, які застосовуються у телефонних мережах;
- причини виникнення дестабілізуючих впливів на сигнали у телефонних трактах та способи покращання якості телефонних повідомлень.

## 1.1. Ретроспективний погляд на телефонний зв'язок

### 1.1.1. Принцип телефонної передачі А. Белла

Учитель школи глухих, шотландець за походженням, Александр Грекхем Белл (Alexander Graham Bell) у 1876 році запатентував у США пристрій для передачі мовних повідомлень дротом, що згодом одержав назву "телефон". У

справі патентування А. Белл усього на кілька годин випередив свого конкурента Еліша Грея (Elisha Gray). Ця драматична подія висвітлена у кількох документальних та художніх творах. Напевне чатачеві доводилось чути сакраментальну фразу, вперше вимовлену Беллом через телефон до свого асистента Ватсона, що знаходився у сусідній кімнаті: "Mr Watson–Come here–I want to see you".

Принцип дії телефону Белла був доволі простим, що й ілюструє рис. 1.1.

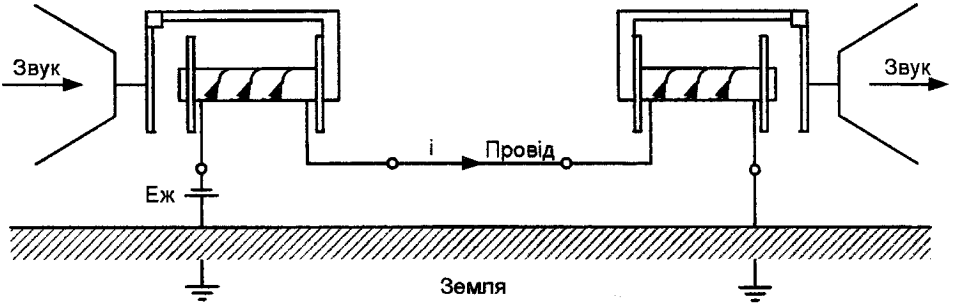



*Рис. 1.1. Схема телефонної передачі А. Белла*

Тонка мембрана вібрувала під дією акустичних хвиль голосу людини. Мембрана була закріплена до електромагніту, тому її коливання наводили електрорушійну силу індукції в електричному колі, утвореному одним проводом і землею. На іншому кінці проводу електричний сигнал знову перетворювався у коливання мембрани, яка виступала вже джерелом звуку.

Телефон Белла містив теж пристрій виклику у вигляді динамо і електричного дзвінка. Абонент, який ініціював розмову, крутив корбу динамо, індукуючи струм виклику, що приводив у дію дзвінок на віддаленому телефоні.

### 1.1.2. Еволюція телефонного зв'язку

Після винайдення телефону Беллом розпочався бурхливий розвиток телефонії, пов'язаний як із удосконаленням самого пристрою, так і способів його використання.

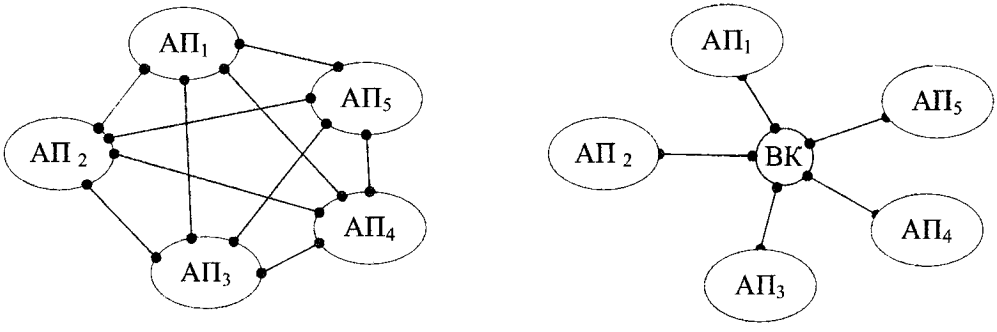
Так, у 1878 році вітчизняний учений М. Михальський розробив перший чутливий мікрофон з вугільним порошком, який у модернізованому вигляді

використовується у сучасних телефонних апаратах. Нагадаємо, що в телефоні Белла і мікрофон, і телефонна капсула були цілком ідентичні та виконані як електромагніти.

Після свого винаходу Белл заснував телефонну компанію, яка спочатку виготовляла і продавала телефонні апарати парами із одним дротом у додаток. Але дуже швидко сам Белл зрозумів проблему раціонального використання засобів телефонного зв'язку між багатьма абонентами. Передусім проблемою була велика кількість ліній зв'язку. У повнозв'язній мережі (рис. 1.2, *а*), коли усі $N_A$ абоненти мережі пов'язані окремими лінiями, кількість ліній $N_{ЛЗ}$ обчислюється за формулою

$$N_{ЛЗ} = \frac{N_A(N_A - 1)}{2}.$$

Наприклад, для $N_A = 5$ абонентів необхідна кількість ліній зв'язку становить $N_{ЛЗ} = 10$, а для $N_A = 10$ – вже $N_{ЛЗ} = 45$.




*а* *б*

*Рис. 1.2. Повнозв'язна (а) та радіальна (б) структури телефонної мережі*

Використання лише одного вузла комутації у так званій радіальній структурі мережі (рис. 1.2, *б*) зменшує кількість ліній відповідно до кількості абонентів ($N_{ЛЗ} = N_A$), але обмежує можливість одночасного обміну повідомленнями.

У 1878 році телефонна компанія Белла вже використовувала ручний комутатор, сконструйований Е.Т. Холмсом (Holmes). Принцип дії полягав у такому. Абонент додзвонювався в офіс телефонної компанії. Коли на комутаторі падала клямка із номером абонента, телефоністка зголошувалася, питаючи з ким має з'єднати абонента, після чого вручну за допомогою кросової комутації реалізувала з'єднання.

Спочатку для телефонного зв'язку використовувалися телеграфні лінії, але для якісної передачі мовних повідомлень знадобилися спеціальні двопровідні телефонні лінії. Вже у 1882 році відбулася перша міжнародна телефонна розмова Париж–Брюссель за допомогою повітряних ліній. В Україні Одеса стала першим містом, де у 1883 році була побудована міська телефонна мережа. У Львові телефонний зв'язок запрацював у 1886 році.

У 1883 році введено в експлуатацію багатопарні кабельні лінії зв'язку, що вирішували проблему перевантаження траверсів повітряних ліній зв'язку.

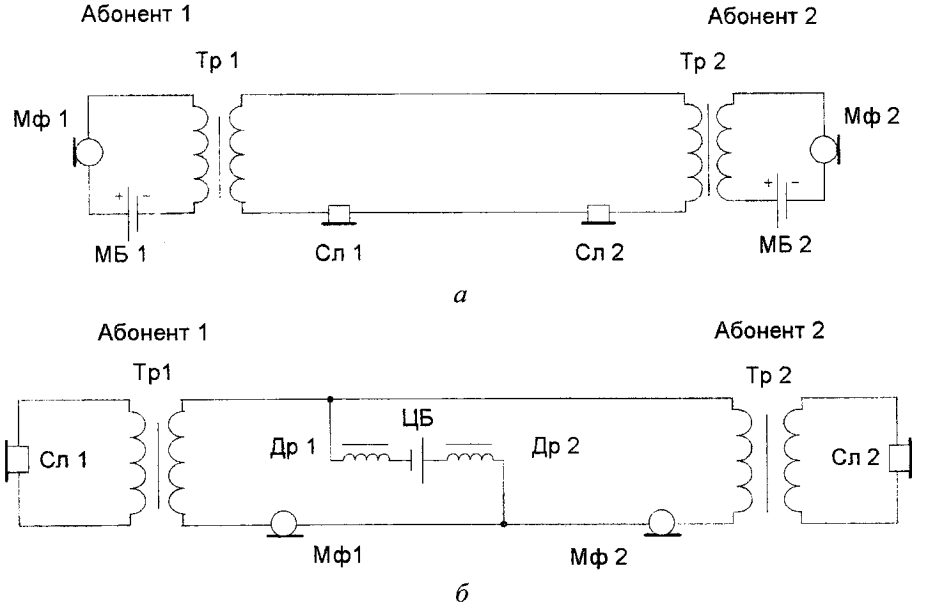



*Рис. 1.3. Схема телефонного зв'язку із місцевою (а) та центральною (б) батареями*

Істотний внесок у вдосконалення телефонного зв'язку зробив російський фізик П.М. Голубицький, який у 1886 році розробив нову схему телефонної мережі, за якою живлення абонентських телефонів здійснювалося від телефонної станції, – так звана система із центральною батареєю (рис. 1.3).

Струм живлення кожного мікрофона проходить через дроселі L1 і L2, оскільки їхній опір постійному струму порівняно незначний (не більше 750 Ом). Водночас дроселі, що мають велику індуктивність, запобігають замиканню змінного (розмовного) струму через центральну батарею, внутрішній опір якої дуже малий (тисячні частки ома). На автоматичних телефонних станціях (АТС) як дроселі часто використовуються двообмоткові реле, що одночасно застосовуються для отримання сигналу про виклик станції абонентом і сигналу закінчення розмови (відбою).

У 1889 році введено в експлуатацію перший таксофон як публічний пункт доступу до послуг телефонної мережі.

У 1892 році підприємець Алмон Браун Строугер (Strowger) із Ла Порте (штат Індіана, США) сконструював першу автоматичну телефонну станцію на 21 номер. Абонент набирав номер абонента за допомогою комбінації трьох клавіш. Після підняття слухавки для оголошення почали використовувати фразу "Aloha, aloha".

У 1923 році запатентовано телефон із дисковим номеронабирачем, який забезпечував імпульсний набір номера і аж у 1960-х роках з'явилась альтернатива у вигляді тонального набору.

У 1927 році компанія AT&T (США) уперше відкрила комерційний трансатлантичний телефонний зв'язок із Лондоном. Вартість дзвінків становила 75 доларів за 5 хвилин.

На 1947 рік припадає перше повідомлення про розроблення фірмою Bell Systems системи з імпульсно-кодовою модуляцією, яка після тривалого доопрацювання у 1962 році була введена в експлуатацію як цифровий канал Т1.

## 1.2. Телефонний апарат як термінальний пристрій телефонної мережі

### 1.2.1. Будова і функції телефонного апарата

Телефонний апарат (ТА) є абонентським термінальним пристроєм телефонної мережі, у складі якого незалежно від конструкції можна виділити три основні функціональні блоки (рис. 1.4):

- розмовну частину, що здійснює перетворення акустичних сигналів мовлення в електричні, і навпаки, електричної енергії у звукову;
- пристрої виклику для генерування звукового сигналу виклику абонента у режимі очікування;
- блок абонентської сигналізації для формування адресної інформації у режимі ініціалізації телефонного сполучення.

Коли трубка ТА не знята, вона натискає на перемикач важеля, утримуючи його у нижньому положенні, як показано на рис. 1.4. При цьому до лінії підключений пристрій виклику, який спрацює під час надходження сигналу виклику від АТС. Пристрій виклику складається із електричного дзвінка Дз та роздільного конденсатора С, який запобігає проходженню постійного струму через обмотки електромагніту дзвінка, а відтак зайвому навантаженню АТС телефонними апаратами, що знаходяться у режимі очікування. Піднімаючи трубку з ТА, перемикач піднімається вгору і підключає до лінії розмовні прилади (мікрофон і телефонну капсулу), а також номеронабирач.

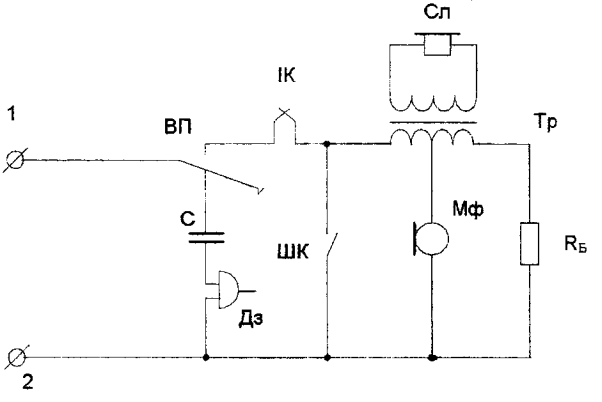



*Рис. 1.4. Схема телефонного апарата: ВП – важільний перемикач; ІК – імпульсні контакти; ШК – шунтувальний контакт; Тр – диференційний трансформатор; Мф – мікрофон; Сл – слухавка; Дз – дзвінок виклику; С – роздільний конденсатор; $R_Б$ – балансний резистор*

***Мікрофон*** – перетворює акустичні хвилі в електричний сигнал. Традиційно у ТА використовуються вугільні мікрофони, що належать до необоротних активних акустоелектричних перетворювачів. Принцип дії ґрунтується на властивості вугільного порошку змінювати опір електричному струму залежно від його щільності, що змінюється під дією звукових коливань повітряного середовища.

Будова вугільного мікрофона і схема його увімкнення в електричне коло показані на рис. 1.5, *а*. Основними елементами мікрофона є рухомий і нерухомий електроди, підключені до електричного кола, і вугільний порошок, що заповнює простір між електродами. Рухомий електрод жорстко пов'язаний із мембраною, яка сприймає акустичні коливання. Елементи мікрофона розміщуються у спільному корпусі, виготовленому із струмопровідного матеріалу. Звукові хвилі викликають коливання мембрани, відтак змінюється густина вугільного порошку. За збільшення густини порошку його опір електричному струму зменшується, а за зменшення – збільшується. Отже, струм у колі, пропорційний до звукового тиску.

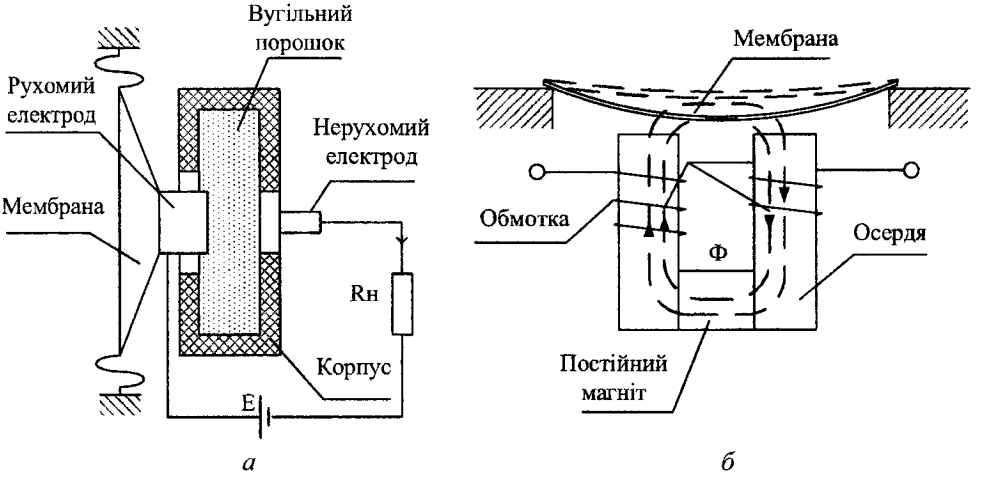



*Рис. 1.5. Будова вугільного мікрофона (а) і електромагнітної телефонної капсули (б)*

***Телефонна капсула,*** або просто ***слухавка*** – здійснює зворотне перетворення електричних сигналів у звукові коливання, призначені для сприйняття

вухом людини. На рис. 1.5, *б* показано будову електромагнітної телефонної капсули, яка належить до пасивних зворотних електроакустичних перетворювачів. Під дією магнітних потоків, що створюються постійним магнітом і електромагнітом, мембрана телефону здійснює коливання, що збігається із змінами електричного струму в обмотці електромагніту.

### 1.2.2. Імпульсний і частотний способи набору номера абонента

Формування адресної інформації, тобто набір номера абонента, може здійснюватися двома способами: **імпульсним і частотним.**

***Імпульсний*** (***"pulse"***) спосіб набору здійснюється за допомогою ***дискового номеронабирача*** замиканням і розмиканням шлейфа на короткий час. У спрощеному вигляді (рис. 1.5) дисковий номеронабирач представлений імпульсними контактами ІК, що власне формують імпульси абонентської сигналізації, та шунтувальним контактом ШК для запобігання потраплянню цих інтенсивних сигналів до розмовної частини телефонного апарата. Кількість циклів замикань і розмикань АТЛ відповідає набраній цифрі номера плюс один стартовий цикл (рис. 1.6). Тривалість одного циклу становить 100 мс, причому 60 мс АТЛ знаходиться у замкненому стані, а 40 мс – у розімкненому.


*Рис. 1.6. Часова діаграма сигналів дискового номеронабирача*

Для забезпечення нормальної роботи приладів АТС до імпульсних номеронабирачів телефонного апарата згідно з ГОСТ 10710-81 ставлять доволі жорсткі вимоги:

1. Частота імпульсів, імп/с – 10.
2. Час розмикання контактів, tp, мс – 60.
3. Час замикання контактів, tз, мс – 40.
4. Шпаруватість імпульсної послідовності – 1,5.
5. Міжсерійна пауза, мс, не менше – 800.

Імпульсний спосіб простий у технічній реалізації і дуже поширений. Проте цей спосіб набору є повільним і незручним у разі потреби набору довгого номера, наприклад, міжміського чи міжнародного.

***Частотний,*** або ***тональний*** (***"tone"***) набір застосовується у ТА із так званими тастатурними (кнопковими) номеронабирачами. Передача кожної цифри згідно з ГОСТ 25554-82 у частотному номеронабирачі здійснюється багаточастотним кодом 2 із 8 (у зарубіжній літературі цей код позначається як ***DTMF – Dual Tone Multi Frequency***). Для цього застосовуються нижня та верхня групи частот (табл. 1.1).

*Таблиця 1.1*

**План частот для тастатурних ТА**

| Частота | 1209 Гц | 1336 Гц | 1477 Гц | 1633Гц |
|---|---|---|---|---|
| 697 Гц | 1 | 2 | 3 | A |
| 770 Гц | 4 | 5 | 6 | B |
| 852 Гц | 7 | 8 | 9 | C |
| 941 Гц | * | 0 | # | D |

Цей код забезпечує 16 комбінацій сигнальних частот, 10 із яких використовуються для набору номера. Кнопки # та * використовуються під час набору кодів додаткових видів послуг. Кнопки **A, B, C і D** застосовуються у розширеній клавіатурі. Тривалість двочастотної посилки повинна бути не меншою за 40 мс, паузи – не меншою за 25 мс, а стабільність частот – не гіршою за ± 1,5 %.

Частотний спосіб передачі адресної інформації використовується лише під час роботи з електронними і квазіелектронними АТС.

## 1.3. Абонентський шлейф, системи передачі та комутації у телефонії

Абонентський шлейф, системи передачі та комутації є трьома основними елементами телефонної мережі, завданням якої є утворення телефонного тракту для забезпечення з'єднання між телефонними апаратами абонентів. Телефонний апарат підключається до ***автоматичної телефонної станції*** (АТС), що виконує у телефонній мережі роль ***вузла комутації***, за допомогою фізичної пари проводів, що називається ***абонентською телефонною лінією*** (АТЛ), або ***абонентським шлейфом***. Своєю чергою, з'єднання між АТС реалізується за допомогою різних ***систем передачі***. У найпростішому випадку системою передачі може бути кабельна з'єднувальна лінія.

### 1.3.1. Способи ефективного використання абонентського шлейфа

Абонентський шлейф переважно утворюється на окремих парах фізичних проводів. У середньому довжина абонентських телефонних ліній становить близько 3 км. За відсутності проміжних підсилювачів максимальна протяжність АТЛ обмежена 4,8 км, щоб виконати вимоги щодо допустимого рівня згасання на цьому відтинку телефонного тракту – 4,5 дБ. Окрема пара проводів та відсутність проміжних підсилювачів дають змогу проводити передачу сигналів в обох напрямках у напівдуплексному режимі.

На деяких АТЛ значної протяжності з метою зменшення експлуатаційних затрат застосовуються технології ущільнення для сумісного використання пар проводів багатьма абонентами. Історично першим способом ущільнення абонентських телефонних ліній були блокатори, але їх вадою були конфліктні ситуації зайнятості лінії, зумовлені жорсткою прив'язкою до однієї фізичної пари двох абонентів. Сьогодні ефективним способом використання АТЛ є технології ***концентрації*** та ***групоутворення*** (рис. 1.7).

Зміст концентрації полягає у комутації активних абонентів на вільні пари АТЛ, причому кількість наявних пар є меншою від загальної кількості обслуговуваних абонентів. Оскільки навіть у години найбільшого навантаження на телефонну мережу активними є близько 30 % абонентів, то концентрація уможливлює на третину зменшити затрати на будову АТЛ.

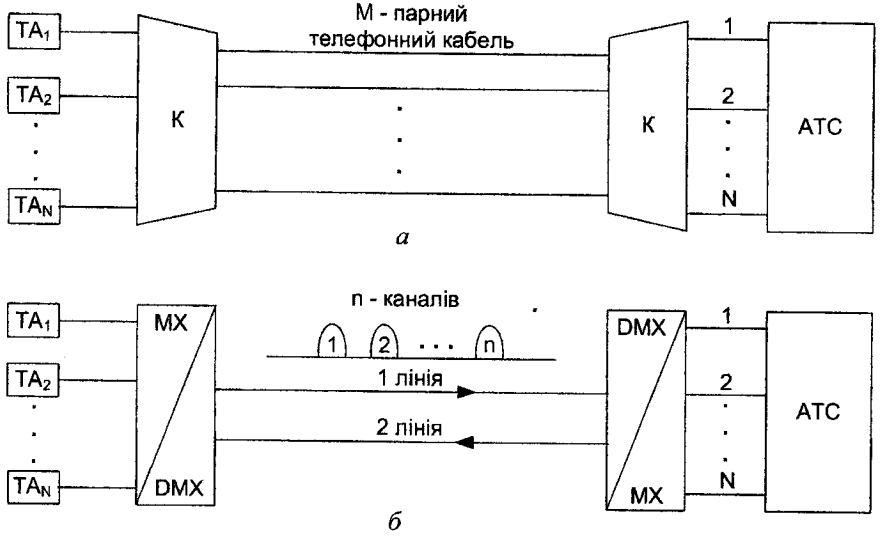



*Рис. 1.7. Ущільнення абонентських телефонних ліній концентрацією (а) та групоутворенням (б)*

Смуга частот пари телефонного кабелю АТЛ значно перевищує спектр частот 300÷3400 Гц сигналу мовлення, тому є можливою передача групового сигналу від кількох абонентів часовим чи частотним ущільненням. Груповий сигнал подається лише в одному напрямку, тобто для двосторонньої передачі на кожну групу абонентів потрібно виділити дві пари проводів. Хоча зростання згасання, яке спостерігається із підвищенням частоти, обмежує кількість абонентів, які можуть обслуговуватися однією парою, проте технологія групоутворення є ефективнішою, ніж проста концентрація первинних сигналів мовлення.

### 1.3.2. Характеристика ліній зв'язку у системах передачі

Лінії зв'язку є фізичним середовищем, яким передаються сигнали. Лінії зв'язку між вузлами комутації (телефонними станціями) прийнято називати з'єднувальними лініями. Сьогодні, крім з'єднувальних ліній на фізичних проводових системах (симетричні та коаксіальні кабелі або світловоди), використовуються також системи радіозв'язку сантиметрового діапазону.

У минулому телефонна мережа будувалася на основі повітряних ліній зв'язку у вигляді телефонних стовпів з горизонтальними траверсами та скляними ізоляторами для підвішування неізольованих металевих дротів. У повітряних лініях зв'язку відстань між дротами становить 20–30 см, отже, діелектриком є повітря. Використовуються дроти: сталевий діаметром 1,5; 2; 2,5; 4 і 5 мм і біметалевий сталево-мідний діаметром 1,2; 1,6; 2; 3 і 4 мм. У біметалевому дроті сталь забезпечує міцність, а зовнішнє мідне покриття завтовшки 0,04÷0,2 мм – захист від корозії та високу провідність завдяки вихровим струмам у приповерхневому шарі. З метою економії міді використовують також біметалевий сталеалюмінієвий дріт.

У подальшому, за винятком сільських районів, повітряні лінії були замінені на кабельні з багатопарними скрученими ізольованими жилами. Основна перевага повітряної лінії полягає у її порівняно малому згасанні у діапазоні частот мовного сигналу (кілька сотих дБ/км). Із збільшенням частоти втрати у лініях зростають, тому сталеві лінії використовують у частотному діапазоні 3÷25 кГц, мідні – до 150 кГц. Основний недолік повітряних ліній полягає у перевитратах міді (діаметр дроту уп'ятеро більший, ніж окремої жили багатопарного кабелю, а значить використовується у 25 разів більше від міді). Крім того, потреба у відчуженні земельних ділянок для стовпів, вплив зовнішніх завад, залежність від погодних умов також є недоліками цього класу ліній зв'язку.

Вирішенням проблеми перевантажених траверсів та великих експлуатаційних витрат на повітряних лініях було введення в експлуатацію (1883 рік) багатопарних симетричних кабелів. Симетричні кабелі складаються з двох абсолютно однакових в електричному і конструктивному відношенні ізольованих дротів (жил), переважно мідних, з діаметрами від 0,32 до 1,4 мм. Для ізоляції використовують такі діелектричні матеріали, як полістирол, поліетилен чи навіть папір.

Ізольовані жили скручуються між собою для ущільнення укладання, тому у зарубіжній літературі симетричний кабель часто називають "скручена пара" (TP – twisted pair). Сучасні симетричні кабелі містять від чотирьох до кількох тисяч пар. Вони використовуються переважно для абонентських телефонних ліній міських телефонних мереж або як з'єднувальні лінії на середні віддалі (до 25 км).

Для зв'язку на більші віддалі використовують широкосмугові коаксіальні кабелі. Якщо однією парою можна передавати близько 100 телефонних сигналів, то одним коаксіальним кабелем можна передати понад 10 тис. таких сигналів. Перший коаксіальний кабель був прокладений у 1941 році і забезпечив передачу 480 телефонних сигналів на віддаль 322 км між містами Мінеаполіс та Стівенс-Пойнтс (США).

Коаксіальні кабелі (від франц. *coaxiale* – співвісний) мають спеціальну конструкцію: один із проводів виготовлений у формі порожнистого циліндра, у центрі якого, відділений діелектриком, розміщається інший провід у вигляді жили.

Найбільше використовують два типорозміри коаксіальних кабелів із такими відношеннями "діаметр жили"/"внутрішній діаметр екрана":

- малогабаритний – 1,2/4,6 мм;
- середній – 2,6/9,5 мм.

Коаксіальна система проводів через свою замкненість викликає мінімальне зовнішнє електромагнітне випромінювання. Сигнал поширюється центральною мідною жилою, коло струму замикається через зовнішній екранний провід.

Вартість коаксіальних кабелів вища, ніж симетричних, але коаксіальні кабелі забезпечують пересилання сигналів у ширшій смузі частот – до кількох сотень мегагерц, хоча сучасні технології дають змогу виготовляти виті пари (категорії 5 і 6) для роботи у частотному діапазоні до 100 мегагерц.

Значним поштовхом у розвитку міжміського телефонного зв'язку стали радіорелейні лінії, які, починаючи з 1948 року (радіолінія між Нью-Йорком і Бостоном), стали використовуватися для створення мережі телебачення. Відстань між антенами радіорелейних систем залежить від структури земної поверхні й висоти антен над нею. Типові відстані становлять 40–50 км за висот башт і щогл, на яких встановлюються антени, близько 100 м. Обмеженість відстані прямої видимості не треба вважати недоліком. Саме за рахунок неможливості вільного поширення радіохвиль на великі відстані усуваються взаємні перешкоди між радіорелейними системами передачі у межах однієї території покриття і сусідніх територій. Крім того, у вказаних діапазонах фактично відсутні атмосферні й промислові перешкоди.

23 квітня 1965 року був запущений на високу еліптичну орбіту перший радянський супутник зв'язку "Молния-1", який ознаменував встановлення супутникового радіозв'язку. Майже одночасно у США був запущений на геостаціонарну орбіту перший супутник комерційного зв'язку "Intelsat-1". Використання супутників різко збільшило дальність зв'язку і посприяло феноменальному збільшенню обсягу міжнародного телефонного трафіку. Перевагами систем супутникового зв'язку є велика пропускна спроможність, висока якість зв'язку і, що найважливіше, глобальність дії, тобто доступність до віддалених районів, зокрема і в гірській місцевості, які не охоплені ні традиційними металевими, ні світловодними лініями, ні наземними радіорелейними лініями. Основним недоліком супутникового зв'язку є затримка розповсюдження сигналу. Для геостаціонарного супутника, розташованого на орбіті понад 36 тис. км, затримка сигналу становить 250 мс, що є відчутним під час телефонної розмови.

Революційним кроком у розвитку ліній зв'язку було винайдення світловода, який, по суті, є кремнієвою ниткою (оптоволокном) діаметром d<100 мкм. Якщо для пересилання електричних сигналів використовується пара металевих дротів, то для світлових сигналів вистачає однієї нитки. Поширення таких сигналів обмежується центральною частиною світловода – так званою серцевиною, яка оточена тоненькою діелектричною оболонкою. Коефіцієнт оптичного заломлення серцевини більший, ніж діелектричної оболонки, що власне і забезпечує режим відбиття світлового променя. Ззовні оптоволокно покривається полімерним шаром.

Для забезпечення механічної міцності у центрі кабелю, що може містити багато волокон, є сталевий трос. Ззовні кабель захищається (від гризунів) сталевим плетенням і герметизується еластичним полімерним покриттям.

У кремнієвих світловодів є три вікна прозорості з малим ослабленням сигналів. Джерелом оптичних сигналів є світловипромінювальний діод або напівпровідниковий лазер.

Світловоди мають унікальні властивості, що позначаються на таких перевагах, як:

- величезна пропускна здатність (одномодове волокно дає змогу одержати смугу пропускання у діапазоні 50÷100 ГГц);

- мале послаблення сигналу (під час використання чутливих фотоприймачів і когерентних методів прийому досягнута довжина ділянки регенерації більше 400 км за використання стандартного одномодового оптоволокна з коефіцієнтом загасання 0,22 дБ/км);
- нечутливість до електромагнітних перешкод, унаслідок чого вірогідність помилки під час передачі по оптичному волокну становить $<10^{-10}$, що у багатьох випадках робить непотрібним контроль помилок у повідомленнях;
- висока безпека від витоку інформації (фактично неможливо зробити відведення);
- невеликі розміри і вага, відносна дешевизна.

### 1.3.3. Етапи розвитку телефонних мереж

Зв'язок між автоматичними телефонними станціями у межах місцевої телефонної мережі може здійснюватися за допомогою з'єднувальних ліній, але на противагу абонентським телефонним лініям використовується так звана чотирипровідна схема, коли для обміну використовуються дві пари проводів – по одній парі на кожен напрям. Крім того, для компенсації згасання сигналів під час передачі на великі віддалі використовуються проміжні підсилювачі, а в сучасних цифрових системах передачі – регенератори. Ще однією особливістю з'єднувальних ліній є використання групоутворення на засадах частотного або часового ущільнення.

Для організації міжміського зв'язку на магістральних лініях значної протяжності використовуються системи передачі на основі засобів радіорелейного зв'язку на сантиметрових хвилях або на перспективних волоконно-оптичних лініях зв'язку. Такі системи передачі є основою первинних мереж зв'язку (див. розділ 3.1).

АТС як система комутації виконує три основні функції – сигналізацію, управління та власне комутацію. Завданням сигналізації є спостереження за станом АТЛ (виявлення активності абонента під час піднесення слухавки й замикання шлейфа) та передачі адресної інформації, одержаної із вхідних ліній до пристрою управління. Крім того, сигналізація передбачає і формування службових сигналів та їх надсилання на вихідні лінії.

Пристрій управління опрацьовує сигналізаційну інформацію та виробляє керуючі сигнали для комутаційного поля, де власне і реалізується функція комутації, тобто зіставлення відповідних вхідних і вихідних ліній.

У процесі розвитку телефонних мереж можна виділити три етапи, які напряму пов'язані із цифровізацією систем передачі та комутації (рис. 1.8, *а, б, в*).

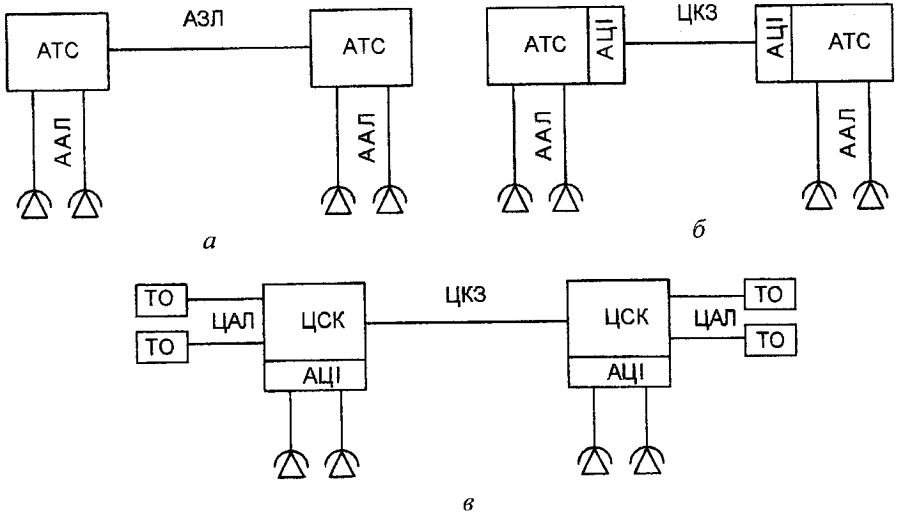



*Рис. 1.8. Еволюція телефонних мереж:*
*ААЛ – аналогова абонентська лінія; ЦАЛ – цифрова абонентська лінія;*
*АЗЛ – аналогова з'єднувальна лінія; ЦЗЛ – цифрова з'єднувальна лінія;*
*АЦІ – аналого-цифровий інтерфейс; ЦСК – цифрова система комутації;*
*ТО – термінальне обладнання*

На першому етапі усі елементи телефонної мережі були аналоговими. У 50-х роках XX ст. розпочався процес переходу від аналогових систем передачі на з'єднувальних лініях до цифрових, що і відображає основний зміст другого етапу. Оскільки АТС залишалися аналоговими, то їх зв'язок із цифровими з'єднувальними лініями відбувався через аналого-цифровий інтерфейс. На третьому, сучасному етапі комутація відбувається у цифровому вигляді, тому аналого-цифровий інтерфейс перемістився до аналогових абонентських ліній. Проте цифрові системи комутації оснащені також цифровим інтерфейсом для під'єднання спеціального цифрового абонентського термінального обладнання.

## 1.4. Чинники, що впливають на якість передачі сигналів у телефонії

У процесі передачі телефонною мережею сигнали мовлення зазнають небажаних змін (спотворень), джерелом яких є різні завади, а також вплив параметрів реальних каналів зв'язку. Для оцінки якості передачі сигналів у телефонії аналізуються такі чинники, як завади, шум, згасання і спотворення сигналу.

### 1.4.1. Завади і шум

***Завада*** – це деякий процес, що перешкоджає проходженню сигналу каналами зв'язку. ***Шум*** – це особливий вид завад, що створюються тепловим рухом електронів у середовищах поширення сигналу. Завадами можуть бути сигнали сусідніх каналів зв'язку, електромагнітне випромінювання різних технічних пристроїв. На відміну від шуму завади мають структурованіший характер, хоча також є випадковим процесом. Якщо параметри завади близькі до корисного сигналу, то вони називаються ***перехресними завадами***.

Зазвичай основним джерелом перехресних завад є електромагнітний зв'язок між жилами кабелю, неадекватна фільтрація в аналогових системах передачі та міжсимвольна інтерференція у цифрових системах.

За місцем утворення розрізняють перехресні завади на ***ближньому*** (***near-end crosstalk – NEXT***) і ***дальньому*** (***far-end crosstalk – FEXT***) кінцях (рис. 1.9). Перехресні завади на ближньому кінці утворюються між передавачем та приймачем одного каналу, а на дальньому – між місцевим приймачем та віддаленим передавачем сусіднього каналу. Перехресні завади на дальньому кінці мають менший вплив, тому що сам сигнал зазнає згасання у процесі проходження каналом зв'язку.

Тепловий шум виникає в усіх електричних компонентах систем зв'язку, зокрема й у акумуляторних батареях, що живлять абонентські телефонні лінії. Моделлю такого шуму є випадковий процес із нормальним (гауссівським) розподілом амплітуд.

Іншими видами шуму є шум квантування, який виникає під час оцифровування аналогових мовних сигналів. Крім того, у телефонії, особливо за

наявності електромеханічних комутаційних полів, виникає так званий імпульсний шум, що є послідовністю імпульсів із випадковими амплітудами, тривалостями і моментами появи.

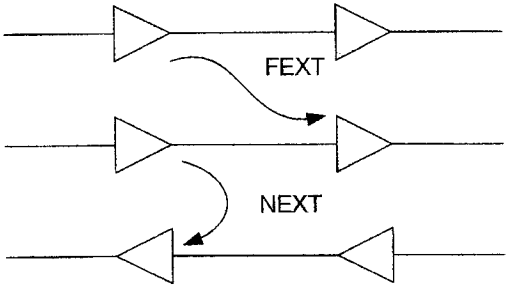



*Рис. 1.9. Утворення перехресних завад на ближньому і дальньому кінцях*

Дослідження показують, що найвідчутнішими у телефонії є спотворення сигналу у діапазоні від 700 до 2000 Гц.

### 1.4.2. Спотворення і згасання сигналу

У телефонній мережі між телефонними апаратами абонентів за допомогою абонентських ліній, пристроїв концентрації, вузлів комутації та лінійного обладнання утворюється канал зв'язку, яким проходить сигнал із нанесеним на нього повідомленням. Зв'язок між вхідним $s(t)$ та вихідним $r(t)$ сигналами каналу повністю визначається ***імпульсною характеристикою каналу*** $h(t)$. Крім того, під час проходження сигналу каналом зв'язку додаткові випадкові шуми і завади спотворюють його, тому у пункті приймання сигнал $r(t)$ відрізняється від переданого $s(t)$:

$$r(t) = s(t) * h(t) + \xi(t), \tag{1.1}$$

де знак "$*$" є операцією згортки, а $\xi(t)$ – адитивні завади.

***Спотворення*** – це небажана зміна параметрів сигналу під дією завад або неідеальних параметрів каналу зв'язку та блоків передавального і приймального трактів. Розрізняють ***випадкові*** й ***детерміновані (лінійні*** та ***нелінійні)*** спотворення. Випадкові спотворення зумовлені накладанням на сигнал випадкового процесу, наприклад, шуму. Детерміновані спотворення можуть виникати внаслідок неідеальної амплітудно-частотної і фазочастотної характеристик каналу, при цьому нелінійні спотворення призводять до появи у спектрі сигналу нових гармонічних складових, а лінійні лише змінюють амплітуди і фази існуючих у сигналі спектральних компонент.

***Згасання*** – це частковий випадок спотворення, за якого форма сигналу $r(t)$ на прийомі зберігається і відрізняється від переданого $s(t)$ лише рівнем, тобто імпульсна характеристика каналу $h(t)$ є дійсним числом. Насправді у реальних каналах змінюються не лише амплітуди окремих гармонік, а також і їхні фази. Для їхньої компенсації використовують вирівнювальні пристрої – ***еквалайзери***.

### 1.4.3. Ехо і самозбудження

Явища еха і самозбудження виникають внаслідок потрапляння передаваних сигналів через паразитні взаємозв'язки у зворотний канал і повернення до свого джерела. Причиною виникнення зворотних зв'язків є неузгодженість імпедансів диференціальних систем (ДС), що використовуються для під'єднання двопровідних систем до чотирипровідних (рис. 1.10). Оскільки на практиці ідеальне узгодження імпедансів ДС неможливе через розкид і нестабільність характеристичних опорів абонентських та з'єднувальних ліній, передавані сигнали відбиваються і поширюються у зворотному напрямі. Розрізняють "ехо диктора", утворене на дифсистемі у пункті передачі, і "ехо слухача" – на дифсистемі у пункті приймання. Якщо у процесі передачі сигнали зазнають багатократних відбиттів, то відбувається явище самозбудження (генерування). Умовою самозбудження є випадок, коли на певній частоті контурне підсилення стає більшим за одиницю.

Ступінь перешкоджаючого впливу еха залежить не лише від рівня відбитого сигналу, але і від його затримки. Якщо довжина телефонного тракту перевищує 1125 км, то двостороння затримка перевищує 45 мс і тому

доводиться вносити у тракт додаткове згасання. Для розрахунку, необхідного для зменшення ефекту еха, рівня згасання на міжміських лініях потрібно враховувати, що сигнал еха зазнає подвійного згасання, оскільки на відміну від прямого сигналу проходить подвійний шлях.

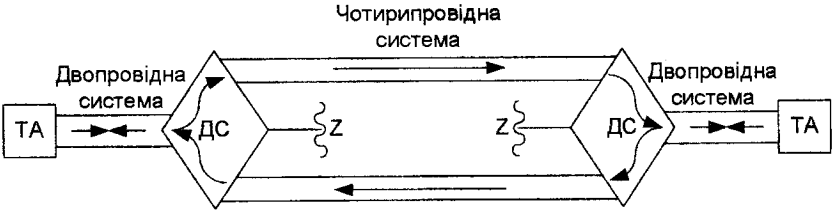



*Рис. 1.10. Утворення еха на стику двопровідної і чотирипровідної систем*

Раніше додаткове згасання вносилося лише у зворотний тракт пристроями, які називаються ***ехо-загороджувачами***. Принцип їхньої дії полягав у порівнянні рівнів сигналів у кожному колі чотирипровідної системи з метою визначення напряму передачі й включення додаткового згасання (35 дБ). Робота ехо-загороджувачів супроводжувалася так званим кліпуванням початкових фрагментів мовних сегментів за зміни напрямів передачі.

Вказаний недолік усунено у сучасних пристроях – ***ехо-компенсаторах***. Принцип дії цих пристроїв полягає у запам'ятовуванні передаваного мовного сигналу впродовж інтервалу, що дорівнює подвійній затримці сигналу та його відніманню із прийнятого сигналу із урахуванням впливу імпульсної характеристики каналу.

## Питання для самоконтролю:

1. Поясніть принцип телефонної передачі, запатентованої А. Беллом.
2. Які винаходи мали визначальний вплив на розвиток телефонії?
3. Порівняйте схеми телефонного зв'язку із місцевою та центральною батареями.
4. Що таке лінія, канал та мережа зв'язку? Як співвідносяться між собою ці поняття?

**5.** Зобразіть спрощену схему телефонного апарата та поясніть призначення кожного елемента.

**6.** Поясніть фізичний принцип роботи вугільного мікрофона та слухавки телефонного апарата.

**7.** Вкажіть на призначення та розкрийте принципи формування сигналів абонентської сигналізації (імпульсної та частотної).

**8.** Охарактеризуйте три етапи еволюції телефонних мереж.

**9.** Що таке абонентський шлейф? Які способи підвищення ефективності його використання ви знаєте?

**10.** Вкажіть призначення і дайте характеристику лініям зв'язку і системам передачі, які застосовуються для передачі телефонних повідомлень.

**11.** Обґрунтуйте переваги світловодів як середовища передачі сигналів у сучасній телекомунікації.

**12.** Які чинники знижують якість передачі телефонних повідомлень?

**13.** Дайте порівняльну оцінку завадам і шумам, що існують у телефонних трактах.

**14.** Що таке спотворення і згасання і якими є причини їх виникнення? Який принцип дії еквалайзерів?

**15.** Поясніть природу еха і самозбудження та вкажіть способи зменшення впливу цих чинників у сучасній телефонії.

# Розділ 2
# ЗАСАДИ І СТРУКТУРНІ ЕЛЕМЕНТИ ЦИФРОВОЇ ТЕЛЕФОНІЇ

Свій вражаючий за масштабами наступ на аналогові системи цифрові технології розпочали саме у галузі електрозв'язку, коли у 60-х роках минулого століття на з'єднувальних магістральних лініях американці застосували імпульсно-кодову модуляцію для передачі телефонних повідомлень. Пізніше стрімкий розвиток і здешевлення мікропроцесорної техніки, що кардинально змінили технологію телекомунікаційної сфери, призвели до появи цифрових систем передачі та комутації, інтегрування послуг зв'язку.

Цей розділ важливий для розуміння принципів, що лежать в основі цифровізації телефонного зв'язку, переваг і нових можливостей, які відкриваються у світі цифрових технологій.

У результаті вивчення цього розділу студент повинен знати:

- основні параметри сигналів мовлення;
- принципи імпульсно-кодової модуляції, підвищення ефективності передачі телефонних повідомлень під час використання компандування та диференціальної імпульсно-кодової модуляції;
- призначення вокодерів, засади будови та функціонування формантних і канальних вокодерів, а також вокодерів із лінійним передбачуванням;
- засади часового групоутворення сигналів імпульсно-кодової модуляції та ієрархії цифрових систем передачі;
- структуру і функції цифрових систем комутації;
- переваги та недоліки цифрової телефонії.

## 2.1. Перетворення сигналу мовлення у цифровий вигляд

### 2.1.1. Параметри сигналів мовлення

За способом генерування звуки людської мови належать до однієї із двох категорій. Перша категорія охоплює звуки, що позначаються на письмі голосними і дзвінкими приголосними буквами. Джерелом цих звуків є голосові

зв'язки людини, які, вібруючи, під дією повітряного струменю легенів формують квазіперіодичний акустичний сигнал, так званий ***основний тон*** (рис. 2.1, *а*). Друга категорія звуків, що включає глухі та шиплячі, утворюється турбулентним повітрям легень, що проходить через звуження голосового тракту за розслаблених голосових зв'язок (рис. 2.1, *б*).

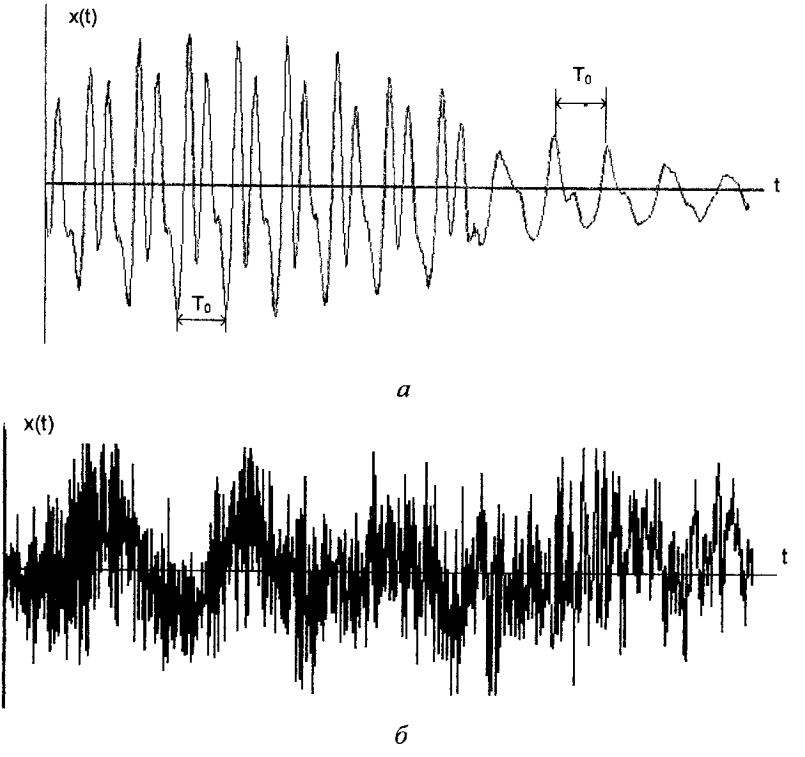



*Рис. 2.1. Фрагменти сигналів голосного чи дзвінкого приголосного звука (а) та глухого чи шиплячого звука (б)*

Зіставлення часових перебігів двох категорій звуків показує, що глухі звуки більше схожі на випадкові шумові сигнали, а дзвінкі – на полігармонічні сигнали. Дослідження показали, що спектр основного тону містить понад 40 гармонік, амплітуда яких спадає із збільшенням частоти із швидкістю приблизно 12 дБ/окт (рис. 2.2, *а*). Перша гармоніка $f_0$ основного тону

знаходиться в діапазоні від 50÷80 Гц (дуже низький голос, бас) до 200÷250 Гц (дитячий і жіночий голоси). Сигнал основного тону пов'язаний із фізіологічною будовою голосових зв'язок людини, а тому несе на собі індивідуальні особливості кожної людини. Біометричні системи із розпізнаванням за голосом працюють на основі аналізу сигналу основного тону.

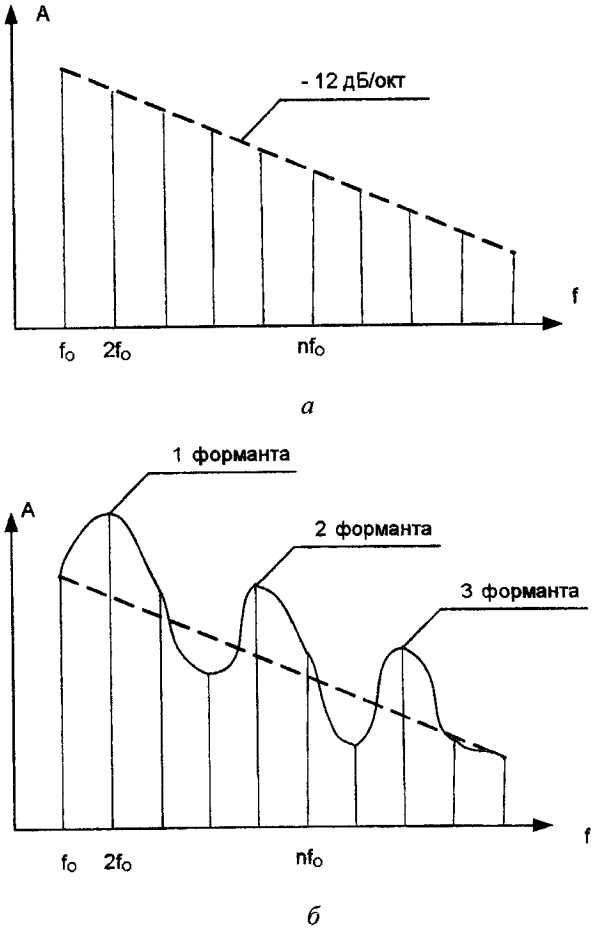



*Рис. 2.2. Спектральний склад основного тону (а) та промодульованого у ротовій порожнині звука (б)*

Конкретні звуки мовлення у кожній із категорій утворюються у результаті оброблення акустичного сигналу (основного тону чи шумоподібного) у ротовій порожнині, що виконує функцію акустичного модулятора. Під час вимовляння різних звуків потужність гармонік основного тону змінюється, утворюючи області підвищеної потужності гармонік основного тону, що називаються ***формантами*** (рис. 2.2, *б*). Різні звуки мови містять від двох до чотирьох формант.

Висока якість передачі телефонного сигналу характеризується рівнем гучності, розбірливістю, природним звучанням голосу, низьким рівнем перешкод. Ці чинники визначають вимоги до телефонних каналів.

Основними параметрами телефонного сигналу є:

- ***максимальна потужність*** телефонного сигналу становить 2200 мкВт (абсолютний рівень+3,5 дБм), окреслюється як значення, ймовірність перевищення якої мала;
- ***мінімальна потужність*** прийнята такою, що дорівнює 0,22 мкВт (відповідає рівню – 36,5 дБм), окреслюється як значення, за якого телефонний сигнал ще чути на тлі шумів;
- ***коефіцієнт активності*** телефонного повідомлення – це відношення часу, впродовж якого потужність сигналу на виході каналу перевищує задане порогове значення, до загального часу утримання каналу для розмови. Під час розмови кожний із абонентів говорить приблизно 50 % часу. Крім того, між окремими словами та фразами є паузи, тому коефіцієнт активності становить 0,25…0,35;
- ***середня потужність*** телефонного сигналу (виміряна у точці нульового відносного рівня) на інтервалах активності (за відсутності тривалих пауз) становить 88 мкВт. Окрім мовних сигналів, у канал зв'язку надходять сигнали управління, набору номера тощо. З іншого боку, під час розмови близько 75 % часу займають паузи (коефіцієнт активності 0,25). Тому середня потужність телефонного сигналу, виміряна в годину найбільшого навантаження (ГНН) із врахуванням службових сигналів та коефіцієнта активності, становить 32 мкВт, що відповідає абсолютному рівню (віднесеному до 1 мВт):

$$P_{CP} = 10\lg\frac{32\,мкВт}{1\,мВт} = -15\ дБм0;$$

- ***динамічний діапазон*** телефонного сигналу визначається вираженим у децибелах відношенням максимальної та мінімальної потужностей:

$$D = 10\lg\frac{P_{\max}}{P_{\min}} = 10\lg\frac{2200\,мкВт}{0,22\,мВт} = 40\ дБ;$$

- ***пік-фактор*** телефонного сигналу визначається вираженим у децибелах відношенням максимальної та середньої потужностей:

$$Q = 10\lg\frac{P_{\max}}{P_{ср}} = 10\lg\frac{2200\,мкВт}{32\,мкВт} = 10lg\,68,75 = 18,4\ дБ;$$

- ***енергетичний спектр*** мовного сигналу – це область частот, в якій зосереджена основна енергія сигналу. Дослідження енергетичного спектра показало, що мова є широкосмуговим нестаціонарним випадковим процесом, спектр якого зосереджений у смузі від 50÷100 до 8000÷10000 Гц. Також виявлено, що основна енергія сигналу зосереджена у смузі 300÷3400 Гц, тому якість мови залишається цілком прийнятною за такого обмеженого спектра. Отже, частотний діапазон 300÷3400 Гц був стандартизований Міжнародним Союзом Електрозв'язку МСЕ-Т (колись МККТТ) як канал тональної частоти (КТЧ). У смузі частот КТЧ зберігається задовільна натуральність звучання мови, складова розбірливість становить близько 90 %, а розбірливість фраз – більше 99 %;

- ***кількість інформації***, що міститься у мовному сигналі, обчислена за формулою Шенона, становить:

$$J = W\log_2\left(1+\frac{P_{ср}}{P_{ш}}\right) = 3100\,Гц\times\log_2\left(1+\frac{0,25\times 88\,мкВт}{178\,нВт}\right) =$$
$$= 3100\times\log_2(125) = 8000\ біт/с.$$

Вплив шумів на якість телефонного зв'язку характеризується так:

- за потужності шумів 17,8 нВт шуми ледь відчутні;
- за потужності шумів 178 нВт розбірливість мови ще добра;
- за потужності шумів 1780 нВт розбірливість мови ускладнена і якість зв'язку незадовільна.

### 2.1.2. Імпульсно-кодова модуляція

Формування цифрового телефонного сигналу із аналогового передбачає послідовне виконання трьох основних операцій (рис. 2.3):

- ***дискретизацію*** аналогового сигналу $x(t)$ в часі, внаслідок чого формуються вибірки $x(nT_S)=x(n)$, що відповідають миттєвим значенням телефонного сигналу у моменти часу $t=nT_S$;
- ***квантування*** одержаних вибірок за рівнем, тобто заміна реального значення вибірки $x(n)$ найближчим дозволеним рівнем $\hat{x}(n)$;
- ***кодування*** проквантованих відліків телефонного сигналу за допомогою подання значень квантованих вибірок $\hat{x}(n)$ у певному форматі чисел, наприклад, двійковому.

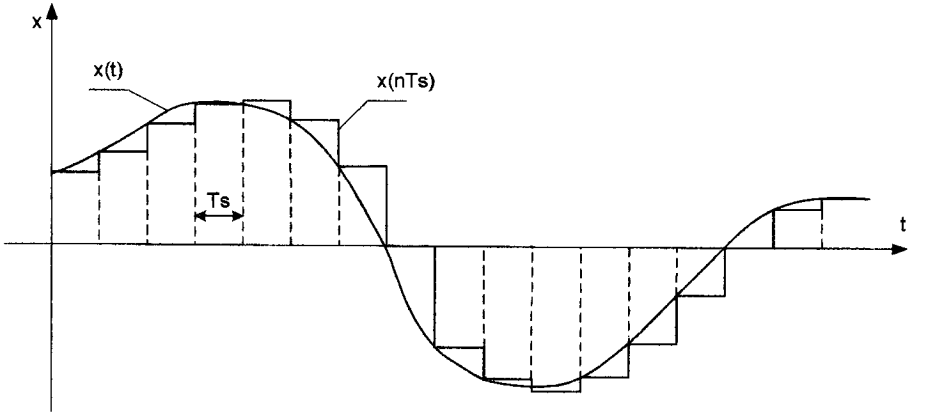



*Рис. 2.3. Оцифровування аналогового сигналу*

Зворотне перетворення ІКМ-сигналу в аналоговий передбачає послідовне виконання таких операцій:

- ***декодування***, тобто перетворення ІКМ-сигналу у дискретний сигнал (сходинкова апроксимація початкового сигналу);
- ***відновлення*** аналогового сигналу (виділення із дискретизованого сигналу початкового телефонного сигналу).

Дискретизація у часі аналогового сигналу здійснюється за відомою теоремою Котельникова–Шенона: будь-який безперервний сигнал, спектр якого обмежений згори частотою $F_M$, повністю визначається послідовністю своїх дискретних відліків, узятих через проміжок часу $T_S = \frac{1}{2F_M}$, що називається періодом дискретизації.

Теоретично скінченні у часі сигнали мають нескінченно широкий спектр, однак у реальних телефонних сигналів основна енергія зосереджена у порівняно вузькій смузі частот 300...3400 Гц. Тому перед дискретизацією за допомогою фільтра нижніх частот з частотою зрізу $F_C = 3400\,Гц$ обмежують спектр телефонних сигналів, а частоту дискретизації вибирають дещо вищою – 8 кГц.

Дискретизація у часі виконується за допомогою так званого пристрою ***вибірки і зберігання*** (англ. ***sample&hold***). На рис. 2.4 показано варіант реалізації такого пристрою.

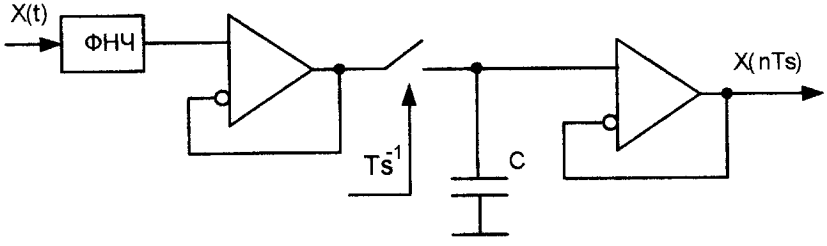



*Рис. 2.4. Пристрій вибірки і зберігання*

У процесі квантування за рівнем значення кожної вибірки замінюється найближчим дозволеним рівнем квантизатора.

***Квантизатор*** характеризується такими параметрами:

- кількість рівнів квантування $N_q$;
- крок квантування $q$ – різниця між двома сусідніми дозволеними рівнями;
- границя діапазону $U_m$ – максимально допустиме значення амплітуди відліку, що піддається квантуванню.

Якщо $q = const$, то квантування називають рівномірним. Амплітудну характеристику рівномірного квантизатора показано на рис. 2.5.

Процес квантування супроводжується виникненням так званих ***помилок квантування*** $\Delta_q(n)$, зумовлених різницею між дійсним $x(n)$ і квантованим $\hat{x}(n)$ значеннями вибірок. За рівномірного квантування значення цієї помилки не перевищує півкроку квантування. Ефект від похибок квантування називається ***шумом квантування.*** Відношення "сигнал/шум квантування", що визначається виразом

$$\eta = \frac{P}{P_q} = \frac{E\left\{x^2(n)\right\}}{E\left\{\left[\hat{x}(n) - x(n)\right]^2\right\}},$$

можна використати для оцінки захищеності сигналу.

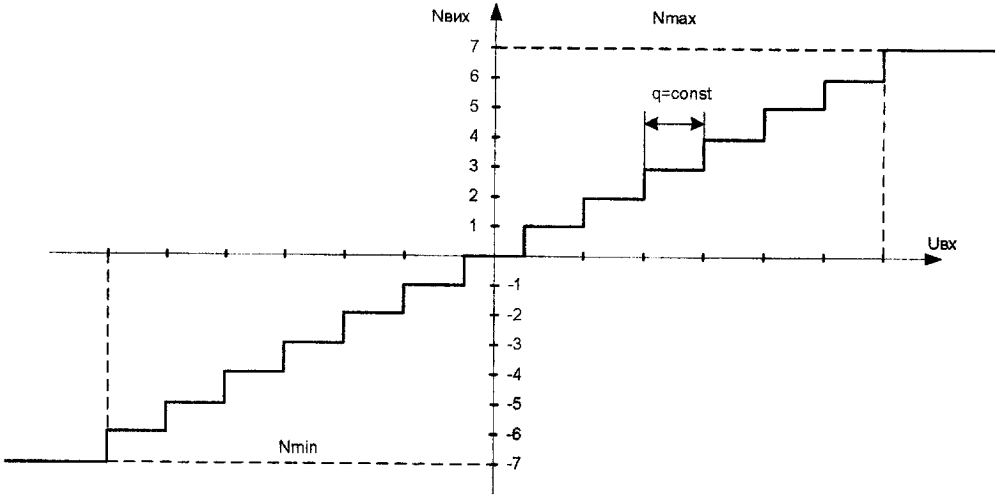



*Рис. 2.5. Амплітудна характеристика рівномірного квантизатора*

За рівномірного розподілу потужність шуму квантування дорівнює

$$\sigma_q^2 = \frac{q^2}{12},$$

а відношення "сигнал/шум квантування" у логарифмічному вираженні

$$\eta = 10lg\frac{x^2}{q^2/12} = 10{,}8 + 20\lg\frac{\sigma_x}{q},$$

де $\sigma_x$ – середньоквадратичне значення сигналу.

Зокрема для синусоїдального сигналу

$$\eta = 10lg\frac{A^2/2}{q^2/12} = 7{,}78 + 20\lg\frac{A}{q},$$

де $A$ – амплітудне значення синусоїдного сигналу.

Для n-розрядної системи ІКМ крок квантування пов'язаний із динамічним діапазоном співвідношенням

$$q = \frac{2U_m}{2^n}.$$

Підставляючи його у попередній вираз, одержуємо

$$\eta = 10lg\frac{6A^2}{q^2} = 10lg\frac{6A^2}{4U_m^2}2^{2n} = 10\lg 1{,}5 + 20n\lg 2 + 20\lg\frac{A}{U_m} =$$

$$= 1{,}76 + 6{,}02n + 20\lg\frac{A}{U_m}.$$

Якщо рівень вхідного сигналу перевищує граничне значення $U_m$, то квантизатор працює у режимі перевантаження, а на виході квантизатора формуються відліки з амплітудою $U_m$. При цьому виникають ***шуми обмеження***, потужність яких значно перевищує потужність шумів квантування. Необхідно застосовувати спеціальні заходи, що запобігають перевантаженню квантизатора.

Недоліком рівномірного квантування є низька захищеність від шумів квантування малих рівнів сигналу. Для забезпечення η не менше 30 дБ в усьому динамічному діапазоні мовного сигналу потрібно $L = 2^{12} = 4096$ рівнів квантування.

### 2.1.3. Компандування

Велика кількість розрядів у коді ($i=12$) за рівномірного квантування призводить до невиправданого збільшення тактової частоти. У цифровій телефонії цей істотний недолік усувається нерівномірним квантуванням, за якого для малих значень сигналів крок квантування вибирається мінімальним і поступово збільшується, досягаючи максимального для великих значень сигналів (рис. 2.6).

При цьому для слабких сигналів потужність шуму квантування зменшується, а для сильних, що мають невиправдано великий запас за завадостійкістю, – зростає. Це приводить до вирівнювання $\eta$ у широкому діапазоні зміни рівнів сигналу (збільшення $\eta$ для слабких сигналів і зниження для сильних). У результаті вдається у півтора раза знизити розрядність коду на відлік до $i=8$ ($L_{кв}=256$), забезпечивши при цьому виконання вимог щодо захищеності від шумів квантування ($\eta \approx 40 дБ$).

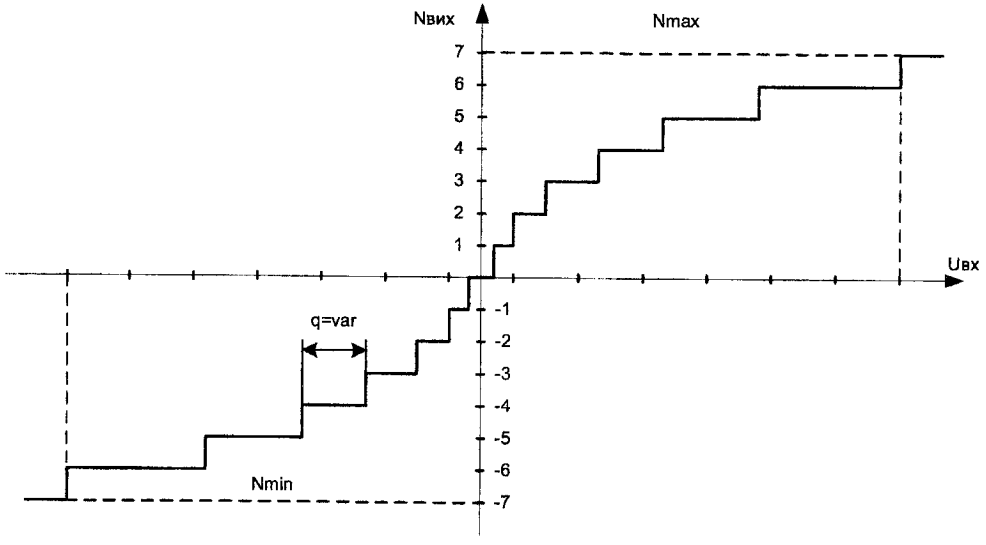



*Рис. 2.6. Амплітудна характеристика нерівномірного квантизатора*

Ефект нерівномірного квантування може бути отриманий за допомогою стискування динамічного діапазону сигналу з подальшим рівномірним квантуванням. Стискування динамічного діапазону сигналу здійснюється за допомогою ***компресора***, що має нелінійну амплітудну характеристику. Чим більшу нелінійність має компресор, тим більший виграш може бути отриманий для слабких сигналів.

Для відновлення початкового динамічного діапазону сигналу на прийомі необхідно встановити ***експандер*** (розширювач), амплітудна характеристика якого повинна бути зворотною до амплітудної характеристики компресора. Отже, результуюча (сумарна) амплітудна характеристика ланцюга ***комп***ресор-експ***андер*** (***компандер***), повинна бути лінійною, щоб уникнути нелінійних спотворень передаваних сигналів.

У цифровій телефонії застосовуються дві характеристики компандування:

– тип А (Європа);

– тип μ (Північна Америка).

У нормованому вигляді ($x = U_{ВХ}/U_m$, $y = U_{ВИХ}/U_m$) характеристики компресії описуються виразами:

$$y = F_A(x) = \begin{cases} sign(x)\cdot\left[A|x|/(1+\ln A)\right] & 0 \le |x| \le 1/A, \\ sign(x)\cdot\left[(1+\ln A|x|)/(1+\ln A)\right] & 1/A \le |x| \le 1 \end{cases}$$

$$y = F_\mu(x) = sign(x)\cdot\left[\ln(1+\mu|x|)/(1+\ln\mu)\right] \qquad -1 \le |x| \le 1,$$

де A=87,6 і $\mu = 255$ – параметри компресії.

Відповідні характеристики експансії мають вигляд:

$$x = F_A^{-1}(y) = \begin{cases} sign(y)\cdot\left[|y|\cdot(1+\ln A)/A\right] & 0 \le |y| \le 1/(1+\ln A) \\ sign(y)\cdot\left\{\left[\exp\{|y|\cdot(1+\ln A)-1\}/A\right\}\right. & 1/(1+\ln A) \le |y| \le 1 \end{cases},$$

$$x = F_\mu^{-1}(e) = sign(y)\cdot\frac{1}{\mu}\left[(1+\mu)^{|y|}-1\right] \qquad -1 \le |y| \le 1.$$

### 2.1.4. Диференціальна імпульсно-кодова модуляція

Між сусідніми відліками мовного сигналу існує значна кореляція, яка зі збільшенням інтервалу між відліками зменшується незначно. Це означає, що

мовний сигнал змінюється повільно, а різниця між сусідніми відліками матиме меншу дисперсію, ніж початковий сигнал. Коли такі сильно скорельовані вибірки закодувати у стандартній системі ІКМ, отриманий в результаті сигнал міститиме значну інформаційну надлишковість. Усунення цієї надлишковості, або компресія сигналу, можливе в системі різницевого кодування – так званої ***диференціальної імпульсно-кодової модуляції*** (***differential pulse-code modulation – DPCM***).

На рис. 2.7 показано схему для реалізації диференціальної імпульсно-кодової модуляції.

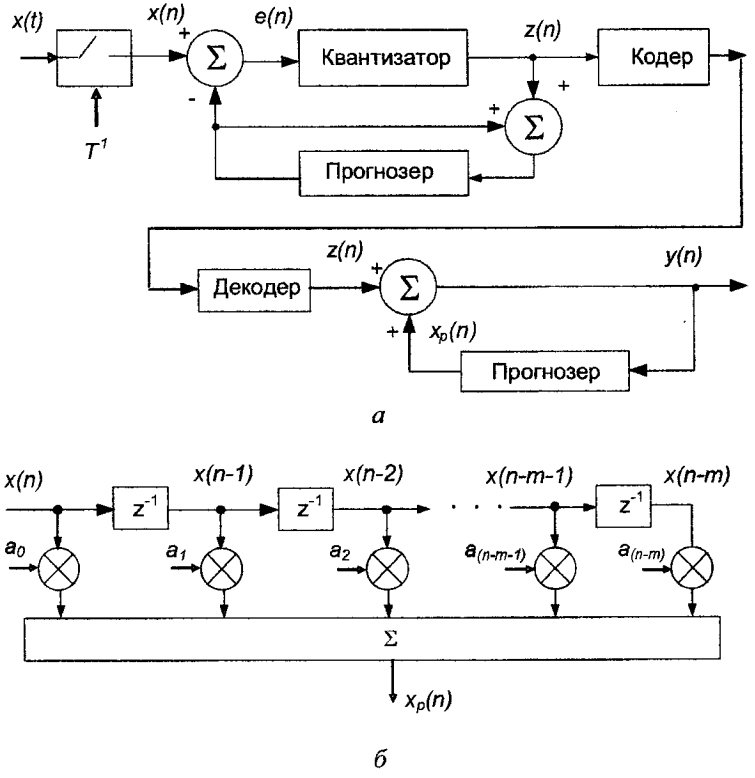



*Рис. 2.7. Схема диференціальної імпульсно-кодової модуляції (а) та варіант реалізації прогнозера у вигляді нерекурсивного фільтра (б)*

На вхід квантизатора надходить сигнал, що є різницею оригінального сигналу $x(n)$ і його прогнозованого значення $x_p(n)$, який, по суті, є помилкою прогнозу:

$$e(n) = x(n) - x_p(n). \tag{2.1}$$

На виході квантизатора одержують квантовану версію помилки прогнозу, яка зрештою і є сигналом DPCM-кодера:

$$z(n) = e(n) + \Delta(n), \tag{2.2}$$

де $\Delta(n)$ – похибка квантування.

Оскільки на вхід прогнозера подається сума прогнозованого значення сигналу $x_p(n)$ та квантованої версії помилки прогнозу $z(n)$:

$$y(n) = x_p(n) + z(n), \tag{2.3}$$

то, розв'язуючи рівняння (2.1), (2.2) і (2.3), можна встановити, що відтворений із алгоритму DPCM сигнал $y(n)$ відрізняється від оригінального сигналу $x(n)$ на похибку квантування:

$$y(n) = x(n) + \Delta(n).$$

За правильного прогнозу дисперсія помилки прогнозу $z(n)$ менша за дисперсію сигналу $x(n)$ так, що квантизатор із заданою кількістю рівнів може забезпечити помилку квантування із меншою дисперсією, ніж у випадку, коли вхідний сигнал $x(n)$ безпосередньо квантувати у стандартній системі ІКМ.

Подальшим розвитком систем різницевого квантування є ***адаптивна диференціальна імпульсно-кодова модуляція (Adaptive Differential Pulse Code Modulation – ADPCM)***. МСЕ-Т стандартизував цей вид модуляції у Рекомендаціях G.726 для швидкості передачі 32 кбіт/с.

## 2.2. Вокодери як спеціалізовані пристрої компресії сигналу мовлення

Основне призначення ***вокодера*** (від англ. словосполучення ***voice coder***) кодувати не сам мовний сигнал, а параметри, які його описують. Оскільки ці параметри змінюються значно повільніше, ніж сигнал, то для передачі інформації про ці параметри буде потрібен канал зв'язку з меншою пропускною

здатністю. Переважно вокодерні системи вимагають швидкостей передачі, менших за 16 кбіт/с.

Виділення і кодування параметрів мовних сигналів вимагає застосування складних алгоритмів цифрової обробки сигналів. Переважно для забезпечення меншої швидкості передачі потрібне застосування складніших алгоритмів, тобто продуктивніших процесорів. Якість передачі сигналу вокодерними системами залежить як від виду алгоритму, так і від використовуваної швидкості передачі.

Нижче описано три основні способи вокодерних перетворень: канальний, формантний та з лінійним передбачуванням.

### 2.2.1. Канальні вокодери

Перший канальний вокодер був розроблений у 1939 році Г. Дадлі. Структурну схему канального вокодера у класичному варіанті показано на рис. 2.8.

На передачі у вокодері за допомогою блока смугових фільтрів мовний сигнал розділяється на спектральні складові (частотні канали). Визначення відносних рівнів енергії у кожній частотній смузі здійснюється двонапівперіодним випрямленням і фільтрацією. У канал зв'язку передаються змультиплексовані дані, одержані аналого-цифровим перетворенням рівнів сигналів на кожній частотній смузі. Крім того, канальний вокодер на передачі визначає та передає у канал зв'язку категорію кодованого звука (дзвінкий чи глухий), а також частоту основного тону (для голосних і дзвінких приголосних звуків).

Оскільки на виділених частотних інтервалах сигнал змінюється дуже повільно, частота дискретизації АЦП є набагато нижчою, ніж 8 кГц, а бітрейт навіть змультиплексованого потоку виявиться значно нижчим від необхідних для передачі оцифрованого сигналу мовлення 64 кбіт/с. У цьому власне і криється ефект компресії телефонних повідомлень.

На прийомі вокодер реалізує функцію голосового тракту, синтезуючи на основі одержаних даних мовний сигнал. Демультексовані дані надходять на цифроаналогові перетворювачі відповідних частотних каналів для формування у вигляді напруг постійного струму поточних значень рівнів спектральних складових. Ці напруги подаються на інформаційні входи амплітудних модуляторів. На опорні входи усіх модуляторів як несуча використовується імпульсна послідовність із налаштовуваного генератора основного тону або

генератора шуму, залежно від інформації про категорію звука (дзвінкий чи глухий). Сигнали модуляторів проходять через смугові фільтри (аналогічні до смугових фільтрів на передачі) і об'єднуються між собою у вихідному суматорі, утворюючи синтезований мовний сигнал.

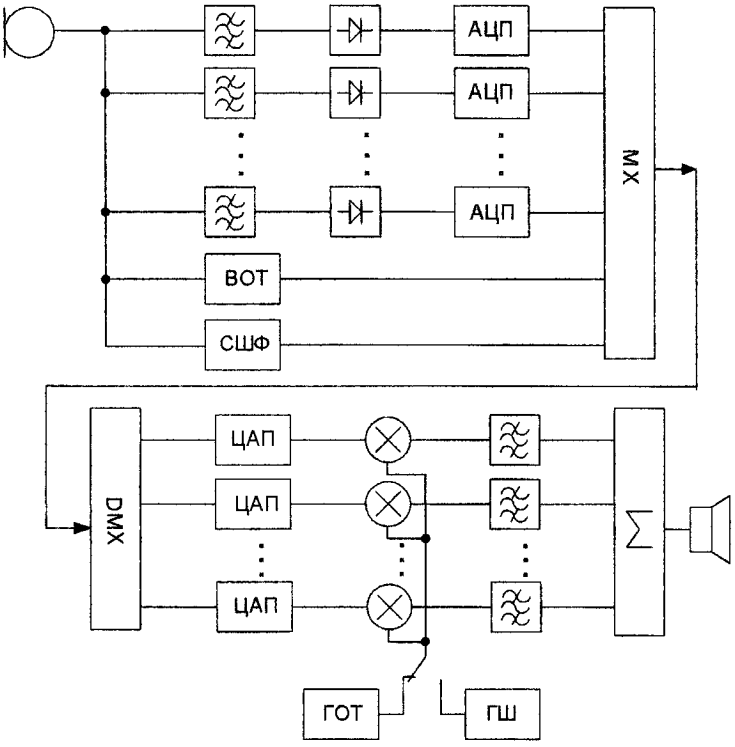



*Рис. 2.8. Структурна схема канального вокодера*

### 2.2.2. Формантні вокодери

Як зазначалося у розділі 2.1, форманти – це частоти у спектрі мовного сигналу, навколо яких спостерігається концентрація енергії сигналу (див. рис. 2.2, *б*). Формантний вокодер визначає розташування і рівень формант і передає цю інформацію в канал зв'язку замість огинаючої усього спектра. Оскільки кодуються лише найістотніші миттєві складові у спектрі мовного

сигналу, то ступінь стискання є вищим, ніж у канального вокодера. Формантний вокодер забезпечує цілком розбірливу мову за швидкості передачі навіть менше 1 кбіт/с. Найважливішою вимогою для одержання прийнятної мови є точне відстеження змін у формантах.

### 2.2.3. Вокодери з лінійним передбачуванням

Вокодер із ***лінійним передбачуванням*** (***LPC – linear predictive coding***) одержує інформацію про найістотніші параметри мови безпосередньо із часової форми сигналу, а не із його спектра, як канальний чи формантний вокодери. У LPC-вокодері (рис. 2.9) голосовий тракт людини моделюється цифровим рекурсивним фільтром із змінними параметрами, передатна функція якого містить лише полюси:

$$H(z) = \frac{1}{1 + \sum_{i=1}^{p} a_i z^{-i}}.$$

Сигнал збудження $e(n)$ є шумом або імпульсною послідовністю з періодом T, що визначає висоту основного тону. На інтервалах часу, що відповідають дзвінким (вокалізованим) звукам (а, д, н) перемикач знаходиться у верхній позиції, а під час передачі глухих звуків (с, ш, ф) – у нижній.

На вхід цифрового фільтра сигнал збудження передається із регульованим коефіцієнтом підсилення $G$, тому вихідний сигнал вокодера можна подати у вигляді різницевого рівняння:

$$y(n) = G \cdot e(n) - a_1 y(n-1) - a_2 y(n-2) - \ldots - a_p y(n-p).$$

Отже, вихідний сигнал у момент часу $n$ є лінійною комбінацією $p$ попередніх вибірок і поточної вибірки сигналу збудження.

Першим вокодером із лінійним передбачуванням був вокодер за алгоритмом LPC-10, стандартизований урядом США. За цим алгоритмом необхідні для синтезу мови параметри визначаються в аналізаторі на основі багатьох обчислень, які виконуються на 22,5 мс відтинку оригінального сигналу мови $x(n)$, що відповідає 180 відлікам за частоти дискретизації 8 кГц. Кодування у цьому випадку здійснюється 54 бітами, що відповідає швидкості передачі

2,4 кбіт/с. При цьому в канал зв'язку для синтезу мови передається набір таких параметрів:

- 41 бітом – значення десяти коефіцієнтів $a_1$, $a_2$, ... $a_{10}$ нерекурсивного фільтра;
- 5 бітами – коефіцієнт підсилення $G$;
- 1 бітом – вид звука (дзвінкий/глухий);
- 7 бітами – період основного тону для дзвінкого звука $T$.

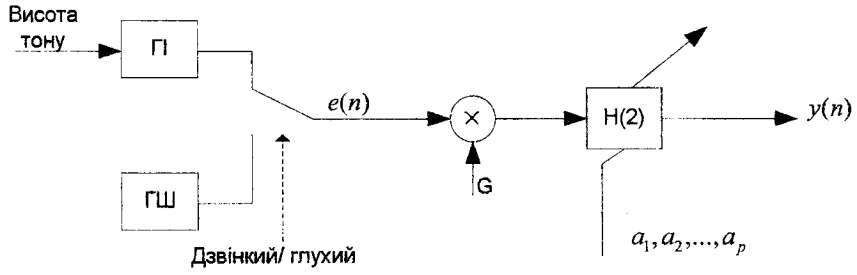



*Рис. 2.9. Модель голосового тракту у LPC-вокодері*

Дослідження показують, що вокодери із лінійним передбачуванням загалом забезпечують природніше звучання мови, ніж канальні вокодери. Для покращання якості відтворення мови швидкість передачі у LPC-вокодерах може збільшуватися до 4,8 кбіт/с. Проте сьогодні існує багато досконаліших алгоритмів кодування мови, наприклад, CELP, VSELP, MP-MLQ, які забезпечують високу якість синтезованої мови на швидкості передачі до 10 кбіт/с.

## 2.3. Цифрові системи передачі

***Цифрові методи передачі*** вперше були застосовані під час передачі телефонних розмов міжміськими сполучними лініями з використанням системи передачі та групоутворення типу Т з часовим (Time) поділом каналів. Економічна ефективність цих систем зумовлена обміном вартості застосування електроніки у термінальних пристроях цифрових систем передачі на вартість багатьох пар проводів у тракті. З кожним роком цей обмін стає все вигіднішим економічно.

### 2.3.1. Принципи часового групоутворення

Для спільного використання ліній зв'язку у цифрових системах передачі застосовується часове ущільнення (групоутворення), суть якого полягає у виділенні кожному абоненту часових проміжків (інтервалів), в межах яких здійснюється передача індивідуальних повідомлень. На відміну від частотного ущільнення аналогових систем передачі за часового ущільнення кожному абоненту доступна уся смуга частот системи передачі, але впродовж обмеженого проміжку часу.

На рис. 2.10 показано схему часового групоутворення сигналу ІКМ. На передачі під управлінням розподільника пристрої вибірки-зберігання здійснюють дискретизацію аналогових телефонних сигналів від кожного із абонентів *1÷K*. Оскільки сигналами розподільника є імпульсна послідовність з періодом $T = T_S / K$, то вибірки абонентів сусідніх каналів будуть зміщені стосовно себе на інтервал $T_S$. Далі АЦП здійснює квантування і кодування усіх вибірок так, що у підсумку на кожному часовому інтервалі $kT \quad (k = 1 \div K)$ каналом зв'язку передається оцифрований телефонний сигнал відповідних абонентів. Потік бітів від *1* до *K* каналів утворює цикл групового сигналу ІКТ. На прийомі із групового сигналу ІКМ під управлінням розподільника відбувається зворотна процедура виділення із групового сигналу ІКМ відповідних канальних цифрових сигналів, на основі яких ЦАП відновлюють аналоговий телефонний сигнал.

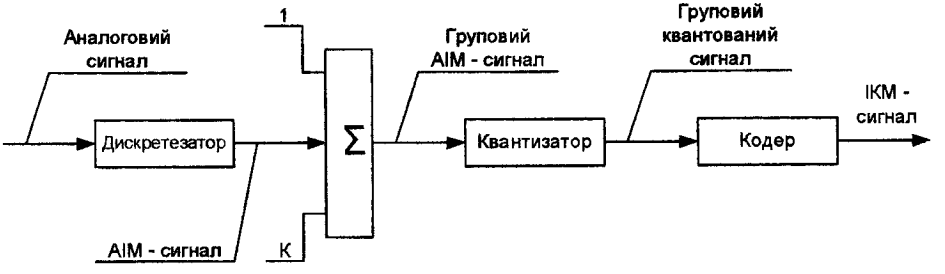



*Рис. 2.10. Схема часового групоутворення сигналу ІКМ*

Першою цифровою системою передачі була американська система Т1 з часовим поділом каналів, яка призначалася для забезпечення міжстанційного

зв'язку на з'єднувальних лініях місцевих телефонних мереж (на віддалях від 15 до 80 км). У системі налічується 24 часові канали для передачі телефонних повідомлень від 24 абонентів. Як відомо, період дискретизації телефонних сигналів становить $T_S = 125$ *мкс*, причому кожна вибірка репрезентується 8-ма бітами. Отже, у циклі налічується 24 × 8 = 192 інформаційні біти. У кожному циклі додається один додатковий біт для розмежування циклів, тому загальна кількість бітів у циклі каналу Т1 становить 193, а бітова швидкість:

$$C_{T1} = \frac{193}{125 \times 10^{-6}} = 1{,}544 \ \text{Мб/с}.$$

Як згодом виявилося, за прийнятного згасання телефонною парою можна передавати імпульси із дещо вищою швидкістю, тому МККТТ стандартизував міжнародну цифрову систему передачі Е1, яка має 32 часові канали. Отже, бітова швидкість в каналі Е1 становить

$$C_{E1} = \frac{32 \times 8}{125 \times 10^{-6}} = \frac{256}{125 \times 10^{-6}} = 2{,}048 \ \text{Мб/с}.$$

Зазначимо, що у каналі Е1 для передачі телефонних повідомлень використовуються лише 30 каналів (1÷15 і 17÷31), а решта два канали (0 і 16) – для синхронізації та сигналізації.

Каналоутворювальна апаратура часового розділення значно простіша, ніж апаратура частотного розділення, де для кожного індивідуального каналу потрібні відповідні індивідуальні смугові фільтри, які доволі важко реалізувати засобами мікроелектроніки.

Часове розділення широко використовують у цифрових системах передачі плезіохронної і синхронної ієрархій.

### 2.3.2. Ієрархія цифрових систем передачі

Структура первинної мережі зумовлює об'єднання і розділення потоків передаваної інформації, тому використовувані на ній системи передачі будуються за ***ієрархічним принципом***. Стосовно цифрових систем цей принцип полягає у тому, що кількість каналів ЦСП, що відповідає цьому ступеню ієрархії, перевищує кількість каналів ЦСП попереднього ступеня у ціле число разів. Аналогові системи передачі з частотним розподілом каналів також буду-

ються за ієрархічним принципом, але на відміну від ЦСП для них ступенями ієрархії є не самі системи передачі, а типові групи каналів.

Цифрова система передачі, що відповідає першому ступеню ієрархії, називається ***первинною***, оскільки об'єднує певну кількість первинних сигналів у первинний цифровий потік. ЦСП другого ступеня ієрархії об'єднують певну кількість первинних потоків у ***вторинний*** цифровий потік тощо.

У рекомендаціях МСЕ-Т представлено два типи ієрархій ЦСП: ***плезіохронна цифрова ієрархія (PDH)*** і ***синхронна цифрова ієрархія (SDH)***. Первинним сигналом для усіх типів ЦСП є первинний цифровий потік із швидкістю передачі 64 кбіт/с, який називається ***основним цифровим каналом (ОЦК)***. Для об'єднання сигналів ОЦК у групові високошвидкісні цифрові сигнали використовується принцип часового групоутворення.

Історично перша плезіохронна цифрова ієрархія має ***європейський, північноамериканський і японський*** різновиди (табл. 2.1).

*Таблиця 2.1*

**Параметри європейської, північноамериканської і японської систем PDH**

| Рівень ієрархії | Європа | | Північна Америка | | Японія | |
|---|---|---|---|---|---|---|
| | швидкість, Мбіт/с | коеф. мульти-плексації | швидкість, Мбіт/с | коеф. мульти-плексації | швидкість, Мбіт/с | коеф. мульти-плексації |
| 0 | 0,064 | - | 0,064 | - | 0,064 | - |
| 1 | 2,048 | 32 (30) | 1,544 | 24 | 1,544 | 24 |
| 2 | 8,448 | 4 | 6,312 | 4 | 6,312 | 4 |
| 3 | 34,368 | 4 | 44,736 | 7 | 32,064 | 5 |
| 4 | 139,264 | 4 | 274,176 | 6 | 97,728 | 3 |

Для цифрових потоків PDH застосовують відповідні позначення. Для північноамериканської і японської PDH застосовується позначення Т (інколи DS), для європейської PDH – Е. Цифрові потоки першого рівня позначаються відповідно Т1 і Е1, другого – Т2 і Е2 тощо.

Для вищих швидкостей передачі застосовується синхронна цифрова ієрархія. У стандарті SDH для мультиплексування використовуються так звані віртуальні контейнери, завдяки чому стає можливим безпосереднє введення

або виведення даних без потреби демультиплексування цілого потоку. У табл. 2.2 наведено ієрархію систем SDH.

*Таблиця 2.2*

**Ієрархія і параметри системи SDH**

| Позначення рівня швидкості | STM-1 | STM-4 | STM-16 | STM-64 | STM-256 |
|---|---|---|---|---|---|
| Швидкість, Мбіт/с | 155,520 | 622,080 | 2,488 | 9,953 | 39,810 |

## 2.4. Структура і функції цифрових систем комутації

***Системи комутації*** є одним із трьох елементів телекомунікаційної мережі – двома іншими є системи передачі та абонентські пристрої. Функцією комутаційної системи є встановлення і роз'єднання з'єднань між каналами передачі згідно з вимогами абонентів.

### 2.4.1. Часово-просторові комутаційні поля цифрових систем комутації

Ядром автоматичних телефонних станцій є комутаційне поле, де власне і відбувається з'єднання фізичних каналів телефонної мережі. Комутаційні поля за більше як сто років пройшли тривалий шлях розвитку – від електромеханічних декадно-крокових шукачів Стровгера, координатних з'єднувачів з механічними, а пізніше електронними контактами (рис. 2.11) до цифрових часово-просторових комутаційних полів.

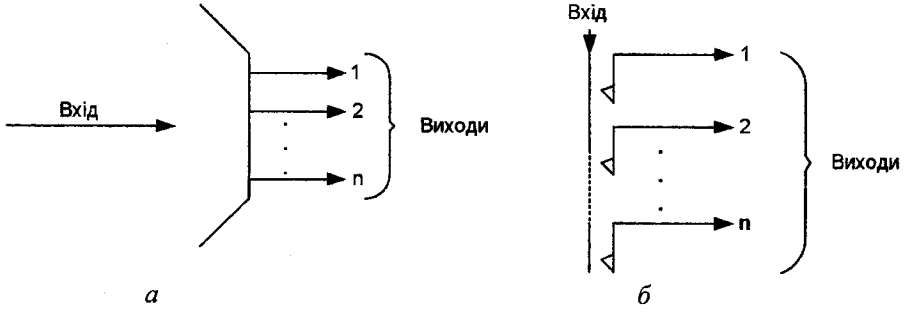



*Рис. 2.11. Схематичне зображення декадно-крокового шукача (а) та координатного з'єднувача (б)*

Часова комутація застосовується до сигналів із часовим ущільненням. Часовий комутатор здійснює перенесення сигналів із одного часового каналу (слоту – slot), наприклад, із 5-го у заданий інший, наприклад, в 27-й (рис. 2.12, *а*). Оскільки цифрові електронні пристрої на відміну від механічних контактних пристроїв є однонапрямними, а телефонний зв'язок є двонапрямним, то виконується подвійна комутація (рис. 2.12, *б*) – пряма (5-й канал із 27-м) і зворотна (27-й канал із 5-м).

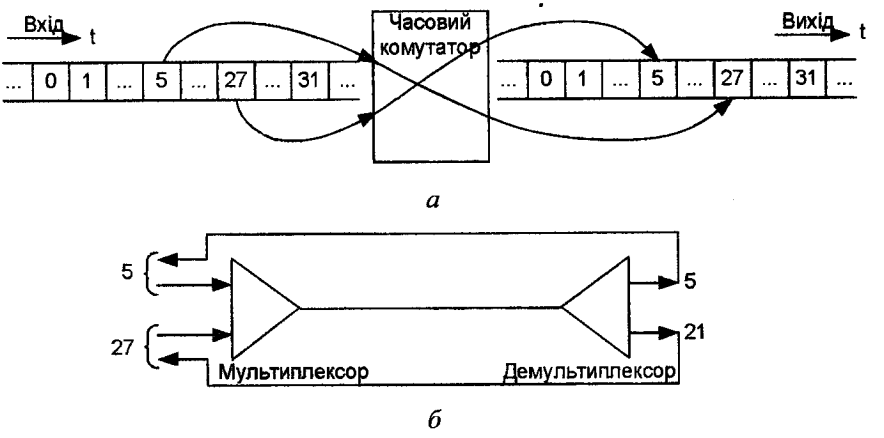



*Рис. 2.12. Принцип часової комутації: а – схематичне зображення; б – схема утворення двосторонньої комутації*

Часовий комутатор, по суті, лише здійснює переміщення інформації із певного часового каналу вхідного тракту ІКМ у адресно визначений часовий інтервал вихідного тракту. Але оскільки телефонне з'єднання у загальному випадку встановлюється між двома різними просторово рознесеними фізичними лініями і в різних часових каналах, то процес комутації вимагає перетворення одночасно як у просторі (просторова комутація), так і в часі (часова комутація). Просторова комутація реалізується за допомогою логічних схем вибіркового типу (мультиплексорів), а часова – запам'ятовування інформації у запам'ятовуючих пристроях. Варто зазначити, що на відміну від комутаційного обладнання у мережах із комутацією пакетів, наприклад, маршрутизаторів, час перебування інформації у часово-просторовому комутаторі

обмежений і не перевищує 125 мкс, тобто одного періоду дискретизації мовного сигналу.

На рис. 2.13 показано принцип роботи часово-просторового комутатора. Для зручності входи комутатора показані зліва, а виходи – справа. Оскільки усі тракти із часовим розподілом каналів є чотирипровідними, то кожному вхідному часовому каналу відповідає вихідний часовий канал вихідного тракту, що утворюють між собою пару. У такий спосіб двонаправлений телефонний зв'язок потребує також з'єднання у зворотному напрямі, тобто паралельно виконуються два пересилання інформації як у часі, так і в просторі.

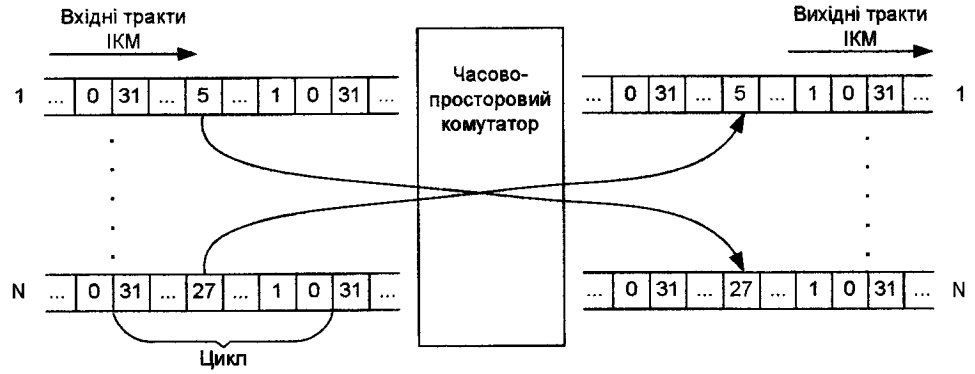



*Рис. 2.13. Принцип роботи часово-просторового комутатора*

На прикладі, показаному на рис. 2.13, у прямому з'єднанні це пересилання вибірки із п'ятого каналу першого тракту ІКМ до 27 каналу останнього тракту, а у зворотному, навпаки, – із 27 каналу останнього тракту до п'ятого каналу першого тракту. Слід зазначити, що кожен із вхідних і вихідних трактів з однаковими номерами асоціюється із певним просторовим розташуванням абонентів.

Часово-просторові комутатори є основою комутаційних модулів сучасних цифрових систем комутації (ЦСК), що прийшли на заміну АТС (див. п. 3.2.2). Операції часово-просторової комутації у ЦСК можна легко інтегрувати із операціями часового групоутворення, що застосовуються у цифрових системах передачі.

Рис. 2.14 ілюструє переваги інтегрування цих двох систем. Якщо раніше системи комутації (тобто АТС) та системи передачі були функціонально незалежні, а для взаємодії потребували каналоутворювальну апаратуру для об'єднання на передачі і поділу на прийомі часових каналів, то за інтеграції цифрових систем комутації із цифровими системами передачі відпадає потреба у каналоутворювальних пристроях.

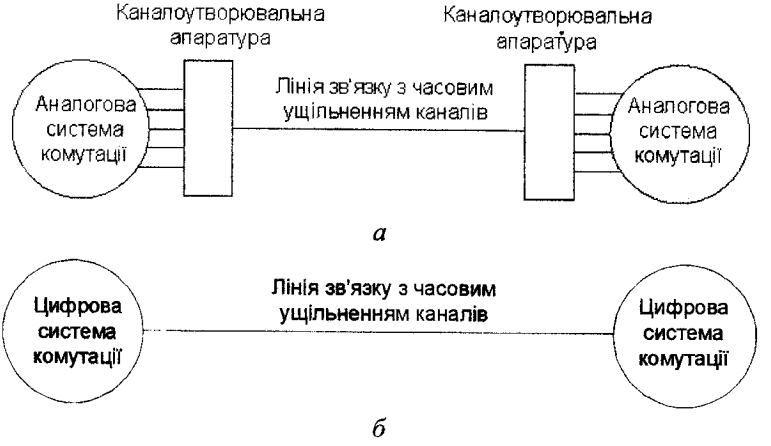



*Рис. 2.14. Інтеграція комутації й передачі: а – роздільна передача й комутація; б – інтегрована передача й комутація на основі часового поділу каналів*

Інтеграція функцій передачі й комутації дає змогу не лише заощадити на устаткуванні, але й значно підвищити якість передачі мови, виключаючи багаторазові аналого-цифрові й цифроаналогові перетворення. У цифрових телефонних мережах якість передачі мови під час міжміського зв'язку ідентична до якості передачі мови під час місцевого зв'язку в усіх відношеннях: з погляду перешкод, рівня сигналу, спотворень. Оскільки усі цифрові канали чотирипровідні, то явище еха виключається, якщо абонентські пристрої також підключені аналоговими або цифровими чотирипровідними лініями. Якщо ж у повністю цифровій мережі аналогові абонентські лінії виявляються двопровідними, то ехо виникає, але його можна зменшити узгодженням повних опорів дифсистем, що забезпечують перехід із двопровідних кіл на чотирипровідні.

### 2.4.2. Лінійні абонентські модулі цифрових систем комутації

***Лінійні абонентські модулі*** (Subsriber Line Interface Circuit – SLIC) виконують у телефонній мережі низку функцій, перелік яких відомий під абревіатурою ***BORSCHT***:

***B (Battery feed)*** – електроживлення;

***(Overload Protection)*** – захист від небезпечної напруги;

***R (Ringing)*** – посилка сигналів виклику;

***S (Supevision)*** – контроль за станом шлейфа;

***C (Coding)*** – кодування;

***H (Hybrid)*** – реалізація диференціальної системи;

***T (Test)*** – випробування абонентських ліній.

Схему абонентського модуля показано на рис. 2.15.

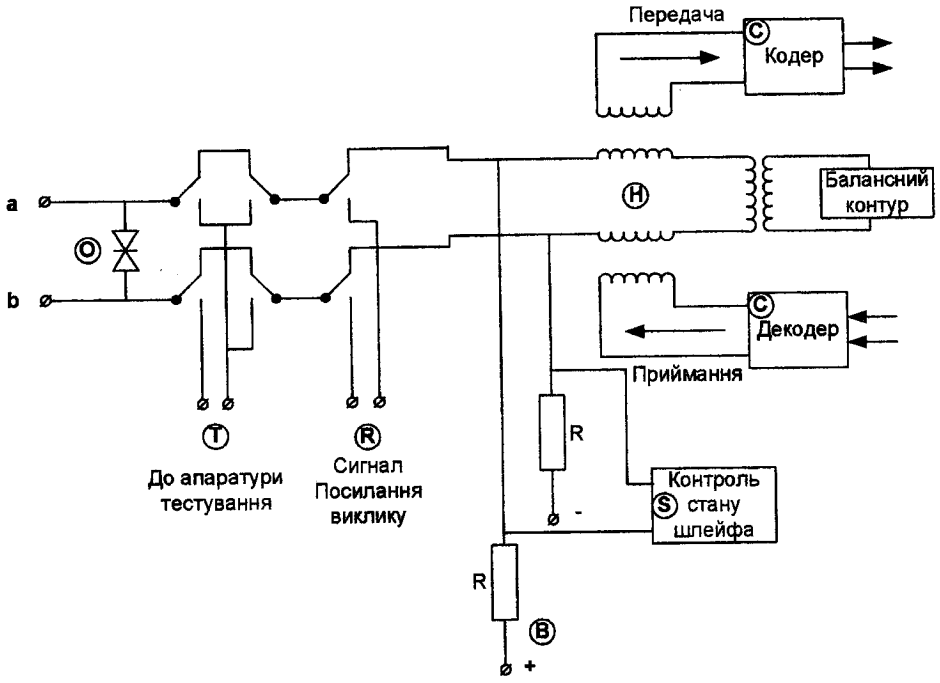



*Рис. 2.15. Схема абонентського модуля*

Живлення абонентського терміналу ***(функція B)*** здійснюється від станційної батареї номіналом в 60 В із заземленим позитивним полюсом. Струм у абонентській лінії обмежується опорами $R \approx 500$ *Ом* обмоток реле, які встановлені симетрично у кожному проводі лінії. Ці самі реле використовуються для контролю стану АТЛ ***(функція S)*** – замикання шлейфа призводить до спрацювання реле.

Захист від небезпечних напруг ***(функція O)*** виконується у двох точках – одна в кросі ЦСК, інша – в абонентському комплекті. За короткочасних перенапруг, наприклад, від розряду блискавки пристрої захисту на кросі ЦСК (т. зв. "антиблиски") спрацьовують "на пробій", замикаючи накоротко вхід абонентського модуля ЦСК. Натомість на боці абонента захист працює за принципом запобіжника, тобто "на розрив". Очевидно, що швидкодія пристроїв захисту має перевищувати швидкість розповсюдження сигналів у захищуваних колах.

Посилка сигналів виклику ***(функція R)*** полягає у надсиланні на тлі сталої складової у 60 В радіоімпульсів амплітудою 90 В, частотою заповнення – 25 Гц, тривалістю – 4 с і паузою – 1 с.

Оцифровування і відновлення мовного сигналу ***(функція C)*** здійснюється кодером на передачі і декодером – на прийомі. Перехід із двопровідної на чотирипровідну лінію і, навпаки ***(функція H)***, реалізується за допомогою диференційної системи. У сучасних пристроях диференційна система будується не на трансформаторних пристроях, а у вигляді електронних балансних схем.

Контроль абонентських ліній ***(функція T)*** передбачає під'єднання через реле спеціальної випробувальної апаратури у напрямку до АТЛ або до ЦСК. Така апаратура дає змогу контролювати параметри АТЛ або проводити випробування абонентського лінійного модуля, імітувати навантаження тощо.

Абонентські лінійні модулі на відміну від комутаційного чи адміністративного модуля є індивідуальним обладнанням ЦСК, а тому займають найбільший об'єм у складі ЦСК. Тому актуальними є роботи із його мініатюаризації.

## 2.5. Переваги і недоліки цифрової телефонії

Переваги цифрової телефонії визначаються такими властивостями:

1. Простота групоутворення – часове (а не частотне) ущільнення реалізується спільними і дешевими цифровими пристроями.

2. Простота сигналізації – цифрова природа усіх сигналів (як мовних, так і сигналізаційних).

3. Використання сучасних цифрових технологій до опрацювання і зберігання даних.

4. Інтеграція систем передачі й комутації (рис. 2.14).

5. Можливість роботи за малого співвідношення *сигнал-завада.*

6. Регенерація сигналу замість проміжного підсилення.

7. Можливість застосування до інших видів обслуговування.

8. Можливість контролю робочих характеристик.

9. Проста процедура засекречування інформації, поданої у цифровому вигляді.

До недоліків цифрової телефонії можна зарахувати:

1. Необхідність часової синхронізації блоків передавальної та приймальної частин телекомунікаційної системи.

2. Розширення смуги частот – аналогові повідомлення потребують менше ресурсів телекомунікаційної мережі (наприклад, передача неперервного телефонного повідомлення потребує смуги у 3100 Гц, натомість цифрового – в двадцятеро ширшої для цифрового потоку 64 кбіт/с).

3. Необхідність аналогово-цифрового й цифроаналогового перетворень на стику із аналоговими елементами і пристроями (наприклад, із аналоговою абонентською лінією).

4. Топологічні обмеження групоутворення.

5. Несумісність із існуючим аналоговим оточенням на стадії "цифровізації" телекомунікаційних мереж.

## Питання для самоконтролю:

**1.** Поясніть засади утворення акустичного сигналу мовлення артикуляційним апаратом людини.

**2.** Що таке основний тон і форманти сигналу мовлення?

**3.** Назвіть основні параметри телефонного сигналу. Яким є енергетичний спектр сигналу мовлення?

**4.** Які операції використовують під час формування сигналу імпульсно-кодової модуляції та зворотного відновлення аналогового телефонного сигналу?

**5.** Наведіть вирази, що описують процеси дискретизації та квантування сигналу мовлення.

**6.** Вкажіть на призначення та розкрийте зміст компандування сигналу. Який виграш дає застосування компандерів під час передачі телефонних повідомлень?

**7.** Наведіть схему та основні математичні співвідношення, які описують роботу кодера і декодера диференціальної імпульсно-кодової модуляції.

**8.** Поясніть принципи часового групоутворення сигналу імпульсно-кодової модуляції.

**9.** Що таке плезіохронна та синхронна цифрові ієрархії? Вкажіть сфери застосування цих систем.

**10.** Для чого використовуються вокодери? Опишіть схему та принцип дії канального вокодера.

**11.** Розкрийте принцип роботи формантних вокодерів та вокодерів із лінійним передбачуванням.

**12.** Опишіть структуру та засади функціонування часово-просторових комутаторів.

**13.** Які функції виконують лінійні абонентські модулі цифрових систем комутації?

**14.** Поясніть принципи інтеграції комутації та передачі у сучасних цифрових системах передачі.

**15.** Розкрийте переваги і недоліки цифрової телефонії.

# Розділ 3

# СТРУКТУРА ТА ФУНКЦІОНУВАННЯ ТЕЛЕФОННИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Телефонія в історичному аспекті є другим видом електрозв'язку і "молодша" за телеграфію на півстоліття. Але саме телефон, а не телеграф в корінний спосіб вплинув на розвиток і сучасний стан телекомунікаційної сфери, бо із розгалуженістю та розмірами телефонної мережі не може зрівнятися жодна інша мережа, зокрема й Інтернет.

Цей розділ вивчає будову та принципи роботи телефонної мережі загального користування (ТфМЗК, англ. Public Switched Telephone Network – PSTN), її місце у структурі сучасної телекомунікації. Розділ є завершальним у блоці цієї дисципліни, що ознайомлює із об'єктом захисту.

У результаті вивчення цього розділу студент повинен знати:

- призначення та будову первинних і вторинних мереж зв'язку і передусім телефонної мережі загального користування України;
- структуру міських і сільських телефонних мереж, основні підходи до їх цифровізації, особливості цифрових мереж з інтеграцією послуг, будову і функціональні можливості цифрових систем комутації;
- принципи функціонування міжміського та міжнародного телефонного зв'язку, системи нумерації на міжзоновому, зоновому та міжнародному рівнях;
- алгоритм встановлення з'єднання у телефонній мережі;
- види сигналів телефонної сигналізації та систему міжстанційної сигналізації із спільним каналом.

## 3.1. Телефонна мережа та її місце у сучасній телекомунікації

### 3.1.1. Первинні та вторинні мережі зв'язку

Сукупність технічних засобів телекомунікаційних мереж, які беруть участь у процесі передачі повідомлень незалежно від їх виду, утворюють ***первинну мережу зв'язку*** (ПМЗ). До складу ПМЗ входять мережеві вузли, мережеві станції і лінії зв'язку (рис. 3.1). Мережеві вузли (МВ) утворюються на

перетині кількох ліній зв'язку. На мережевих вузлах встановлюється каналоутворювальна апаратура систем передачі та виконується довготривала комутація групових каналів. Мережеві станції (МС) виконують ті самі функції, що і мережеві вузли, але додатково забезпечують під'єднання користувачів у вигляді обладнання вторинних мереж.

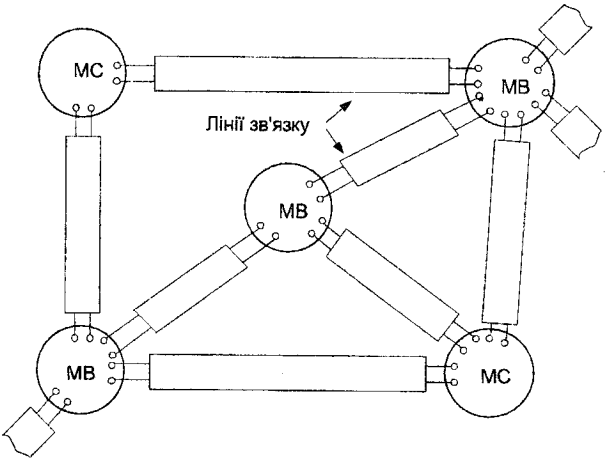



*Рис. 3.1. Первинна мережа електрозв'язку*

Структура ПМЗ будується із урахуванням адміністративного устрою країни. Так, територія України (як і колишнього СРСР) поділена на зони, які збігаються із адміністративними територіями областей. Відповідно до цього розподілу ПМЗ складається із мереж зонового та магістрального рівнів. Зонова ПМЗ охоплює територію зони, забезпечуючи з'єднання місцевих мереж усередині зони, а магістральна ПМЗ сполучає між собою зонові мережі.

На сучасному етапі провідні оператори зв'язку будують свої первинні мережі як трирівневі (рис. 3.2):

- внизу фізичний рівень (коаксіальний кабель, радіорелейні лінії чи оптоволоконний кабель із хвильовим розподілом каналів WDM);
- посередині технологія синхронної цифрової ієрархії SDH із широкосмуговою комутацією каналів (структуризація широкосмугових каналів за допомогою довготривалої гнучкої комутації);

- зверху технологія асинхронного режиму передачі ATM із комутацією комірок та механізмом QoS (для забезпечення ефективного використання пропускної здатності мереж).

Кожна мережа зв'язку, крім технічних засобів первинної мережі, використовує властиві лише цій мережі пристрої. Сукупність технічних засобів, що забезпечують передачу повідомлень ***певного виду***, утворює ***вторинну мережу зв'язку***. Трьома найбільшими вторинними мережами є телефонна мережа, телерадіомережа та комп'ютерні мережі (мережі передачі даних).

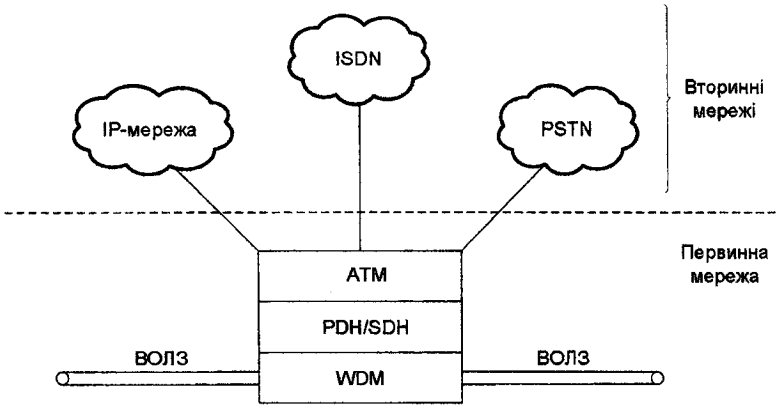



*Рис. 3.2. Трирівнева структура будови перспективних первинних мереж*

До складу вторинної мережі зв'язку належать термінальні абонентські пристрої, абонентські лінії, комутаційні пристрої і канали, виділені з первинної мережі зв'язку для організації цієї вторинної мережі.

### 3.1.2. Первинна мережа ВАТ "Укртелеком": стан і перспективи розвитку

ВАТ "Укртелеком" є національним оператором зв'язку України. Його первинна мережа зв'язку складається із магістральних і зонових ліній зв'язку. Магістральні лінії пов'язують обласні центри та інші великі міста і стикуються з міжнародними лініями. Зоновий рівень мережі забезпечує зв'язок у межах області і має вихід на магістральні лінії зв'язку.

Транспортна телекомунікаційна мережа ВАТ "Укртелекому" станом на 2009 р. складалася із 172967 км кабельних ліній зв'язку, зокрема волоконно-оптичних ліній зв'язку (ВОЛЗ) – 38143 км [13]. До складу Дирекції ПМЗ "Укртелекому" зараховано 12 центрів технічної експлуатації ПМЗ і 137 їх підрозділів, які рівномірно розподілені по усій території України.

***Магістральна мережа*** побудована на обладнанні SDH із швидкостями передачі 2,5 Гбіт/с *(STM-16)* і 622 Мбіт/с *(STM-4)*. Лініями зв'язку магістральної мережі є волоконно-оптичні лінії зв'язку, кабелі із металевими проводами, радіорелейні лінії і супутникові канали. Сьогодні волоконно-оптичним кабелем ємністю 18–24 оптичних волокон охоплені усі області України.

Довжина ліній зв'язку на звичайних кабелях – понад 31 тис. км. Довжина радіорелейних ліній становить понад 47 тис. км, з яких 40 % – цифрові. Крім того, Дирекція ПМЗ обслуговує 26 станцій супутникового зв'язку.

Побудовані міжнародні переходи на ВОЛЗ сусідніх країн – Росії (два), Білорусії, Польщі, Словенії, Угорщини, Румунії, Молдови. Експлуатуються підводні міжнародні переходи ВОЛЗ ***ITUR*** і ***BSFOCS***, які забезпечують високошвидкісний зв'язок з Італією, Туреччиною, Болгарією і Росією.

***Зонова мережа*** побудована на ВОЛЗ, кабелях із металевими проводами та радіорелейних лініях. Будівництво ВОЛЗ зонового зв'язку (обласний центр – район) відбувалось за рахунок відгалужень від магістральних ВОЛЗ. Волоконно-оптичні кабелі прокладені у райцентрах і містах обласного підпорядкування (в Україні є 530 таких міст).

На зоновій мережі експлуатуються близько 40 тис. км кабелів з металевими провідниками. Цифровізація зонової мережі проводиться прискореними темпами (понад 50 % каналів зонової мережі є цифровими). На зоновій мережі 3 % каналів організовані на радіорелейних лініях і усі вони цифрові.

Кожний обласний центр України отримав два підходи по 10 Гбіт/с, районні центри та виділені міста – по 1 Гбіт/с, причому більшість районних центрів також уже отримали по два підходи волоконно-оптичного кабелю [13].

Резервування трафіку на первинній мережі відбувається за допомогою об'ємних кілець, організованих на магістральному та зоновому рівнях. Станом на 2009 рік по волокну цифровізовано 99,6 % населених пунктів.

### 3.1.3. Телефонна мережа загального користування України

Сьогодні в Україні послуги телефонного зв'язку можуть надавати стаціонарні (традиційні) телефонні мережі (з комутацією каналів), мережі стільникового зв'язку та комп'ютерні мережі (з комутацією пакетів, наприклад, IP-телефонія).

За належністю розрізняють ***телефонні мережі загального користування*** (ТфМЗК) та відомчі мережі, які можуть з'єднуватися із ТфМЗК або можуть бути закритими. Телефонні мережі можуть надавати у користування абонентам ***комутовані*** (із щосекундною тарифікацією) і ***виділені*** (із орендною оплатою) канали.

За видами розрізняють ***міжнародний*** зв'язок, міжміський зв'язок (***зоновий та міжзоновий)***, а також місцевий ***(міський і сільський)*** зв'язок (рис. 3.3). Телефонні мережі можуть використовуватися не лише для передачі телефонних розмов, але і для інших видів повідомлень – телеграм, факсу, даних, зокрема й телеметричних.

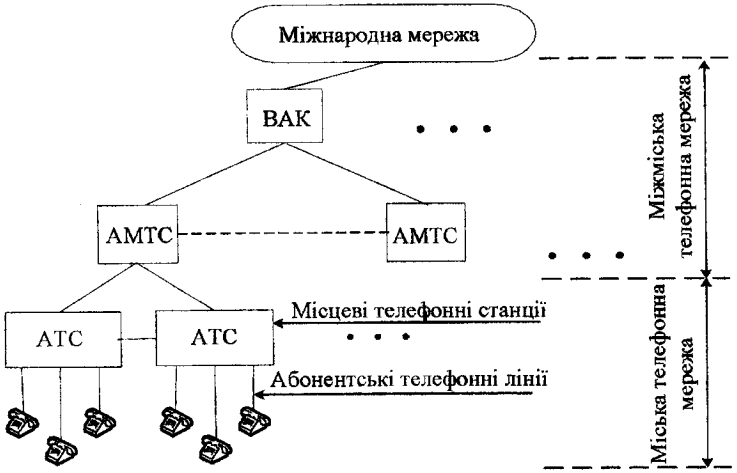



*Рис. 3.3. Ієрархія телефонної мережі*

Особливість ТфМЗК полягає у такому:

**1.** ТфМЗК є мережею із комутацією каналів, причому канали мережі є загальним ресурсом, що використовується усіма користувачами мережі.

**2.** На вимогу абонента у мережі створюється з'єднання у вигляді фізичного каналу із кінця в кінець, що складається з однієї або кількох ланок, сполучених послідовно у вузлах комутації.

**3.** Ланки з'єднання можуть утворюватися каналами тональної частоти (КТЧ) аналогових систем передачі з частотним розділенням каналів (FDM) або каналами цифрових систем передачі із часовим розділенням каналів (TDM).

**4.** Для створення каналу з кінця в кінець використовується обмін сигналізацією естафетним способом (від ланки до ланки).

**5.** Телефонні мережі надають користувачам тракт для передачі інформації із затримкою у 10–20 с, яка визначається часом набору номера абонента і встановлення з'єднання каналів на станціях та вузлах комутації; тривалість сеансу зв'язку залежить винятково від користувача.

**6.** Якість надання послуг ТфМЗК оцінюється часткою блокувань (втрат), які виникають унаслідок зайнятості ресурсів мережі або ж допустимим часом очікування.

**7.** Надання каналу "із кінця в кінець" ефективне не лише для передачі сигналів мовлення, але і для сформованих масивів великого обсягу (файлів), повідомлень факсиміле, цифрових відеосигналів.

Структура телефонної мережі істотно залежить від кількості абонентів і розмірів території. Під час проектування телефонних мереж вибирається одна з чотирьох топологій (рис. 3.4): радіальна (а), радіально-вузлова (б), повнозв'язна (в) за принципом кожний з кожним, змішана (г), що є поєднанням радіально-вузлової і повнозв'язної.

Телефонні мережі України перебувають на стадії цифровізації, для якої характерним є таке:

– переважно цифровізований за допомогою цифрових систем передачі міжстанційний зв'язок;

– більшість місцевих телефонних мереж належать до змішаного типу аналогово-цифрових.

Наприклад, у 2005 р. коефіцієнт цифровізації місцевих телефонних мереж становив приблизно 50 %, отже, подальша їх цифровізація залишається актуальним завданням найближчих років. Складність процесу цифровізації зумовлена величезною розбудованістю телефонних мереж, залежністю від концентрації абонентів на теренах населених пунктів, а також проведенням модернізації мереж в умовах неперервної їх експлуатації.

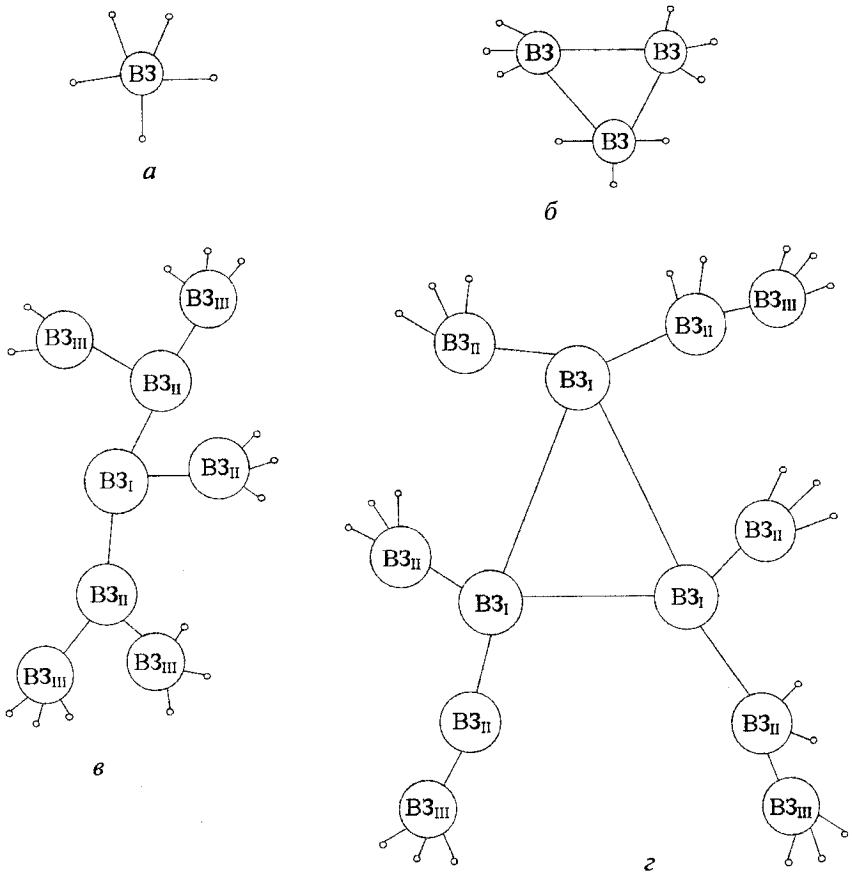



*Рис. 3.4. Типові топології телефонних мереж*

## 3.2. Місцеві телефонні мережі загального користування

***Місцевий телефонний зв'язок*** – це послуга, яка забезпечує доступ до телекомунікаційної мережі ВАТ "Укртелеком", та надає користувачу можливість спілкуватись з особами, які знаходяться у тому самому місті (районі, області). Послугами місцевого зв'язку можна користуватись з телефону (домашнього чи офісного), з таксофонів, з автоматизованих переговорних пунктів.

В усіх обласних центрах та більшості великих міст України налагоджений почасовий облік місцевих розмов. Відлік тривалості місцевої телефонної розмови починається з моменту відповіді будь-якої особи або абонентського пристрою (факсимільний апарат, автовідповідач, автоматичний визначник номера, модем тощо) і закінчується в момент розриву з'єднання. Одиницею вимірювання часу з'єднання є 1 секунда. Місячний обсяг користування послугами місцевого телефонного зв'язку визначається як сума тривалості усіх місцевих розмов, здійснених упродовж місяця з телефону абонента.

### 3.2.1. Структура міських та сільських телефонних мереж

Структура ***міської телефонної мережі*** (МТМ) залежить від її місткості, форми території та інших чинників. Структура нецифровізованих телефонних мереж істотно залежала від їх місткості (кількості телефонних апаратів абонентів і таксофонів).

Якщо місткість мережі не перевищувала 10000, будувалася так звана нерайонована мережа із радіальною топологією (рис. 3.5, *а*), оскільки усі абоненти за допомогою абонентських ліній під'єднувалися до єдиної АТС.

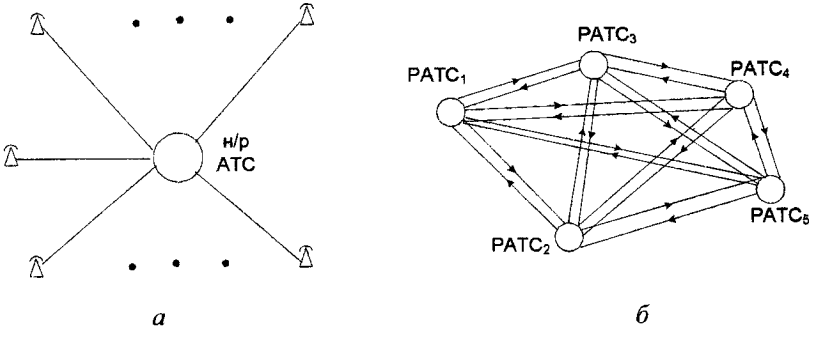



*Рис. 3.5. Структура нерайонованої (а) і районованої (б) телефонних мереж*

Коли кількість абонентів перевищувала 10000, то радіальний спосіб побудови мережі ставав неекономічним через зростання затрат на прокладання і утримування абонентських ліній (АЛ). Для зменшення затрат територію міста поділяли на райони, в кожному із яких встановлювали районну АТС (РАТС)

ємністю близько 10000 абонентів, причому усі РАТС з'єднувалися між собою за повнозв'язною топологією пучками фізичних ліній або каналами систем передачі (рис. 3.5, *б*). Довжина абонентських ліній при цьому істотно зменшувалася порівняно із варіантом нерайонованої мережі. Нумерація абонентів такої мережі – п'ятизначна, причому перша цифра визначає номер РАТС. Оскільки перші цифри 0 і 8 зарезервовані відповідно для спеціальних служб та міжміського зв'язку, то телефонна мережа могла бути поділена на 8 районів, а максимальна кількість номерів за п'ятизначної нумерації мала становити 80000. Проте коли кількість абонентів перевищує 40–50 тис., зростає кількість міжстанційних з'єднувальних ліній (ЗЛ), пропускна здатність яких недовикористовувалася.

Для кращого використання міжстанційних ЗЛ вводять так звані вузли вхідних повідомлень (ВВхП), що здійснювали ущільнення ліній на основі технології FDM або TDM. Такий варіант побудови телефонної мережі передбачає поділ території міста на вузлові райони, у кожному із яких розміщувалися до десяти АТС ємністю близько 10000 номерів. У кожному вузловому районі встановлюється ВВхП, який з'єднаний вихідними лініями з усіма АТС свого району, та вхідними лініями з усіма АТС інших вузлових районів. У кожному вузловому районі встановлюється ВВхП, який радіально з'єднаний вихідними лініями з усіма АТС свого району та вхідними лініями з усіма АТС інших вузлових районів (рис. 3.6). У межах кожного вузлового району АТС з'єднувалися каналами за способом "кожний з кожним".

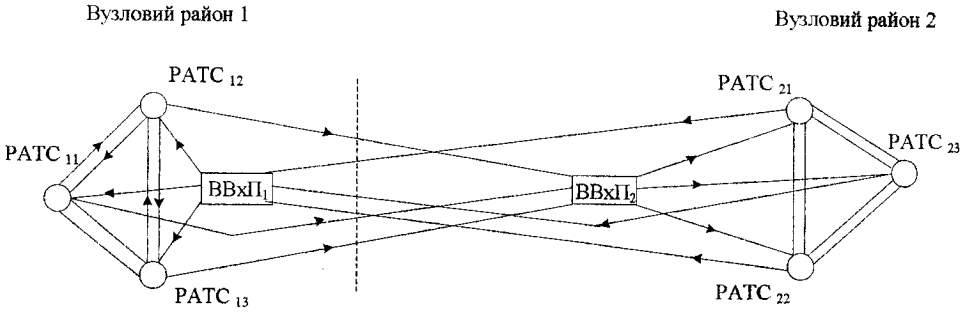



*Рис. 3.6. Структура телефонної мережі із вузлами вхідних повідомлень*

Такий варіант побудови телефонної мережі передбачає використання шестизначної нумерації, причому перша цифра номера визначає номер вузлового району, а друга – номер АТС. Враховуючи обмеження на використання 0 і 8 на позиції першої цифри у номері, можна будувати до 8 вузлових районів і до 10 АТС – у кожному такому районі.

За місткості телефонної мережі понад 400–500 тис. номерів кількість пучків з'єднувальних ліній на мережі з ВВхП стає дуже великою (відповідно 40–50 вхідних ЗЛ від кожної АТС інших вузлових районів). Щоб покращати використання з'єднувальних ліній збільшенням пучків, доводилось ще більше ускладнювати структуру телефонної мережі, вводячи на вузлових пунктах на додаток до вузлів вхідних повідомлень новий тип вузлів – вузли вихідних повідомлень (ВВихП). Такий вузол концентрував інформаційні потоки від усіх АТС свого вузлового району і розподіляв їх по ущільнених ЗЛ до ВВхП усіх інших районів. Зв'язки між АТС одного вузлового району можуть утворюватися за повнозв'язною топологією або через ВВхП і ВВихП (рис. 3.7). Нумерація абонентів на такій мережі – семизначна, причому перші дві цифри є індексом вузлового району, а третя – індексом АТС у вузловому районі.

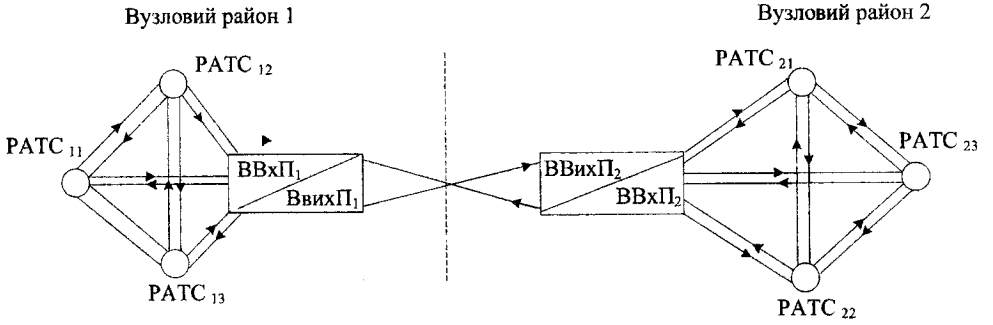



*Рис. 3.7. Структура телефонної мережі із вузлами вхідних і вихідних повідомлень*

В Україні досі існують мережі великих міст зі складною структурою. Територію міста поділяють на телефонні райони, що збігаються або не збігаються з його адміністративним поділом.

Подальше зниження затрат на побудову і експлуатацію МТМ пов'язано із покращанням використання абонентських та магістральних ліній та використанням замість квазіелектронних чи електронних АТС цифрових систем комутації.

Сільські телефонні мережі (СТМ) будують за радіальним або за радіально-вузловим способом із одним вузлом першого класу ВСІ (центральна АТС сільського району області) і кількома вузлами другого ВСІІ і, можливо, третього ВСІІІ класу (рис. 3.8).

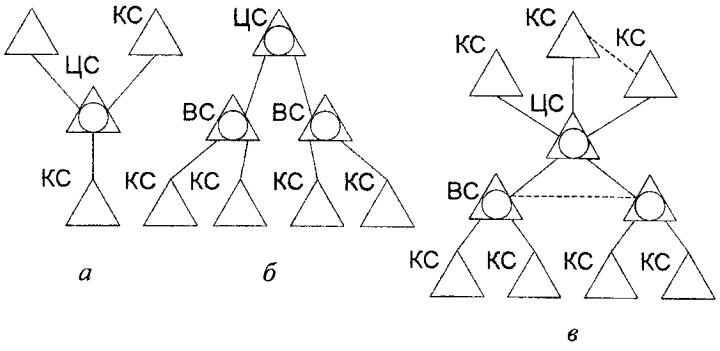



*Рис. 3.8. Схеми побудови сільських телефонних мереж: а – одноступенева; б – двоступенева; в – комбінована*

### 3.2.2. Перехід від аналогових телефонних мереж до цифрових

Перетворення аналогових вторинних мереж у цифрові – актуальне завдання для ТфМЗК України. Можливі різні шляхи переходу від аналогових мереж до цифрових. Для великих мереж цей перехід можна реалізувати у кілька етапів:

– заміна усіх аналогових міжстанційних ліній цифровими;

– заміна аналогових телефонних станцій і вузлів цифровими системами комутації (ЦСК);

– побудова цифрової мережі з інтегрованими послугами (Integrated Service Digital Network – ISDN).

ISDN – цифрова мережа, що забезпечує цифрові з'єднання між кінцевим обладнанням для підтримки широкого спектра таких телекомунікаційних

послуг (мовних та інформаційних). Мережа ISDN поєднує у собі можливості як звичайної телефонної мережі, так і мережі передачі даних. У мережі ISDN за наявності відповідного термінального обладнання усі послуги надаються з вищою надійністю і якістю завдяки захищеності від електричних перешкод.

Може бути запропонована й інша стратегія переходу – створення так званої накладеної цифрової мережі (рис. 3.9). Такий шлях дає змогу мінімізувати одноразові затрати, оскільки на момент введення перших мереж ISDN можливе створення повністю цифрової ділянки мережі, у межах якої інформація від абонента до абонента може передаватися у цифровій формі. Користувачі накладеної мережі відразу одержують сучасні послуги цифрових мереж. Окрім того, частину послуг цифрової мережі зможуть одержувати і абоненти аналогової мережі завдяки спеціально організованому доступу до ресурсів накладеної мережі.

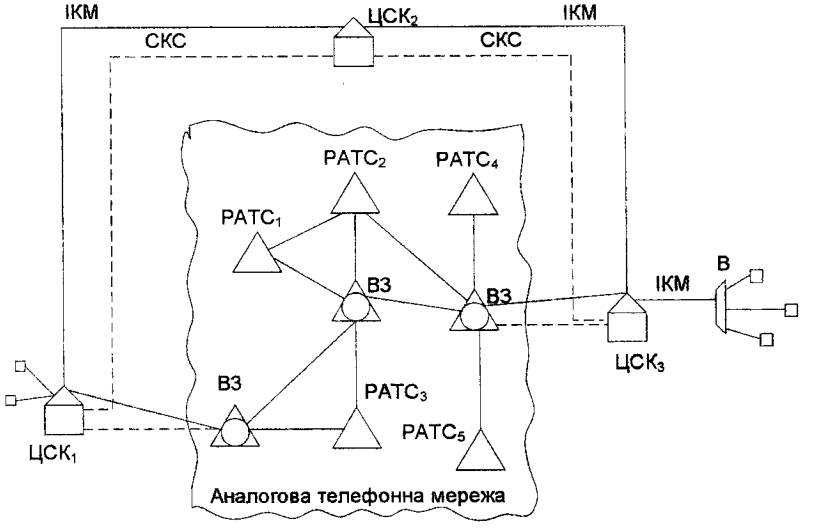



*Рис. 3.9. Структура змішаної аналогово-цифрової мережі*

Є ще одна перевага такої стратегії, яка полягає у тому, що раціонально вибрана ділянка для побудови накладеної мережі дає змогу прокласти певну кількість маршрутів міжстанційного зв'язку через мережу. Це відразу позна-

читься на підвищенні якості надаваних послуг завдяки використанню протяжних маршрутів лише із цифровими каналами. Для цифрової мережі природною є централізована міжстанційна сигналізація спільним каналом сигналізації (СКС).

Застосування централізованої сигналізації дає змогу істотно підвищити достовірність передачі сигнальної інформації (адресної, лінійних та інформаційних сигналів). Віддалені групи користувачів можуть бути економічно включені у цифрові системи комутації за допомогою виносів (В), які є частиною програмно-апаратних засобів цих ЦСК, наближених до місць групування користувачів. Функціонально виноси цифрової мережі відрізняються від підстанцій аналогової мережі здатністю замикати внутрішні потоки інформації без займання каналів, що пов'язують виноси з ЦСК. Ці канали використовуються тільки для зовнішнього зв'язку (вхідних і вихідних повідомлень) користувачів виносів.

На рис. 3.10 показано узагальнену структурну схему цифрової системи комутації 5ESS фірми AT&T (США).

Ядром цифрової системи комутації є комутаційні модулі (SM – Switching Module), які здійснюють комутацію часових каналів абонентів телефонної мережі. Окремі комутаційні модулі можуть виконувати функції районних АТС і розташовуються у відповідних районах міста як виносний варіант (RSM – Remote Switching Module). Усі комутаційні модулі SM і RSM з'єднуються між собою за допомогою комунікаційного модуля (CM – Communication Module). Абоненти телефонної мережі одержують доступ до ЦСК через аналогові (ААЛ) чи цифрові (ЦАЛ) абонентські лінії. Роль абонентського інерфейсу виконує лінійний модуль інтегрованих послуг (ILSU – Integrated Services Line Unit). До одного такого модуля можна підключати близько 2048 ААЛ та до 1024 – ЦАЛ. Задля наближення до абонентів і економії на протяжності абонентських ліній організовуються так звані виноси у вигляді віддалених комутаційних модулів RSM або віддалених лінійних модулів (RILSU – Remote Integrated Services Line Unit). Управління усіма компонентами СК здійснюється із одного пункту за допомогою адміністративного модуля (AM – Administrative Module). Для з'єднання із існуючими аналоговими АТС чи іншими ЦСК слугують аналогові (АЗЛ) і цифрові (ЦЗЛ) з'єднувальні лінії відповідно.

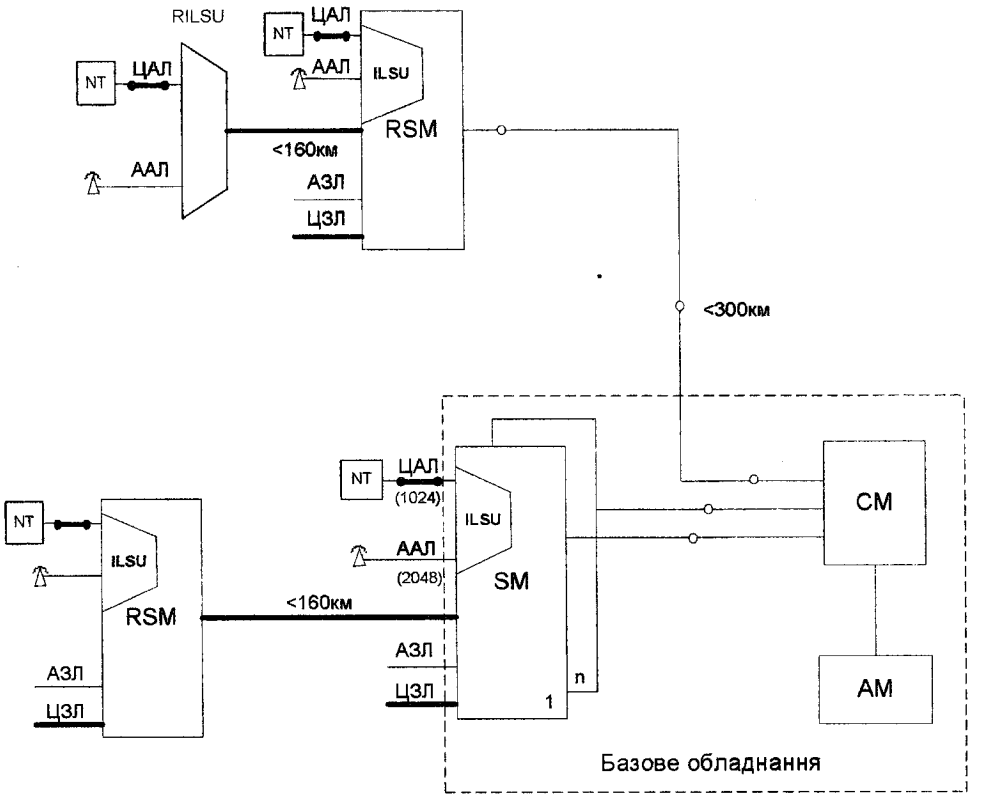



*Рис. 3.10. Структурна схема цифрової системи комутації 5ESS*

У максимальній комплектації ЦСК 5ESS дає змогу обслуговувати 750 тисяч абонентів. За потреби частина модулів ЦСК може виконувати функції АМТС.

Абонентам цифрових телефонних станцій ВАТ "Укртелеком" пропонує широкий вибір додаткових послуг, які підвищують функціональність телефону. Використовуючи одну цифрову абонентську лінію, можна телефонізувати невеликий офіс або реалізувати у себе вдома ще один телефон.

### 3.2.3. Особливості цифрових мереж з інтеграцією послуг

Цифровою називають мережу, в якій інформація передається між абонентними пунктами користувачів тільки у цифровій формі. Структура цифрової мережі може бути істотно спрощена порівняно із структурою аналогової вторинної телефонної мережі. Це пов'язано насамперед з тим, що немає таких жорстких обмежень максимальної місткості ЦК (кількості портів – абонентських і сполучних ліній), які існують для аналогових крайових станцій і вузлів. Тому для побудови цифрової мережі заданої місткості потрібна ***менша кількість станцій***, ніж для побудови аналогової мережі. Ще одна важлива відмінність цифрової мережі від аналогової – практична ***відсутність обмежень на відстань між станціями*** і вузлами завдяки застосуванню систем передачі з ІКМ. Ці особливості дають змогу будувати цифрову міську або відомчу вторинну мережу як ***однорівневу (тобто без вузлів)***. Станції такої мережі можуть бути пов'язані одна з одною способом ***"кожна з кожною"*** лініями з ІКМ (рис. 3.10). Ці станції можуть використовуватися ***як крайові або як суміщені (крайові та транзитні)***.

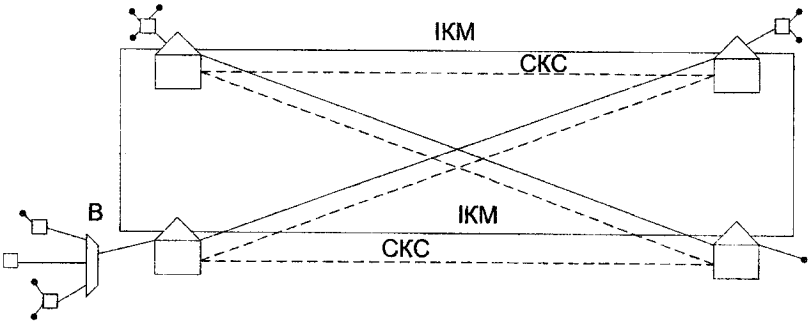



*Рис. 3.11. Однорівнева структура цифрової вторинної мережі*

З метою обміну сигнальними повідомленнями під час міжстанційного зв'язку у цифровій мережі виділяють сигнальну підмережу з комутацією пакетів. Ця підмережа утворена пунктами сигналізації (ПС) і пов'язуючими їх СКС. Сигнальні повідомлення у цій підмережі передаються у формі пакетів змінної довжини з високою швидкістю і достовірністю. У сигнальній підмережі, що є ефективним транспортним засобом, передаються не тільки

сигнальні повідомлення традиційних користувачів, але і команди управління мережею, а також дані для адміністрування.

Мережа з описаними властивостями може підтримувати безліч служб – таких, як телефонну, передачі даних, зображень, – і її прийнято називати цифровою мережею інтегрального обслуговування. Станції цифрової мережі, реалізовуючи функції абонентських і транзитних, можуть мати місткість близько 60 тис. портів і більше. У цифровій мережі винятково широко використовуються виноси (концентратори) частини устаткування крайових станцій, оскільки це дає змогу знизити витрати на абонентну мережу, яка називається мережею доступу (мережею доступу користувачів до ресурсів цифрової мережі).

## 3.3. Міжміський та міжнародний телефонний зв'язок

Міжміський телефонний зв'язок – це послуга, яка забезпечує користувачу можливість спілкуватись з особами, які знаходяться в інших областях України чи районах області, а також з абонентами мереж мобільних операторів.

Міжнародний телефонний зв'язок забезпечує можливість розмовляти по телефону з особами, які знаходяться в інших країнах. ВАТ "Укртелеком" надає послуги міжнародного телефонного зв'язку з користувачами як фіксованих телефонних мереж, так і мобільних мереж зарубіжжя.

Вартість розмови (з'єднання) визначається її тривалістю та тарифом. Тариф залежить від виду з'єднання (у межах області, у межах України, до мереж операторів мобільного зв'язку, міжнародної тарифної зони, до якої належить та чи інша країна), дня тижня та періоду доби. Послуги міжміського зв'язку оплачуються за тарифами, встановленими ВАТ "Укртелеком". Відлік тривалості розмови починається з моменту відповіді абонента, якого викликають, або абонентського пристрою (факсимільний апарат, автовідповідач, автоматичний визначник номера, модем тощо) і закінчується у момент розриву з'єднання. Одиниця вимірювання часу з'єднання – 1 секунда.

### 3.3.1. Зонові та міжзонові телефонні мережі

Територія України розбита на 25 зон семизначної нумерації, які збігаються із адміністративними межами областей. Семизначна нумерація дає можливість розмістити у зоні близько 8 мільйонів абонентів.

На території кожної зони встановлюється одна чи кілька АМТС, причому одна АМТС є в обласному центрі, а решта – у великих містах області (рис. 3.11). До зонової мережі належать внутрішньозонова телефонна мережа та місцеві (міські й сільські) мережі цієї області.

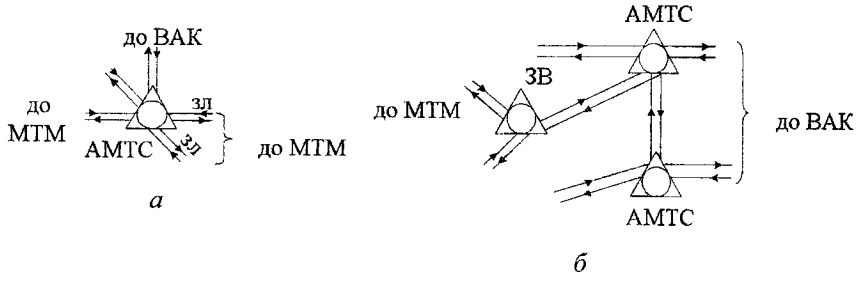



*Рис. 3.12. Принцип побудови міжміських телефонних мереж: а – з однією АМТС; б – з двома АМТС і зоновими вузлами*

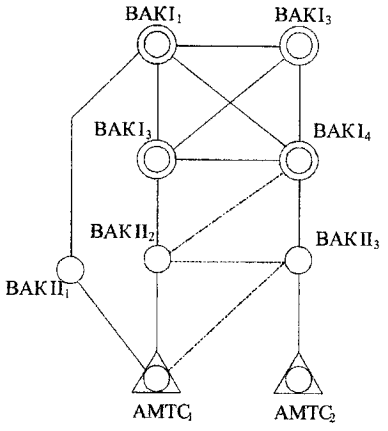



*Рис. 3.13. Ієрархічна структура міжміської телефонної мережі*

Внутрішньозонова телефонна мережа складається із АМТС зони, що входить одночасно у міжміську мережу, та з'єднувальних ліній і каналів систем передачі між АМТС, МТМ і СТМ цієї зони. За значного навантаження між

окремими місцевими мережами зони створюються зонові вузли (ЗВ), через які місцеві мережі з'єднуються між собою та АМТС.

Кожна місцева мережа з'єднується із найближчою АМТС зони або ЗВ вхідними і вихідними лініями.

Для зв'язку АМТС між собою слугує міжміська телефонна мережа. Прикінцевими міжміськими телефонними станціями є АМТС зонової мережі. Для з'єднання між собою передбачені вузли автоматичної комутації (ВАК), які не використовуються як прикінцеві (рис. 3.12).

Є два різновиди систем нумерації – ***закритий і відкритий.*** Якщо в мережі використовується закрита система нумерації, то з будь-якого пункту необхідний абонент викликається набором однієї і тієї самої кількості знаків. Для відкритої системи нумерації ця умова не виконується. На міжміській мережі України та країн СНД використовується відкрита система нумерації, а на міських телефонних мережах – закрита.

### 3.3.2. Системи нумерації у телефонних мережах

Уся територія України та інших країн СНД розділена на зони семизначної нумерації. Семизначний номер абонента всередині зони складається з двох складових: двозначного внутрішньозонового коду (ab) і п'ятизначного номера абонента місцевої мережі (xxxxx). Повний внутрішньозоновий номер має вигляд – abxxxxx. Раніше внутрішньозоновий номер (a) міг починатися із будь-якої цифри, окрім 0 і 8. З нуля починалися номери служб спеціального призначення у місцевій мережі, а цифра 8 була префіксом (індексом) міжміського зв'язку. Жодних обмежень у застосуванні десяткових знаків для (b) і (xxxxx) не було. Такі обмеження у використовуванні цифр для першого знака (a) внутрішньозонового номера дають можливість мати у зоні нумерації не більше 8 млн. абонентів.

Кількість зон на території колишнього СРСР перевищувала 100, тому кожній зоні присвоювався тризначний міжміський код ABC. Абонент місцевої мережі, який хотів викликати абонента іншої зони, набирав 11 знаків: 8ABCabxxxxx. Наприклад, щоб зателефонувати до Москви, потрібно було набрати:

8-095-abxxxxx,

де 8 – індекс міжміського зв'язку;

095 – код Москви;

abxxxxx – номер абонента.

Аналогічно виконувалися телефонні з'єднання між абонентами різних зон у межах України. Наприклад, щоб зателефонувати до Києва, місцева телефонна мережа якого семизначна, набирали:

8-044-abxxxxx,

де 8 – індекс міжміського зв'язку;

044 – код Києва;

abxxxxx – номер абонента.

Отже, раніше не існувало жодної різниці в алгоритмі набору міжзонових з'єднань у країнах СНД та Україні.

З 14 жовтня 2009 року змінився порядок набору міжміських та міжнародних напрямків. Щоб вийти на міжміську телефонну мережу, потрібно замість міжміського префікса "8" набрати префікс "0". Для виходу на міжнародну телефонну мережу замість міжнародного префікса "8-10" – префікс "0-0". Крім того, код зони змінено із тризначного на двозначний (без першої цифри "0" в існуючому коді), як наведено у табл. 3.1.

*Таблиця 3.1*

**Таблиця кодів зон телефонної мережі загального користування України до та після 14 жовтня 2009 року**

| Назва зони | Старий код | Новий код |
|---|---|---|
| 1 | 2 | 3 |
| Закарпатська | 031 | 31 |
| Львівська | 032 | 32 |
| Волинська | 033 | 33 |
| Івано-Франківська | 034 | 34 |
| Тернопільська | 035 | 35 |
| Рівненська | 036 | 36 |
| Чернівецька | 037 | 37 |
| Хмельницька | 038 | 38 |
| Житомирська | 041 | 41 |

*Продовження табл. 3.1*

| 1 | 2 | 3 |
|---|---|---|
| Вінницька | 043 | 43 |
| Київ (столиця) | 044 | 44 |
| Київська* (область) | 044 | 45 |
| Чернігівська | 046 | 46 |
| Черкаська | 047 | 47 |
| Одеська | 048 | 48 |
| Миколаївська | 051 | 51 |
| Кіровоградська | 052 | 52 |
| Полтавська | 053 | 53 |
| Сумська | 054 | 54 |
| Херсонська | 055 | 55 |
| Дніпропетровська | 056 | 56 |
| Харківська | 057 | 57 |
| Запорізька | 061 | 61 |
| Донецька | 062 | 62 |
| Луганська | 064 | 64 |
| Кримська | 065 | 65 |

На цей час в Україні розрізняють три різновиди форматів телефонної нумерації для з'єднань поза межами місцевої мережі:

- для міжміських викликів та викликів на номери телефонів абонентів операторів мобільного зв'язку – усього 10 цифр;
- для викликів у межах області (зони) – усього 9 цифр;
- для міжнародних викликів (зокрема і країн СНД) – 13 та більше цифр.

Порядок набору для міжміських викликів та викликів на номери телефонів абонентів операторів мобільного зв'язку такий:

Набрати "0" і дочекатися неперервного сигналу (це вихід на міжміську телефонну мережу).

Набрати "КОД МІСЬКОЇ ТЕЛЕФОННОЇ МЕРЕЖІ", або "ПРЕФІКС ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ".

Набрати "НОМЕР ТЕЛЕФОНУ АБОНЕНТА".

---

* Для Київської області введено новий власний код "45" замість коду "044"

Перші дві цифри у коді міста збігаються із префіксом зони. Наприклад, код міста Дрогобич на Львівщині – це 32-44, код міста Біла Церква на Київщині – це 45-63. Винятком із цього правила є лише місто центрального підпорядкування Севастополь, що має код "692". Коди інших населених пунктів України, чинні із 14 жовтня 2009 року, наведено в додатку 11. При цьому кількість цифр у коді населеного пункту залежить від кількості цифр місцевої телефонної мережі (у підсумку має бути 10-цифровий формат).

Такий самий порядок набору діє і при наборі абонентів мереж мобільного зв'язку зі стаціонарного телефону. Наприклад, щоб зателефонувати абонентам оператора мобільного зв'язку Utel, потрібно набрати 0 – 91, а далі без інтервалу – номер телефону абонента, для абонентів МТС префікс 0-50, для абонентів Київстар 0-67.

Для здійснення викликів у межах області порядок набору можна спростити, скориставшись так званим внутрішньозоновим кодом "2":

Набрати "0" і дочекатися неперервного сигналу (це вихід на міжміську телефонну мережу).

Набрати внутрішньозоновий код "2" замість двох перших цифр коду міста (префіксу зони).

Набрати "НОМЕР ТЕЛЕФОНУ АБОНЕНТА".

Наприклад, щоб зателефонувати зі Львова до Дрогобича (з'єднання у межах зони) замість повного коду

0-3244-xxxxx

достатньо здійснити такий набір:

0-2-44-xxxxx,

де 3244 – код міської телефонної мережі Дрогобича на міжзоновому рівні;

44 – код міської телефонної мережі Дрогобича усередині зони.

Отже, загальна кількість цифр для міжзонового міжміського з'єднання становить 10 цифр, а для міжміського з'єднання всередині зони – 9 цифр. Міжзонові міжміські з'єднання відбуваються за участі магістральних каналів первинної мережі зв'язку, натомість міжміські з'єднання всередині зони задіюють лише канали первинної зонової мережі зв'язку.

Для здійснення міжнародного зв'язку застосовується такий порядок набору:

- набрати "0" і дочекатися неперервного сигналу;

- набрати ще один "0" (префікс виходу на міжнародний зв'язок);
- набрати "КОД КРАЇНИ";
- набрати "КОД МІСТА";
- набрати "НОМЕР ТЕЛЕФОНУ АБОНЕНТА".

Наприклад, щоб зателефонувати до міста Москви, потрібно набрати 0-0-7 (код Росії), 495 (код м. Москва) та семизначний номер абонента, щоб зателефонувати до міста Кракова, потрібно набрати 0-0-48 (код Польші) – 12 (код м. Краків) та семизначний номер абонента.

На місцевих телефонних мережах зони застосовують закриту систему нумерації. Значність нумерації визначається структурою мережі (без вузлів, з ВВхП, з ВВхП і ВВихП) і кількістю абонентів. На міській мережі без вузлів використовується п'ятизначна нумерація, на мережі з ВВхП – шестизначна, на мережі з ВВхП і ВВихП – семизначна. На сільській телефонній мережі переважно використовується закрита п'ятизначна система нумерації.

Для виклику екстрених служб та інформаційно-довідкових послуг, які користуються найбільшим попитом, на міських телефонних мережах застосовується система конечної спеціальної нумерації.

З 3 по 18 лютого 2009 року відбувся перехід на новий формат набору номерів екстрених, інформаційно-довідкових та служб замовлення. При переході на нову систему нумерації скорочені номери екстрених служб 0Х замінені на 10Х (табл. 3.2).

*Таблиця 3.2*

**Формат набору номерів екстрених служб**

| Назва служби | Старий формат набору номерів | Новий формат набору номерів |
|---|---|---|
| Пожежна охорона | 01 | 101 |
| Міліція | 02 | 102 |
| Державна швидка медична допомога | 03 | 103 |
| Аварійна служба газової мережі | 04 | 104 |

Також замінені номери інформаційно-довідкових послуг телефонних мереж загального користування ВАТ "Укртелеком" (табл. 3.3).

*Таблиця 3.3*

**Формат набору номерів інформаційно-довідкових та служб замовлення**

| Назва служби | Старий формат набору номерів | Новий формат набору номерів |
|---|---|---|
| Інформаційно-довідкова послуга АМТС (МТС) | 070 | 170 |
| Приймання замовлень на розмови з населеними пунктами України | 071 | 171 |
| Довідкова послуга замовлень розмов з населеними пунктами України | 072 | 172 |
| Довідкова послуга замовлень міжнародних розмов | 073 | 173 |
| Приймання замовлень на розмови з готелю | 074 | 174 |
| Приймання замовлень на міжнародні розмови | 079 | 179 |
| Довідкова послуга з надання номерів | 09 | 109 |
| Централізована служба бюро ремонту телефонів | 08 (008) | 1508 |
| Довідка про скорочені номери | | 120 |
| Служба точного часу | 060 | 121 |
| Прогноз погоди | | 122 |

## 3.4. Телефонна сигналізація

### 3.4.1. Види сигналів телефонної сигналізації

Сукупність електричних сигналів, що використовуються у мережі для встановлення з'єднання, називається ***системою телефонної сигналізації***. Телефонній сигналізації присвячені Рекомендації МСЕ-Т серії Q.

До системи телефонної сигналізації переважно зараховані такі види сигналів:

1. ***Лінійні (Л) сигнали***, що визначають стан пристроїв мережі на основних етапах встановлення з'єднання (зайняття, відбій, роз'єднання тощо).

2. ***Адресні (А), або керуючі сигнали,*** які передають відомості між керуючими пристроями комутаційних вузлів про маршрут у мережі до абонентського пристрою призначення. У багатьох системах також передаються

сигнали про категорію виклику, запиту апаратури автоматичного визначення номера (АВН) тощо.

3. ***Оповіщувальні (О) акустичні сигнали*** передаються від АТС до ТА і слугують для інформування абонента про етапи (фази) встановлюваного з'єднання:

– відповідь станції;
– зайнято;
– посилання виклику;
– контроль посилання виклику.

В АТС із електронним керуванням може передаватися сигнал попередження про міжміський виклик. Набір сигналів системи сигналізації залежить від типу комутаційного обладнання, типу систем передачі, що використовуються, структури мережі тощо.

Розрізняють абонентську та міжстанційну сигналізації. Система абонентської сигналізації визначає порядок обміну сигналами між абонентським пристроєм (телефонним апаратом, факсом тощо) і АТС, натомість система міжстанційної сигналізації визначає порядок обміну сигналами між станціями. Для місцевих, внутрішньозонових, міжміських і міжнародних мереж використовуються різні системи міжстанційної сигналізації (див. 3.4.3).

### 3.4.2. Алгоритм встановлення з'єднань у телефонній мережі

Під час встановлення з'єднання між абонентським пристроєм (ТА) і вузлом комутації (АТС), а також між вузлами комутації передаються сигнальні повідомлення, послідовність яких показана на рис. 3.14.

Будь-яка станція повинна правильно інтерпретувати лінійні та адресні сигнали, що надходять лініями зв'язку, та генерувати необхідні сигнали для взаємодії з іншими елементами мережі. Процес обробки викликів включає такі операції:

1. ***Виявлення зміни стану абонентських, або з'єднувальних ліній.*** Зміна стану може бути пов'язана із сигналами адресної інформації або лінійними. Адресні сигнали можуть передаватися імпульсами постійного струму або тональними сигналами набору номера (багаточастотними сигналами).

2. ***Генерування вихідних сигналів.*** За допомогою цих сигналів абоненти оперативно оповіщаються про процес з'єднання або роз'єднання і забезпечується взаємодія за міжстанційного зв'язку.

3. ***Вибір шляху*** (маршруту) через комутаційне поле станції.
4. ***Встановлення розмовного тракту*** у комутаційному полі.
5. ***Передача мовних або інших інформаційних сигналів.***
6. ***Роз'єднання абонентів*** (руйнування розмовного тракту).

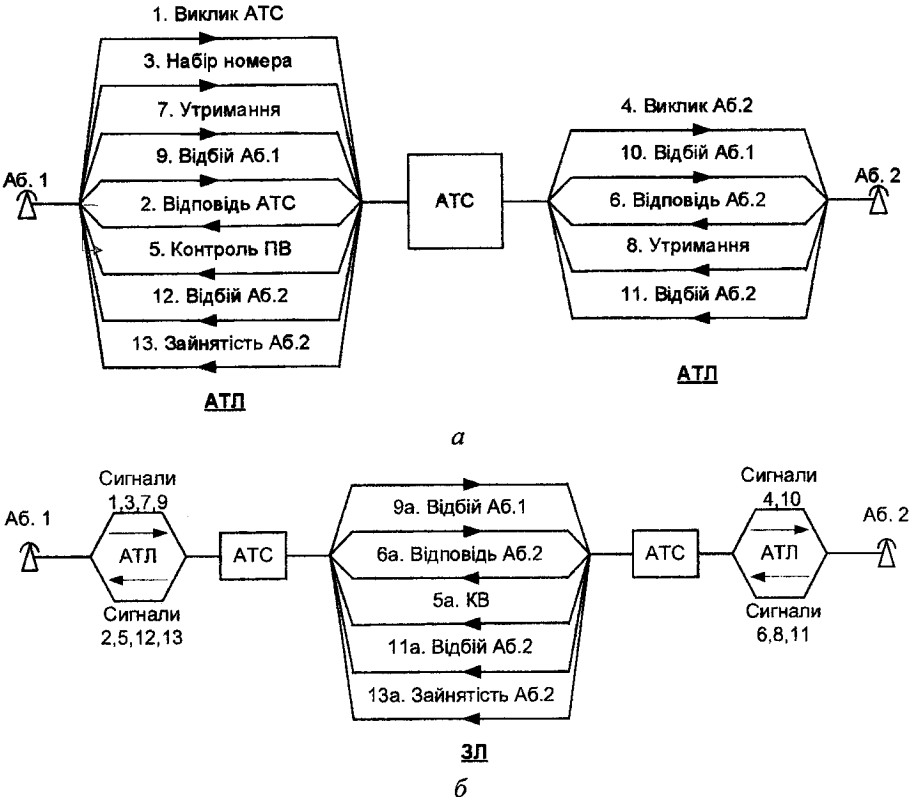



*Рис. 3.14. Типовий порядок обміну сигналами систем абонентської (а) і міжстанційної (б) сигналізації*

Типова послідовність процесів на станції незалежно від типу (електромеханічна, електронна, цифрова) за успішного з'єднання така:

а) виявлення запиту ресурсів станції від абонента або з'єднувальної лінії (каналу);

б) пошук необхідних ресурсів (наприклад, приймача цифр набору номера);

в) сповіщення абонента про надання ресурсів (наприклад, сигналом "відповідь станції");

г) прийом і накопичення цифр номера, припинення передачі сигналу "відповідь станції";

д) передача лінійних і адресних сигналів у з'єднувальну лінію або канал міжстанційного зв'язку;

е) встановлення розмовного тракту у комутаційному полі станції;

ж) визначення стану лінії абонента, що викликається;

з) генерування посилань виклику (ПВ), якщо лінія вільна;

и) генерування сигналу "контроль посилань виклику" (КПВ);

к) виявлення відповіді абонента, що викликається, припинення ПВ і КПВ.

### 3.4.3. Системи міжстанційної сигналізації

Типовий порядок обміну повідомленнями систем міжстанційної сигналізації під час встановлення телефонного з'єднання розглядався у 3.4.2.

Сигнали міжстанційної сигналізації можуть передаватися ***децентралізованим і централізованим*** способами.

Традиційно у телефонних мережах використовується децентралізована сигналізація. За такого способу сигнальні повідомлення передаються тим самим каналом, що й інформація користувача ***(in-band),*** або спеціальним сигнальним каналом, прокладеним паралельно з інформаційним. У цифрових мережах використовується так звана централізована сигналізація, суть якої полягає у тому, що сигнальні повідомлення багатьох користувачів передаються у цифровому вигляді спільним для них каналом сигналізації (СКС) у формі пакетів сталої або змінної довжини.

У системах міжстанційної телефонної сигналізації застосовуються такі способи передачі ***лінійних*** сигналів:

- шлейфовий (loop-start) – за фізичними дводротовими проводами (як у АТЛ);
- ***частотний*** – виділеним сигнальним каналом (поза смугою каналу тональної частоти) на частоті 3825 Гц під час використання ***аналогових систем передачі*** з частотним розділенням каналів;

• ***накладення*** – виділеним сигнальним каналом під час використання ***цифрових систем передачі.***

У сучасних системах для передачі сигналів ***управління*** застосовуються різні реалізації багаточастотного (Multi Frequency – MF) способу у смузі каналу ТЧ. Міжнародні системи сигналізації ***R1 і R2***_використовують частоти з інтервалом 120 Гц в діапазоні 1380...1980 Гц у прямому і 540...1140 Гц – у зворотному напрямі (***MF-R1 і MF-R2***). Широко вживана у ТфМЗК України система сигналізації використовує частоти в діапазоні від 700 до 1700 Гц із кроком 200 Гц.

Вищерозглянуті системи сигналізації історично виникли першими і використовуються за децентралізованого способу передачі. Проте із розвитком систем комутації з'явився новий клас систем із централізованим способом сигналізації по СКС, який безпосередньо пов'язує керуючі пристрої АТС. Перша система подібного класу – ***система сигналізації № 6 МСЕ-Т*** – призначалася для передачі усіх видів управляючої інформації каналами ТЧ аналогових систем передачі на швидкостях 2,4...4,8 кбіт/с. Система має добрі експлуатаційні параметри і поширена в Європі, Японії і особливо у США, де вона експлуатується дотепер.

Поява і швидке упровадження ЦСП зумовили появу ***системи сигналізації № 7 МСЕ-Т (SS7)***, орієнтованої на застосування у цифрових мережах. Один канал SS7 зі швидкістю 64 кбіт/с дає змогу передавати сигнальну інформацію для пучка з однієї–двох тисяч каналів ТЧ.

Маючи величезний потенціал, SS7 не лише забезпечила потреби передачі сигнальної інформації для існуючого у момент її появи рівня розвитку зв'язку, але й сприяла створенню нових послуг зв'язку. По суті SS7 утворює мережу передачі даних – мережу сигналізації, при цьому усі сигнали збираються у пакети і забезпечуються заголовком, що встановлює належність кожного з сигналів певному каналу тональної частоти.

У сучасних цифрових мережах, що використовують спеціальну підмережу сигналізації, забезпечується відновлення каналу під час його несанкціонованого руйнування.

## Питання для самоконтролю:

**1.** Дайте означення первинної та вторинної мереж зв'язку. Які види вторинних мереж набули найбільшого поширення?

**2.** Опишіть трирівневу структуру побудови і назвіть засоби утворення перспективних первинних телекомунікаційних мереж.

**3.** Яку роль у функціонуванні первинних мереж відіграють технології WDM, SDH і ATM?

**4.** Опишіть структуру та особливості телефонної мережі загального користування України, а також охарактеризуйте її місце у міжнародному телекомунікаційному просторі.

**5.** Наведіть типові типології телефонних мереж та вкажіть доцільні випадки їх застосування.

**6.** Покажіть, як кількість абонентів впливає на структуру міських телефонних мереж.

**7.** Охарактеризуйте стратегії переходу від аналогових телефонних мереж до цифрових.

**8.** У чому полягає особливість цифрових мереж з інтеграцією послуг та які її основні відмінності від аналогової мережі?

**9.** У чому полягають переваги застосування цифрових систем комутації під час побудови телефонних мереж?

**10.** Назвіть відмінності між цифровими автоматичними телефонними станціями та цифровими системами комутації.

**11.** Опишіть принципи побудови та функціонування міжміського та міжнародного телефонного зв'язку.

**12.** У чому полягає особливість передачі телефонних повідомлень на місцевому, зоновому та міжзоновому рівнях?

**13.** Поясніть системи нумерації у телефонній мережі загального користування.

**14.** Поясніть алгоритм встановлення з'єднань у телефонній мережі та процес оброблення виклику на АТС за успішного з'єднання.

**15.** Що називається системою телефонної сигналізації та які види сигналів її визначають?

**16.** Назвіть відмінності міжстанційної централізованої сигналізації від децентралізованої. У чому полягає суть міжстанційної сигналізації спільним каналом?

# Розділ 4

# ТЕЛЕФОННИЙ ЗВ'ЯЗОК ПОЗА ТЕЛЕФОННОЮ МЕРЕЖЕЮ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Телефонна мережа загального користування давно вже втратила монополію на телефонний зв'язок. Сьогодні мережі стільникового зв'язку та комп'ютерні мережі не лише доповнюють, але й успішно конкурують із телефонною мережею загального користування у сфері надання послуг із обміну телефонними повідомленнями. Мережі стільникового зв'язку є бездротовими, а тому забезпечують зв'язок між рухомими абонентами, натомість основною перевагою комп'ютерних мереж у передачі голосових повідомлень є дешеві тарифи. Це є наслідком високої ефективності використання пропускної спроможності каналів, утворюваних у мережах із пакетною комутацією.

Цей розділ ознайомлює із технологією функціонування, загрозами та методами і засобами захисту телефонних повідомлень у стільниковій мережі стандарту GSM, а також IP-телефонії.

У результаті вивчення цього розділу студент повинен знати:

- принципи функціонування і архітектуру стільникового зв'язку на прикладі стандарту GSM;
- засоби безпеки системи GSM, процеси аутентифікації та шифрування;
- принципи формування і передачі телефонних повідомлень у мережах із комутацією пакетів;
- особливості організації телефонного зв'язку у локальній мережі та через Інтернет;
- проблеми забезпечення якості телефонних розмов у пакетній телефонії.

## 4.1. Стільниковий зв'язок

### 4.1.1. Архітектура і технологія системи GSM

У ***стільниковому зв'язку*** (рос. ***сотовой связи***) зона дії поділена на фрагменти або комірки (рис. 4.1), які нагадують бджолині "чарунки" (звідси і назва). Розміри "чарунок" залежать від потужності базової приймально-передавальної станції, що розташована у центрі комірки (BTS – Base Transceiver

Station). Форма і розмір комірок узгоджуються із вимогами населеного пункту (на сільських теренах розмір більший, в аеропортах та густонаселених районах великих міст – менший).

Щоб забезпечити утримання каналу під час переміщення активного абонента між комірками у системах стільникового зв'язку використовується складна система службових сигналів, яка істотно навантажує мережу.

Оператори стільникового зв'язку забезпечують своїм клієнтам можливість комунікації із абонентами стаціонарних телефонних мереж загального користування, зокрема і міжнародні сполучення (roaming).

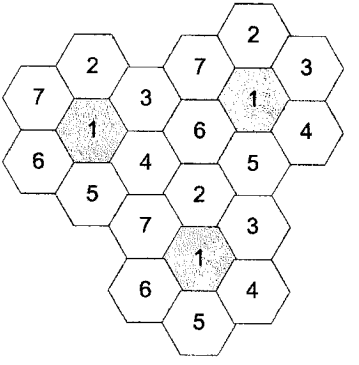



*Рис. 4.1. Поділ зони дії стільникового зв'язку на комірки*

Структура системи GSM містить три складові (рис. 4.2):

- підсистему рухомих терміналів;
- підсистему базових станцій;
- підсистему мережевого рівня.

Типовими складовими системи GSM (рис. 4.2) є:

- рухомі термінали (MS – Mobile Station);
- базові станції (BTS);
- контролери базових станцій (BSC – Base Station Controller) – керують багатьма (від десяти до кількох сот) BTS;
- шлюзи для обслуговування зовнішніх мереж (GMSC – Gateway Mobile Swiching Center);

- центр експлуатації і обслуговування мережі (OMC – Operational& Maintenance Center) – здійснює конфігурацію BTS і BSC, моніторинг стану навантаження і помилок у мережі;
- реєстр власних станцій (HLR – Home Location Register) – містить інформацію про MS своїх клієнтів;
- реєстр чужих станцій (VLR – Visitor Location Register) – веде реєстр MS, що тимчасово перебувають у зоні обслуговування мережі;
- центр автентифікації (AC – Authenfication Center) – становить ядро безпеки системи;
- реєстр ідентифікації обладнання (EIR – Equipment Identification Register) – містить серійні номери загублених і вкрадених телефонів.

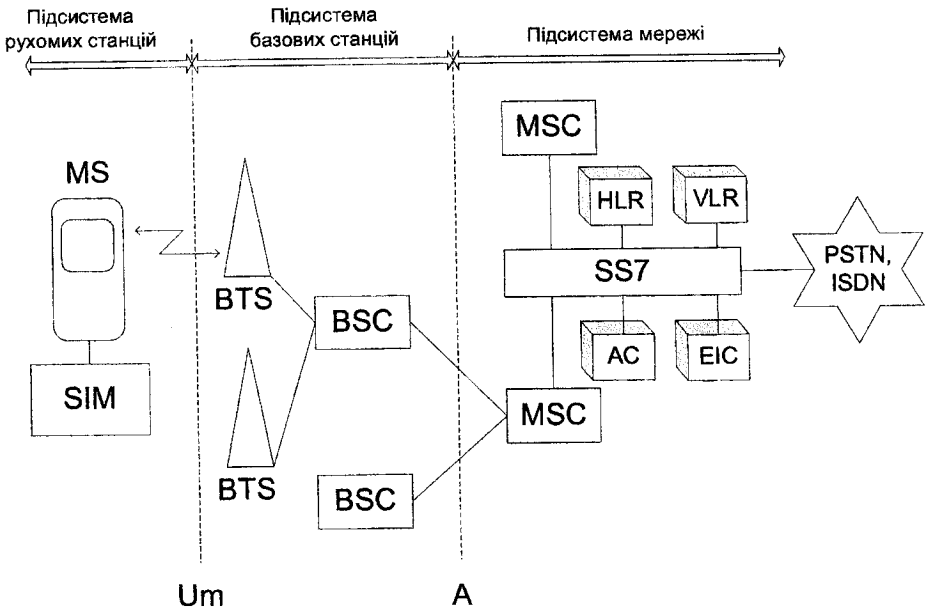



*Рис. 4.2. Структура та складові системи GSM*

Мобільна станція MS – це стільниковий телефонний апарат із мікропроцесорною картою SIM – Subscriber Identity Modul. Карта SIM містить

міжнародний номер мобільного абонента (IMSI – International Mobile Subscriber Number), індивідуальний ключ автентифікації, алгоритм шифрування, PIN – для контролю доступу до самої карти. Підсистема базових станцій побудована із двох складових:

- базових приймально-передавальних станцій BTS, кожна з яких містить близько 16 передавально-приймальних пристроїв, які працюють на частотах своєї комірки, забезпечуючи через радіоканал Um зв'язок з MS;
- контролерів базових станцій BSC, які через інтерфейс Abis керують багатьма BTS, зокрема встановлюють частоти радіоканалів, контролюють перемикання з'єднань між комірками, стрибки частоти для забезпечення стабільності зв'язку в умовах нестаціонарності параметрів радіоканалу, а також утворюють з'єднання із комутаційною станцією MSC.

З'єднання між абонентами, що знаходяться у межах однієї комірки, забезпечується у межах підсилення базових станцій, тобто за участю BTS і BSC.

Підсистема рівня мережі утворена із:

- комутаційної станції MSC;
- реєстрів власних HLR і чужих VLR станцій;
- реєстру ідентифікації обладнання EIR;
- центру автентифікації AC.

Комутаційна станція MSC стільникової мережі відповідає АТС в ТфМЗК. MSC обслуговує групу комірок, використовуючи інформацію, нагромаджену у реєстрах HLR, VLR, EIR та центру AC. Через шлюз GMSC здійснюється комутація з клієнтами з інших мереж.

Радіоканал Um у системі GSM займає смугу частот 890 ÷ 915 МГц для трансмісії вгору (від MS до BTS) і смугу 935 ÷ 960 МГц – для трансмісії вниз (від BTS до MS). У кожній із смуг завширшки 25 Мгц розміщаються 124 частотні канали (FDMA) завширшки 200 кГц. Кожний частотний канал додатково ущільнюється на 8 часових інтервалів (TDMA), що у підсумку дає 992 дуплексні канали.

Іншими важливими властивостями радіоканалу GSM є:

- адаптаційне підлаштовування у часі, що забезпечує MS користування власної часової щілини для компенсації затримки розповсюдження;

- модуляція з мінімальним стрибком частоти і гауссівської фільтрації прямокутного імпульсу (GMSK – Gaussian Minimum Shift Keying), яка поєднує спектральну ефективність і низький рівень інтерференції;
- стрибки несучої з метою запобігання завмиранню і спотворенням окремих частотних каналів.

### 4.1.2. Засоби безпеки системи GSM

До засобів безпеки, що використовуються у стандарті GSM, належать:

- центр аутентифікації AC;
- реєстри власних HLR і чужих VLR станцій;
- карти SIM;
- ідентифікаційні номери абонента, міжнародний IMSI і тимчасовий TMSI;
- шифрування;
- часовий колективний доступ TDMA;
- стрибки частоти несучого коливання;
- реєстр ідентифікації обладнання EIR та ідентифікаційний номер рухомого терміналу IMEI.

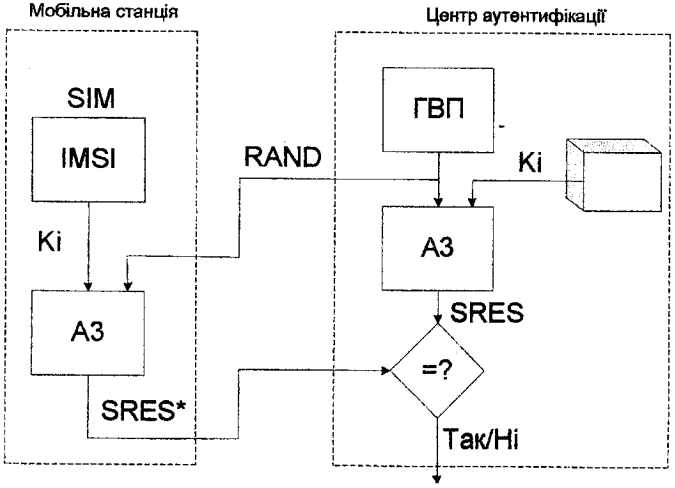



*Рис. 4.3. Процес аутентифікації в GSM*

Аутентифікація повідомлень і користувача є засадничими аспектами безпеки. Аутентифікація ґрунтується на використанні SIM-карти, доступ до якої вимагає знання 4-значного PIN коду з обмеженням вводу до трьох спроб.

Процес аутентифікації пояснює рис. 4.3.

Крім аутентифікації, у системі GSM використовується шифрування даних у радіоканалі Um (рис. 4.4).

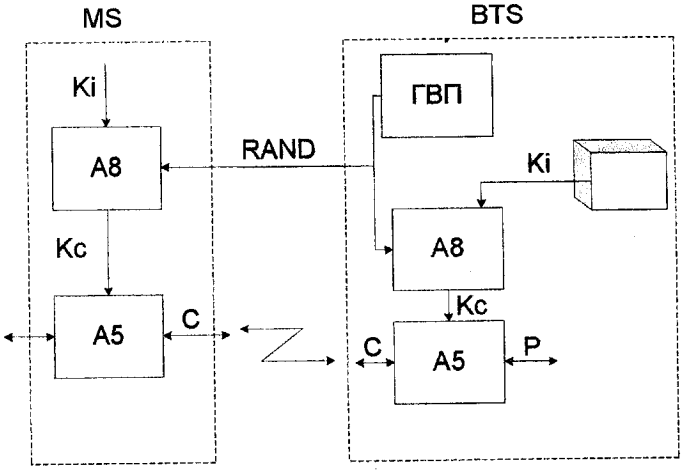



*Рис. 4.4. Процес шифрування в GSM*

## 4.2. Телефонія у мережах з пакетною комутацією

Сприйняття людиною голосового повідомлення дуже чутливе до затримок, а особливо до їх коливань. У телефонних мережах загального користування вузли комутації функціонують за технологією комутації каналів, утворюючи наскрізний фізичний тракт для передачі голосових повідомлень, тому їх затримка визначається переважно лише часом розповсюдження сигналу. Стандарти вимагають, щоб значення затримки не перевищувало 150 мс, а під час використання супутникових каналів – 250 мс.

Комп'ютерні мережі – це мережі із комутацією пакетів, що передбачають поділ (фрагментацію) цифрових повідомлень на окремі блоки (пакети) та їх буферування у вузлах комутації. Процес комутації у таких вузлах за своєю

природою спричиняє затримку повідомлень, не лише через їх запис і зчитування, але також через очікування у черзі на вузлі комутації. Сумарна затримка повідомлень від джерела до одержувача є не прогнозованою, оскільки залежить від навантаження на окремих ділянках мережі та кількості вузлів комутації.

Передача пакетів у комп'ютерних мережах здійснюється за допомогою спеціальних протоколів. На цей час як у локальних (LAN), так і у глобальних (WAN) мережах, найпоширенішим є набір протоколів TCP/IP. Тому передачу голосових повідомлень за допомогою таких мереж називають IP-телефонією.

### 4.2.1. Телефонний зв'язок у локальній мережі

Телефонний зв'язок можна організувати на основі локальної мережі (LAN) без використання традиційної телефонної інфраструктури (відомчих АТС, виділених телефонних ліній, телефонних апаратів).

Як термінальне обладнання в LAN-телефонії можуть використовуватися (рис. 4.5):

- спеціальні, так звані Ethernet-телефони;
- телефонні шлюзи як адаптери для під'єднання звичайних телефонних апаратів;
- персональні комп'ютери із навушниками і мікрофоном.

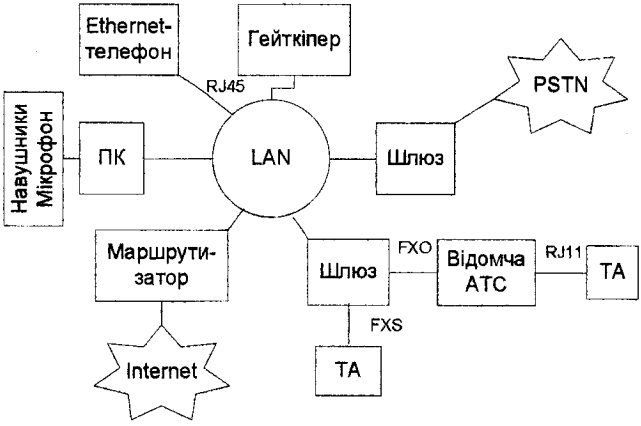



*Рис. 4.5. Структура телефонного зв'язку на основі локальної комп'ютерної мережі*

Ethernet-телефон за зовнішнім виглядом нагадує звичайний телефонний апарат, в якому, крім перетворення акустичних коливань в електричні сигнали, відбувається аналого-цифрове перетворення, розбиття "оцифрованого" сигналу мовлення на Ethernet-кадри та їхня передача проводами локальної мережі.

Щоб ПК виконував роль телефонного терміналу, його потрібно оснастити відповідним апаратним та програмним забезпеченням (рис. 4.6). Апаратне забезпечення – це мережева і звукова карти, навушники та мікрофон. Програмне забезпечення містить протокол H.323 та спеціальну прикладну програму, що підтримує телефонний зв'язок на основі IP-мережі (наприклад, програма Skype).

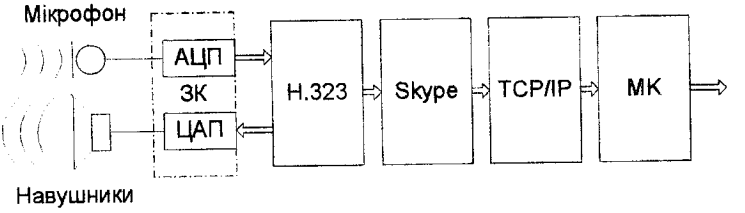



*Рис. 4.6. Склад програмно-апаратного забезпечення комп'ютера для пакетної телефонії: ЗК – звукова карта; МК – мережева карта*

***Телефонний шлюз*** – це пристрій, який виконує обмін голосовими та службовими повідомленнями між LAN і традиційною телефонною мережею PSTN. У шлюзі голосові повідомлення, що передаються по LAN, вилучаються із кадрів, декодуються і перетворюються до вигляду електричних сигналів, які використовуються у телефонній мережі. До шлюзу можна підключати як аналогові, так і цифрові пристрої. Під час підключення стандартних телефонних апаратів (порт FXS) шлюз емулює для цих апаратів стандартні сигнали АТС. Під час підключення аналогової відомчої АТС (порт FXO) шлюз емулює роботу звичайного абонентського терміналу. До шлюзу може бути підключена АТС через цифровий канал E1, що одночасно підтримує близько 30 телефонних з'єднань.

Ядром LAN-телефонії є комп'ютер із спеціальною серверною програмою, яка називається гейткіпером, або адміністратором викликів. Його завданням є зіставлення телефонного номера абонента із IP-адресою його

терміналу, визначення номера абонента, що ініціює з'єднання, ведення журналу викликів, фіксація тривалості розмов. Адресна інформація із терміналу (телефону чи комп'ютера) надходить на гейткіпер, який, спираючись на свою базу даних, визначає IP-адресу адресата і надсилає йому виклик. Якщо виклик адресовано абоненту звичайної телефонної мережі, то він скеровується на відповідний телефонний шлюз.

### 4.2.2. Телефонний зв'язок через Інтернет

Телефонний зв'язок через Інтернет може здійснюватися різними способами. Для організації телефонних переговорів між користувачами персональних комп'ютерів, останні, як і у випадку локальної мережі, потрібно оснастити мультимедійним обладнанням і (або) спеціальними програмними засобами. Комп'ютери можуть входити до складу локальної мережі, мати персональну IP-адресу або підключатися до мережі Інтернет за допомогою модему (рис. 4.7).

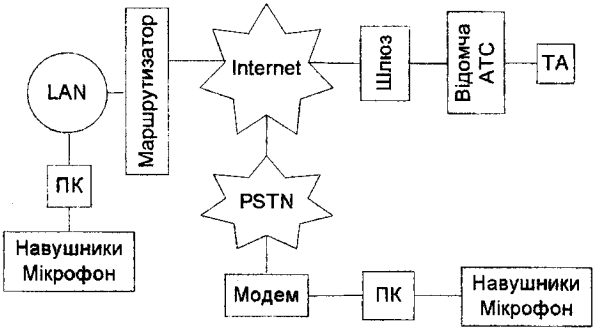



*Рис. 4.7. Структура IP-телефонії*

Важливим аспектом практичного використанням IP-телефонії є організація дешевого міжміського зв'язку між абонентами міських телефонних мереж (рис. 4.8). Для цього на міських телефонних станціях або відомчих АТС встановлюються шлюзи, які призначені для перетворення аналогових мовних і службових сигналів у цифрову послідовність, організації з цієї послідовності пакетів глобальної мережі Інтернет і передачі їх у мережу, прийом пакетів і

відновлення цифрової послідовності – цифрових мовних і службових сигналів і їх перетворення в аналогову форму.

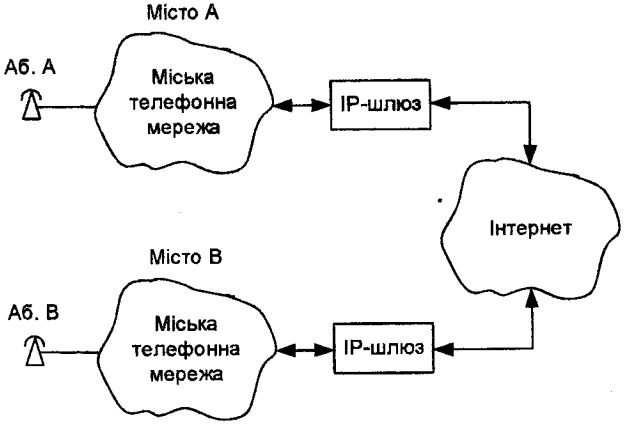



*Рис. 4.8. Використання IP-телефонії для міжміського зв'язку*

### 4.2.3. Проблеми забезпечення якості телефонних розмов у IP-телефонії

Серед каналів, на яких може бути організований IP-телефонний зв'язок, особливе значення мають канали Інтернету. Незважаючи на велику різноманітність, що характеризується пропускними спроможностями, кількістю маршрутизаторів, характеристиками фізичних ліній тощо, реально діючі канали Інтернет характеризуються:

- реальною пропускною спроможністю, що визначається "найвужчим місцем" у віртуальному каналі у цей момент часу;
- трафіком, що також є функцією часу;
- затримкою пакетів, що визначається трафіком, кількістю маршрутизаторів, реальними фізичними властивостями каналів передачі, які у цей момент часу утворюють віртуальний канал, затримками на обробку сигналів у мовних кодеках і шлюзах;
- втратою пакетів, зумовленою наявністю "вузьких місць", чергами;
- перестановкою пакетів, що прийшли різними шляхами.

Відомі два підходи до вирішення цієї проблеми:

- резервування частини пропускної здатності мережі для передачі пакетів із голосовими повідомленнями;
- побудова магістральної транспортної мережі Інтернет на основі технології ATM або FR.

Мережі з комутацією пакетів були створені для передачі даних, тому можливість їх використання для передачі голосового трафіку у реальному часі (як у традиційній телефонії) значною мірою залежить від затримки, що вноситься цими мережами під час проходження сигналу. На рис. 4.15 показані затримки, що вносять окремі структурні елементи пакетної телефонії.

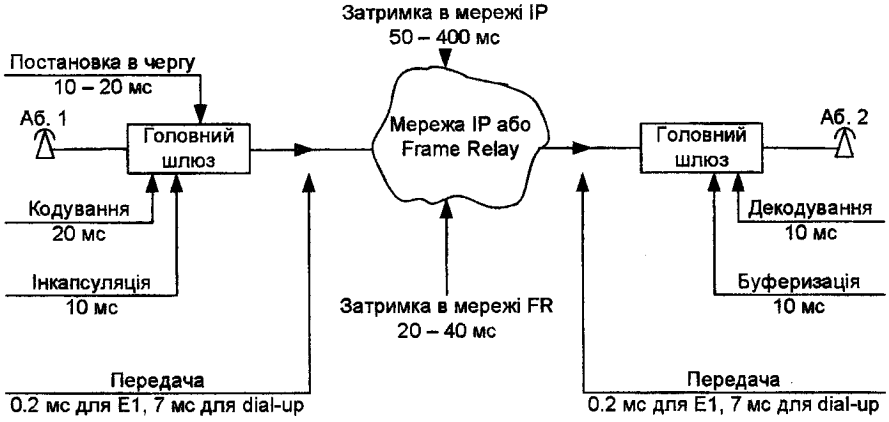



*Рис. 4.9. Характерні для пакетної телефонії затримки (у верхній частині рисунка зазначено змінні затримки, у нижній – фіксовані)*

### 4.2.4. Особливості кодеків голосу для IP-телефонії

Джерелом голосового повідомлення є акустичний сигнал, у якому можна виділити такі типи сигнальних фрагментів: вокалізовані, невокалізовані, перехідні і паузи. Кожен тип сигналу має різний ступінь інформативності, а отже, за однакової тривалості та якості вимагає різної кількості бітів для кодування – для особливо відповідальних за якість мови ділянок мовного сигналу відводиться більше біт, для менш відповідальних – менше. За такої

побудови кодеків можна знизити бітрейт до 2 – 4 кбіт/с за високої якості синтезу голосових повідомлень.

Отже, на відміну від традиційних, кодеки для IP-телефонії доцільно будувати із змінною швидкістю, в основі якої лежить класифікатор вхідного сигналу, що визначає ступінь його інформативності (у найпростішому випадку – це аналізатор активності).

У IP-мережах окремі пакети можуть бути втрачені. Повторна передача голосових пакетів позбавлена сенсу через ліміт часу (використовується протокол UDP). Тому одним із найважливіших завдань під час побудови кодеків для IP-телефонії є створення алгоритмів компресії мови толерантних до втрат пакетів. При цьому час кодування не відіграє принципового значення на тлі затримок у вузлах комутації.

### Питання для самоконтролю:

**1.** Які фізичні принципи функціонування стільникового зв'язку та у чому полягають особливості утворюваних каналів?

**2.** Наведіть структуру та опишіть функції основних структурних елементів системи GSM.

**3.** Перерахуйте засоби безпеки системи GSM.

**4.** Опишіть процеси аутентифікації та шифрування у системі GSM.

**5.** Який принцип передачі телефонних повідомлень у мережах із комутацією пакетів?

**6.** Наведіть структуру телефонного зв'язку на основі локальної комп'ютерної мережі.

**7.** Опишіть типовий склад програмно-апаратного забезпечення комп'ютера для пакетної телефонії.

**8.** Покажіть способи організації телефонного зв'язку через Інтернет.

**9.** Як використовують IP-телефонію для організації міжміського зв'язку?

**10.** Назвіть особливості каналів Інтернету, які мають пряме відношення до передачі телефонних повідомлень.

**11.** Перерахуйте джерела затримок та орієнтовні їх значення у IP-телефонії.

**12.** Які особливості голосових кодеків у системі пакетної телефонії?

# Розділ 5

# КОНЦЕПТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ ІЗ ТЕЛЕФОННИМ ЗВ'ЯЗКОМ

Телефонний зв'язок є одним із найнезахищеніших, що значною мірою є наслідком історичних та економічних аспектів. До того ж проблематика інформаційної безпеки абонентів телефонного зв'язку має свою специфіку. Це зумовлено, з одного боку, природою телефонних повідомлень, а з іншого, – особливістю утворення та функціонування телефонних трактів. Тому просте перенесення принципів захисту інформації, наприклад із комп'ютерних мереж, є недостатнім і неефективним.

На цей час в Україні абонети можуть обирати кілька шляхів для досягнення інформаційної безпеки під час обміну телефонними повідомленнями конфіденційного характеру. За підключення до Державної системи урядового зв'язку або Національної системи конфіденційного зв'язку абоненти одержують, так би мовити, у пакеті комплекс послуг як щодо функціональності, так і щодо захищеності каналів. Інший варіант передбачає забезпечення захисту засобів телефонної мережі загального користування своїми коштами та на свій розсуд.

У результаті вивчення цього розділу студент повинен знати:

- джерела загроз та специфіку завдань інформаційної безпеки на об'єктах із телефонним зв'язком;
- призначення Державної системи урядового зв'язку і Національної системи конфіденційного зв'язку України, а також доцільні випадки використання абонентами каналів цих спеціальних мереж та обмеження, які при цьому виникають;
- принципи організації захищеної корпоративної мережі телефонного зв'язку і основні вимоги до систем закриття мовної інформації у трактах телефонної мережі загального користування.

## 5.1. Аналіз загроз для інформації у телефонних мережах загального користування

Як відомо, інформаційну безпеку розуміють у трьох аспектах:

- конфіденційність – це забезпечення інформаційної системи від витоку інформації;

- доступність – це можливість у будь-який момент отримати сервіс заданої якості;
- цілісність – це запобігання несанкціонованій модифікації інформації.

Стосовно телефонного зв'язку загроза конфіденційності проявляється у:

- підслуховуванні телефонних розмов (піднята телефонна трубка);
- прослуховуванні приміщень, у яких знаходиться телефонний апарат (покладена телефонна трубка).

***Підслуховування телефонних розмов*** можливе за допомогою доволі простих технічних засобів, оскільки голосові повідомлення передаються у відкритому вигляді. Утворення елементами телефонного апарата паразитних сигналів створює загрозу ***прослуховування приміщень***.

Загрозу доступності можна розглядати як ***блокування доступу*** внаслідок пошкодження елементів телефонного тракту чи спотворення службових сигналів на етапі встановлення з'єднання. Крім того, значне погіршення стану каналів зв'язку, а відтак і зниження якості голосових повідомлень також можна розглядати як вид блокування.

Загроза цілісності стосовно телефонного зв'язку має свою специфіку. Насамперед модифікувати телефонні голосові повідомлення складно через їх природу (передача у реальному часі мережами із комутацією каналів). Фальшування телефонних повідомлень між знайомими абонентами також малоймовірне через натуральний спосіб взаємної автентифікації за голосом, манерами розмовляти, можливістю задати будь-яке питання, щоб зняти підозри. Проблема автентичності виникає у разі, коли абоненти не є знайомими. Загалом автентичність абонента можна було б пов'язати із його абонентським номером та здійснити повторне віддзвонювання, але недостатня захищеність абонентської телефонної лінії від несанкціонованих підключень залишає це питання відкритим. Є ще один аспект загрози цілісності системи телефонного зв'язку – це телефонне шахрайство, тобто несанкціоноване використання засобів телефонного зв'язку. Порушення цілісності системи телефонного зв'язку відбувається гальванічним підключенням до абонентської телефонної лінії.

Розглянемо структуру телефонного зв'язку з позицій інформаційної безпеки. Телефонний тракт утворюється за допомогою фізичного з'єднання абонентської лінії, елементів комутаційного поля АТС, каналів з'єднувальних ліній та систем передачі (рис. 5.1).

Аналіз загроз для телефонного зв'язку показав, що абонентська лінія є найвразливішим елементом телефонного тракту, оскільки доступ до обладнання АТС є обмежений для сторонніх осіб, а перехоплення голосових повідомлень у з'єднувальних лініях і магістральних каналах систем передачі є складним через потребу демультиплексації групових сигналів. Абонентська телефонна лінія є неоднорідною за своєю будовою – у стандартному варіанті в її складі можна виділити три ділянки (рис. 5.2).

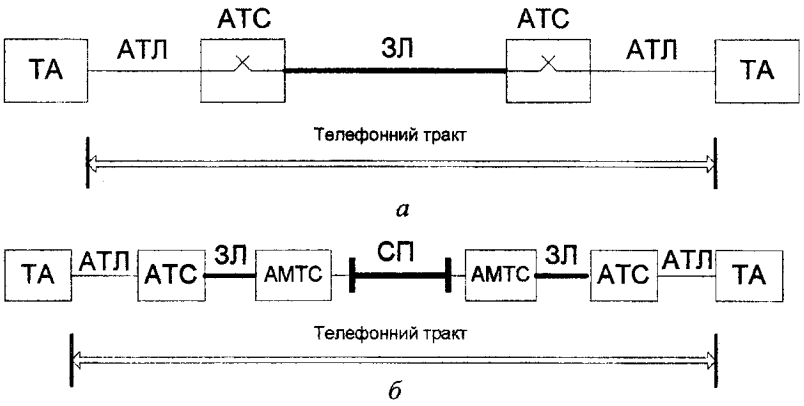



*Рис. 5.1. Елементи телефонного тракту міської (а) та міжміської (б) мереж*

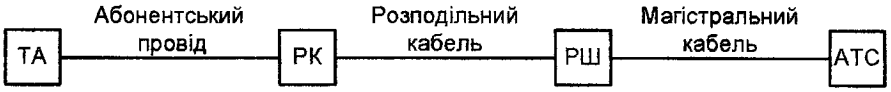



*Рис. 5.2. Елементи абонентської телефонної лінії: ТА – телефонний апарат; РК – розподільна коробка; РШ – розподільна шафа*

Ділянка АТЛ у вигляді прокладеного під землею магістрального багатопарного телефонного кабелю від АТС до розподільної шафи є найдовшою. Далі від розподільної шафи до внутрішньої розподільної коробки АТЛ має продовження також у вигляді багатопарного телефонного кабелю, але порівняно із магістральним меншої ємності та протяжності. Від розподільної коробки до кожного абонента розводка виконується двопровідним телефонним

проводом марки ТРП або ТРВ. Довжина магістрального кабелю становить кілька кілометрів (у середньому 2 – 3 км), розподільного – порядку сотні метрів, а абонентського проводу порівняно невелика – кілька десятків метрів.

Загрози для інформації реалізуються через підключення до АТЛ засобів технічної розвідки. На ділянці багатопарних телефонних кабелів таке підключення малоймовірне (особливо це стосується магістральної ділянки, на якій кабель прокладено у підземних комунікаціях). Найпростішим, а отже, і найвірогіднішим є підключення до відкритих ділянок абонентської проводки, телефонної розетки, телефонного апарата, розподільної коробки чи шафи (рис. 5.2).

У телефонних мережах загального користування кожна АТЛ асоціюється із конкретним абонентом цієї мережі, тобто автентифікація абонентів здійснюється лише на основі фізичного підключення до АТЛ. Зважаючи на відкритість та доступність прикінцевих ділянок АТЛ, існує доволі велика загроза інформаційній безпеці за допомогою несанкціонованих підключень.

Найпростіший спосіб підслухати телефонну розмову – підключитися за допомогою паралельного телефону, "монтерської" слухавки чи звичайних навушників до плеєра. Використовують також спеціальні адаптери для підключення магнітофонів до телефонної лінії. Таке підключення фактично неможливо виявити за допомогою простих технічних засобів. Поширеними є також телефонні ретранслятори, які часто називають "жучками" чи "закладками". Їх підключають паралельно чи послідовно у будь-якому місці абонентської телефонної лінії. Вони мають тривалий термін дії, бо живляться від телефонної мережі. Ці вироби популярні через простоту й дешевизну.

Більшість телефонних "закладок" автоматично вмикаються під час підняття слухавки і передають розмову радіоканалом на приймач пункту перехоплення, де її можуть слухати та записувати. Для маскування телефонні "закладки" роблять у вигляді елементів телефонного апарата. Утім доволі часто закладки встановлюють за межами контрольованого приміщення, що зменшує ризик їх виявлення.

Підслуховування телефонних розмов може здійснюватися і безконтактним способом, тобто без гальванічного контакту із дротами АТЛ, наприклад, використовуючи індуктивні давачі.

## 5.2. Шляхи забезпечення захищеності обміну інформацією у каналах зв'язку

Сьогодні в Україні захищений обмін інформацією між абонентами забезпечується:

- Державною системою урядового зв'язку України;
- Національною системою конфіденційного зв'язку;
- мережею зв'язку загального користування із забезпеченням власними силами захисту.

### 5.2.1. Використання Державної системи урядового зв'язку

Державна система урядового зв'язку України (ДСУЗ) являє собою систему спеціального зв'язку, яка забезпечує передачу інформації, що містить державну таємницю і функціонує в інтересах управління державою у мирний та воєнний час.

ДСУЗ в установленому порядку забезпечує урядовим зв'язком Президента України, Голову Верховної Ради України, прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації.

На відміну від існуючих і створюваних в Україні спеціальних систем зв'язку ДСУЗ має тільки їй притаманну властивість: ***забезпечувати гарантоване засекречування інформації, яка містить державну таємницю***, що передається каналами та лініями зв'язку.

Відповідно до свого призначення ДСУЗ забезпечує послугами зв'язку абонентів у стаціонарних умовах, рухомих об'єктах та непідготовлених з питань зв'язку районах.

Переважно ДСУЗ ґрунтується на стаціонарних об'єктах (станціях) урядового зв'язку, які забезпечують функціонування і взаємодію побудованих в усіх регіональних та великих промислових центрах України мереж і комплексів урядового зв'язку. Забезпечення урядовим зв'язком у місцях, необладнаних стаціонарними засобами зв'язку, здійснюється рухомими вузлами урядового зв'язку.

Технічна експлуатація мереж і комплексів урядового зв'язку здійснюється ***регіональними органами*** та ***територіальними підрозділами*** Держспецзв'язку України.

З метою правового врегулювання питань із забезпечення урядовим зв'язком посадових осіб органів державної влади, місцевого самоврядування, підприємств, установ та організацій Указом Президента України від 18 квітня 2005 року № 663 затверджено "Положення про державну систему урядового зв'язку України", "Порядок забезпечення урядовим зв'язком посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій", а також "Граничну кількість абонентських установок для забезпечення урядовим зв'язком посадових осіб органів державної влади, органів місцевого самоврядування, керівників підприємств, установ і організацій".

ДСУЗ складається із взаємопов'язаних підсистем спеціального зв'язку і ґрунтується на власних комплексах технічних засобів та телекомунікаційних мережах загального користування.

Спроможність системи урядового зв'язку за будь-яких умов забезпечувати надійний та якісний зв'язок досягається ефективною структурною побудовою мереж, обов'язковим резервуванням основних інформаційних напрямків і обладнання зв'язку, застосуванням спеціальних технічних та криптографічних методів захисту інформації, яка передається, підбором і підготовкою висококваліфікованого інженерно-технічного складу підрозділів урядового зв'язку.

Завдання з організації функціонування, безпеки та розвитку ДСУЗ покладено на Департамент організації урядового зв'язку, Департамент урядового польового зв'язку, Управління контролю безпеки урядового зв'язку, які структурно входять до Адміністрації Держспецзв'язку України.

Для убезпечення системи урядового зв'язку на основі цих підрозділів створено ***Центральний орган урядового зв'язку,*** який виконує організаційні та контрольно-наглядові функції з питань дотримання встановлених норм і правил із захисту інформації, що передається телекомунікаційними мережами урядового зв'язку та циркулює на об'єктах інформаційної діяльності (кабінетах, приміщеннях, спорудах, де встановлено абонентські установки та інше обладнання урядового зв'язку).

### 5.2.2. Використання Національної системи конфіденційного зв'язку

Національна система конфіденційного зв'язку (НСКЗ) – це сукупність спеціальних систем (мереж) зв'язку подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії у мирний час та у разі введення надзвичайного і воєнного стану.

Абонентами цієї системи можуть бути як державні, так і комерційні структури, юридичні та фізичні особи.

Однією з особливостей цієї системи є те, що вона створюється як система подвійного призначення. Цей принцип полягає у тому, що у мирний час мережі цієї системи можуть використовуватися організаціями для передачі сучасними видами зв'язку конфіденційної інформації в інтересах як органів державної влади, так і інших юридичних осіб, зокрема суб'єктів фінансово-економічної сфери. В особливий період та у разі виникнення надзвичайних ситуацій ресурс цієї системи буде задіяний для передачі конфіденційної інформації в інтересах національної безпеки та оборони держави.

Конфіденційний зв'язок покладається на Департамент стратегії розвитку спеціальних інформаційно-телекомунікаційних систем, Департамент безпеки інформаційно-телекомунікаційних систем, державне підприємство "Українські спеціальні системи".

НСКЗ дає можливість вирішувати такі стратегічні питання, а саме:

- забезпечити надійний захист конфіденційної інформації, що є власністю держави, відповідно до вимог законодавства;
- створити передумови інтеграції розподілених інформаційних ресурсів та інформаційно-аналітичних систем органів державної влади різного рівня державного управління, в яких циркулює конфіденційна інформація, що є власністю держави;
- забезпечити можливість інформаційної взаємодії між інформаційно-аналітичними системами органів державної влади різного рівня державного управління;

• забезпечити надійний обмін конфіденційною інформацією, яка є власністю держави, між абонентами НСКЗ.

Послуги в НСКЗ реалізуються із забезпеченням необхідного рівня захисту інформації, а саме: здійснюється шифрування інформації за допомогою вітчизняних засобів криптографічного захисту інформації, резервування критичного обладнання та каналів зв'язку, цілодобовий контроль за функціонуванням системи, блокування поширення комп'ютерних вірусів та забезпечується швидка реакція на можливі спроби несанкціонованого доступу до інформації та ресурсів системи.

До складу НСКЗ належать транспортна (телекомунікаційна) мережа, спеціальні мережі надання послуг стаціонарного та мобільного зв'язку, централізована система захисту інформації, централізована система оперативно-технічного управління. На поточний момент здійснюється розгортання регіональних вузлів зв'язку НСКЗ.

В НСКЗ створюються спеціальні мережі мобільного зв'язку які призначені для надання послуг мобільного конфіденційного радіозв'язку під час перебування абонентів НСКЗ у стаціонарних та позастаціонарних умовах за допомогою спеціальних портативних та мобільних абонентських терміналів з функціями КЗІ із забезпеченням захисту інформації за допомогою застосування криптографічних та технічних методів і засобів.

Так, на виконання розпорядження Кабінету Міністрів України від 24.09.2005 р. № 405-р "Про створення спеціальної мережі стільникового зв'язку Національної системи конфіденційного зв'язку" забезпечено створення Спеціальної мережі стільникового зв'язку НСКЗ (СМСЗ).

Основною метою створення СМСЗ є підвищення ефективності функціонування суб'єктів НСКЗ забезпеченням надійного обміну конфіденційною інформацією у позастаціонарних умовах.

Пропонований перелік послуг дає змогу задовольнити потреби в усіх видах зв'язку. Застосовуються сучасні методи криптографічного захисту, що фактично виключають можливість несанкціонованого доступу до передаваної інформації з метою її перехоплення чи фальшування. Під час підключення абонента до системи проводяться роботи щодо захисту абонентського пункту від просочування інформації технічними каналами, пов'язаними з акустичними чи електромагнітними явищами.

### 5.2.3. Використання мереж зв'язку загального користування

Отже, використання Державної системи урядового зв'язку України є єдино можливим шляхом у випадках, коли передавана інформація належить до державної таємниці, і може виявитися зручним для захисту комерційної інформації, якщо підприємство одночасно виконує завдання з захисту держтаємниць. До того ж цей шлях має багато особливостей, що обмежують його застосування:

- захист забезпечується на рівні жорстких вимог захисту держтаємниць, що робить його доволі дорогим і надмірним для комерційних цілей;
- захист забезпечується лише для абонентів, підключених до цієї мережі, що є істотним обмеженням в умовах широких і динамічних зв'язків комерційного підприємства.

Використання Національної системи конфіденційного зв'язку має подібні особливості та обмеження. Тому комерційні підприємства найчастіше обирають третій шлях, пов'язаний із організацією обміну інформацією мережами зв'язку загального користування із забезпеченням захисту власними силами. При цьому абоненти самостійно вибирають ступінь захисту інформації, а обмін конфіденційною інформацією реалізується за тим самим територіальним доступом, що і відкритою.

Отже, найзручніший шлях захисту інформації для комерційних організацій – це створення корпоративної захищеної мережі на основі мережі зв'язку загального користування (МЗЗК). Основна проблема під час виконання цього завдання полягає у виборі ефективних методів та засобів захисту із урахуванням наявних загроз, зумовлених відкритістю та доступністю телефонних каналів.

Організація інформаційного обміну мережами зв'язку загального користування із забезпеченням власними силами захисту як від перехоплення або спотворення інформації в каналі зв'язку, так і від перехоплення у місці розташування абонента, – це найчастіше застосовуваний варіант. Інакше кажучи, йдеться про створення корпоративної захищеної мережі.

Суб'єкт, який організує інформаційний обмін, самостійно вибирає ступінь захисту інформації, може довільно визначати місцерозташування абонентів; захищений інформаційний обмін організовується з тим самим територіальним доступом, з яким реалізується обмін незахищений; потрібна взаємна довіра лише між взаємодіючими абонентами.

Одним із питань, що виникають на цьому шляху, є оцінка доступності для зловмисника ліній зв'язку і комутаційних вузлів МЗЗК мережі, що використовуються. За станом правопорядку сьогодні доводиться орієнтуватися на повну доступність усіх ліній і комутаційного устаткування. Перешкодою можна вважати тільки технічні складнощі під час перехоплення ущільненого магістрального каналу або незручності доступу до кабельних ліній. У разі використовування радіовставок для віддалених або рухомих абонентів потрібно орієнтуватися на повну незахищеність їх від перехоплення.

Принципово побудова захищених радіоканалів можлива, що і пропонує своїм клієнтам ДССЗЗІ, але захист радіоканалів, розрекламований окремими компаніями-провайдерами стільникових і транкінгових мереж рухомого зв'язку з урахуванням можливостей сучасних засобів перехоплення, не може вважатися надійним. Ефективним він може бути тільки щодо випадкового перехоплення або за такої малої значущості передаваної інформації, що витрати кількох тисяч доларів на перехоплення із залученням фахівця виявляться для зловмисника невиправданими.

Для того, щоб рекламовані захисні заходи могли бути взяті до уваги, фірма, яка надає таку послугу, повинна повністю розкрити технологію захисту для оцінки її фахівцями. Так, у рекламних матеріалах ДССЗЗІ конкретно вказуються алгоритми шифрування і порядок поводження з ключовою системою. Для того, щоб зайняти аналогічну позицію, фірма-провайдер радіорухомого зв'язку повинна, як мінімум, мати повну інформацію із захисних алгоритмів, використаних в апаратурі, що поставляється, і мати можливість повною мірою ознайомити з ними клієнта.

За дуже високих вимог до захищеності інформації витрати на реалізацію захисту цим шляхом, природно, будуть порівняльні з витратами першим шляхом, можливо, навіть перевищать їх, але при цьому зберігається незалежність від дислокації партнерів і від системи управління ДСУЗ мережі.

Слід враховувати, що існуюча правова база не дає достатніх підстав для застосування як першого, так і другого шляху. Чинні документи унеможливлюють однозначне визначення ступеня відповідальності держави за збереження інформації абонента і прав державної організації щодо втручання в інформаційний процес. Немає однозначного тлумачення і в частині прав суб'єкта на захист інформації. У частині надання послуг із захисту інформації

іншим суб'єктам діють доволі жорсткі вимоги із ліцензування та сертифікації, але можливість застосування цих вимог до захисту власних інформаційних ресурсів у власних цілях не є очевидною.

У подальшому описано лише технічні аспекти, юридичні питання можливості застосування тих чи інших засобів захисту інформації повинні вирішуватися у конкретних умовах із урахуванням правової бази.

## 5.3. Організація захищеної корпоративної мережі телефонного зв'язку

Передбачається, що для організації захищеного зв'язку використовується державна телефонна мережа і пов'язані з нею системи, що надають абоненту стандартні послуги: телефонний канал (аналогове або цифрове абонентське закінчення) і з'єднання з іншими абонентами мережі.

Під час організації інформаційного обміну, зокрема його захисту, визначальними чинниками є види передаваної інформації і розміщення абонента. Нижче розглядається питання захисту телефонного зв'язку під час обміну мовною інформацією.

### 5.3.1. Основні вимоги до систем закриття мовної інформації у телефонних каналах

Мовний зв'язок вимагає захисту під час спілкування осіб, які допущені та обмінюються конфіденційною інформацією. Це, як правило, керівники організацій або підрозділів. У процесі переговорів важлива не тільки передача семантичного змісту, але й голосова ідентифікація партнера, оцінка його інтонацій.

Можливими партнерами можуть бути як особи, забезпечені захищеним зв'язком, так і особи, що його не мають; тобто має існувати можливість вибору відкритого чи закритого режиму. Водночас процеси встановлення з'єднання, переходу у захищений або відкритий режим не повинні вимагати жодних спеціальних навиків і мінімально відволікати абонента від суті переговорів, що ведуться.

Час, затрачуваний на перехід у захищений режим або вихід з нього, повинен бути мінімальним. Алгоритм входження у захищений зв'язок і виходу у відкритий зв'язок повинен бути стійким до помилок чи неузгоджених взаємних дій партнерів; реакція апаратури на помилки повинна бути зро-

зумілою і "доброзичливою", не повинно відбуватися розриву з'єднання через помилки абонентів, оптимальною реакцією на помилки є перехід у звичний відкритий режим з чіткою індикацією цього факту. Апаратура захисту не повинна обмежувати абонента у частині надання послуг, передбачених для відкритого режиму (наприклад, повинні зберігатися усі можливості системного телефону відомчої АТС або ISDN-консолі).

За просторовим розміщенням можна виділити:

- стаціонарні абоненти, тобто обидва абоненти підключені до державної мережі через стандартні проводові закінчення, що належать безпосередньо цим абонентам;
- хоча б один абонент рухомий – знаходиться в автомобілі, у пішому режимі тощо, причому у ролі абонентського терміналу виступає радіостанція, що не має стандартного провідного стику;
- хоча б один абонент знаходиться у "блукаючому режимі", тобто входить у мережу через випадкові абонентські термінали (телефони у місцях випадкових відвідувань, таксофони).

Вказані варіанти висувають різні вимоги до апаратури захисту у частині виду сигналів обміну, способу підключення до лінії, масогабаритних показників і енергозабезпечення.

### 5.3.2. Вимоги до систем захисту мовних повідомлень для стаціонарних абонентів

Для стаціонарних абонентів може застосовуватися як апаратура зв'язку з вбудованими засобами захисту, так і різні приставки. Апаратура захисту повинна забезпечувати сумісність з усіма варіантами абонентного стику, які можуть застосовувати абоненти корпоративної захищеної мережі.

Під час безпосереднього їх підключення до двопровідного абонентського закінчення державної телефонної мережі проблема полягає лише у забезпеченні нормальної роботи в умовах доволі значного розкиду параметрів комутованих каналів. Методи виконання цього завдання відомі, а необхідна елементна і схемотехнічна бази доволі розвинені. У цьому випадку для побудови мережі достатньо мати один тип захисної апаратури.

Складнішим є завдання захисту абонентів, підключених через офісні АТС, абонентські лінії яких доволі різноманітні – від чотирипровідних

цифрових стандарту ISDN до двопровідних аналогових із різними значеннями імпедансу. У цьому випадку застосовувана апаратура захисту повинна забезпечувати адаптацію не лише до параметрів, але і до структури стику.

### 5.3.3. Вимоги до систем закриття мовних повідомлень для рухомих абонентів

Для рухомого абонента найвразливішою є ділянка радіовставки. З цього випливає постановка завдання захисту не усього каналу "від абонента до абонента", а лише радіоканалу. Такий варіант має ту перевагу, що захист забезпечується під час встановлення усіх зв'язків, а не тільки зв'язків з абонентами, що мають відповідну апаратуру захисту.

З іншого боку, впровадження захисту на ділянці радіоканалу вимагає застосування апаратури захисту у комплексі базової радіостанції, яка переважно не належить власникам корпоративної захищеної мережі. Необхідно враховувати, що така апаратура захисту повинна включатися на вході в радіоканал абонента, тобто комутаційна апаратура базової радіостанції повинна забезпечувати розпізнання абонента і управління апаратурою захисту.

Така організація захисту фактично нереальна, за винятком відомчих радіосистем рухомого зв'язку. Багато фірм, що надають радіодоступ до телефонних мереж, рекламують наявність захисту у каналі, проте якість її не підтверджена. Реальнішою і ефективнішою видається постановка завдання захисту усього каналу "від абонента до абонента", а не лише радіоканалу.

Переважно у корпоративній мережі захищеного зв'язку є не тільки рухомі абоненти. Більше того, кількість стаціонарних абонентів перевищує кількість рухомих. Тому важливою вимогою є сумісність апаратури захисту стаціонарного і рухомого абонента.

Підключення апаратури захисту каналу до рухомої радіостанції, по-перше, радикально відрізняється від підключення до стаціонарного терміналу, по-друге, не є стандартизоване і відрізняється для різних типів рухомих радіостанцій.

Рухомий режим висуває підвищені вимоги до масогабаритних і експлуатаційних параметрів апаратури захисту. Під час розміщення радіоапаратури в автомобілі або на іншому транспортному засобі ці вимоги відрізняються від вимог до офісної апаратури переважно за способом електроживлення і стійкості до механічних і кліматичних дій. За пішого режиму абонента на перший план виходять: вага, енергоспоживання, зручність розміщення і управління.

В апаратурі захисту каналу для "блукаючого абонента" повинні бути виконані вимоги сумісності із стаціонарною апаратурою, зручності транспортування у неробочому стані, простота переходу у робочий режим і можливість підключення до загальнодоступних телефонних апаратів без втручання в їх зовнішні і тим більше внутрішні з'єднання. Здебільшого допускається застосування стандартного роз'ємного підключення телефонного апарата до двопровідної лінії, але цей варіант, безумовно, не універсальний. Оптимальним видається застосування акустичного підключення до мікротелефонної трубки через накладені на неї мікрофон і телефон з доволі якісною зовнішньою звукоізоляцією.

Необхідно також враховувати, як вже згадувалося вище, що на відміну від державних систем захищеного зв'язку, де значну частину операцій зі встановлення зв'язку і обслуговування системи виконує спеціально навчений персонал, у цій корпоративній мережі усі основні операції виконує сам абонент у процесі інформаційного обміну, що визначає жорсткі вимоги до ергономіки апаратури.

## Питання для самоконтролю:

**1.** Якими є джерела загроз інформаційної безпеки абонентів телефонного зв'язку?

**2.** Якими є завдання захисту інформації на об'єктах із телефонним зв'язком та чим зумовлена їх специфіка?

**3.** Як виглядає завдання забезпечення конфіденційності на об'єктах із телефонним зв'язком?

**4.** Наведіть схему телефонних трактів, утворених на міських та міжміських з'єднаннях.

**5.** Який елемент телефонної мережі є найвразливішим з погляду інформаційної безпеки?

**6.** Які шляхи забезпечення захищеності обміну інформації в Україні можуть обирати абоненти?

**7.** У чому полягає особливість Державної системи урядового зв'язку України та які завдання вона виконує?

**8.** Для чого створена в Україні Національна система конфіденційного зв'язку?

**9.** Як досягається захищеність на мережах зв'язку загального користування?

**10.** Перерахуйте основні вимоги до систем закриття мовної інформації у телефонних каналах.

**11.** Які вимоги ставляться до систем закриття мовних повідомлень для рухомих і стаціонарних абонентів?

# Розділ 6

# МЕТОДИ І ЗАСОБИ НЕСАНКЦІОНОВАНОГО ОДЕРЖАННЯ ІНФОРМАЦІЇ ІЗ ТЕЛЕФОННИХ ЛІНІЙ

Чим більше знаємо про супротивника та його озброєння, тим надійніший та ефективніший захист можемо створити. Більше того, напевне, взагалі не вдасться вибудувати захист, нічого не знаючи про загрози. У цьому контексті фахівцям із захисту інформації важливо знати технічні характеристики засобів технічної розвідки та способи їх застосування потенційними зловмисниками.

У результаті вивчення цього розділу студент повинен знати:

- будову, різновиди та основні технічні характеристики засобів технічної розвідки, які можуть використовуватися на телефонних лініях та найімовірніші місця їх встановлення;
- способи застосування закладок для перехоплення телефонних повідомлень;
- фізичну суть "мікрофонного ефекту" і "високочастотного нав'язування", а також варіанти використання цих явищ у засобах технічної розвідки;
- особливості застосування виносних мікрофонів для прослуховування розмов у приміщеннях;
- причини виникнення небезпечних сигналів у телефонних лініях та принципи безконтактного знімання інформації.

## 6.1. Принципи побудови та класифікація засобів технічної розвідки, які використовуються у телефонних лініях

***Засоби технічної розвідки*** (ЗТР) можуть використовуватися як для перехоплення телефонних розмов, так і для прослуховування приміщень, де розташований телефонний апарат, тому їх часто називають ***телефонними закладками***. На рис. 6.1 показано узагальнену структуру телефонних закладок, а на рис. 6.2 – їх класифікацію.

Основою ЗТР є телефонний адаптер, що забезпечує знімання сигналу із АТЛ. Наступним важливим елементом є вузол опрацювання сигналу, до функцій якого належить виділення інформативного сигналу та тлі різного роду

перешкоджаючих чинників та його підсилення до рівня, придатного для подальшого використання.

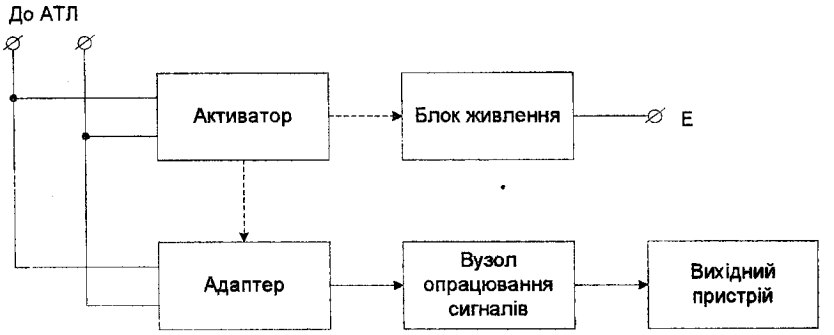



*Рис. 6.1. Узагальнена структура ЗТР, призначених для використання в АТЛ*

Телефонні закладки переважно виконуються у вигляді окремого модуля або камуфлюються під елементи телефонного апарата, наприклад, конденсатор, телефонну або мікрофонну капсули, телефонний штекер, розетку тощо (див. Додаток 1). Телефонні закладки мають невеликі розміри (об'єм від одного до кількох $см^3$) і вагу від 10 до 70 г. Наприклад, телефонна закладка HKG-3122 має розміри 33×20×12 мм, а SIM-A64 – 8×6×20 мм.

У телефонних закладках можливі такі способи використання перехоплених сигналів:

- прослуховування розмови у реальному часі;
- запис розмовного сигналу;
- ретрансляція сигналу за межі контрольованої зони.

Для прослуховування використовується перетворювач електричного сигналу в акустичний, для запису – пристрій фіксації мовного сигналу на магнітну стрічку чи флеш-пам'ять, а для ретрансляції – радіопередавач, що реалізує випромінювання перехоплених з телефонної лінії сигналів в ефір з подальшим їх прийомом на радіоприймач. Для приховування радіоканалу можуть використовуватися спеціальні формати кодування та модуляції, зокрема технологія шумоподібних сигналів.


*Рис. 6.2. Класифікація телефонних закладок*

Живлення телефонних закладок може здійснюватися двояко – безпосередньо від АТЛ або від автономного джерела. У першому варіанті блок живлення реалізується у вигляді спеціального узгоджувального пристрою і забезпечує фактично необмежений термін дії, хоч може бути виявлений за ознакою додаткового навантаження АТЛ. Другий варіант має протилежні властивості.

Для заощадження ресурсу автономних джерел живлення та маскування ЗТР до їх складу включають спеціальні пристрої-активатори. Їхня робота може ґрунтуватися на аналізі стану телефонної лінії (активація ЗТР відбувається після піднесення трубки) або на детектуванні розмовного сигналу в АТЛ.

Залежно від способу підключення до абонентських телефонних ліній розрізняють ***безконтактні та контактні*** ЗТР. Контактні ЗТР, своєю чергою, бувають ***послідовного і паралельного*** типів.

За цією класифікаційною ознакою передусім визначається тип телефонного адаптера. Так, безконтактний адаптер може бути виготовлений у вигляді індуктивного знімача, який у найпростішому варіанті являє собою навиту на розрізане феритове кільце котушку. При охопленні кільцем АТЛ відбувається перетворення електромагнітних коливань, створених проходженням розмовного струму лінією в електричні коливання, що після підсилення надходять на пристрій відтворення чи запису (див. Додаток 1).

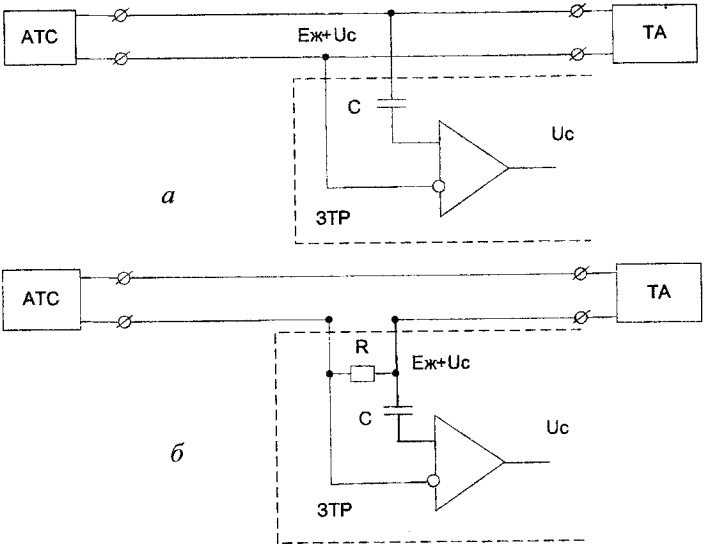



*Рис. 6.3. Паралельне (а) та послідовне (б) підключення ЗТР до АТЛ*

Безконтактні ЗТР неможливо виявити вимірюванням електричних параметрів телефонної лінії, але якість відтворення чи запису на диктофон не дуже

висока через чутливість індуктивного знімача до різних електромагнітних перешкод. Контактні адаптери мають гальванічний контакт із телефонною лінією і тому здатні забезпечити значно вищу якість.

Паралельний адаптер підключається до лінії паралельно і відрізняється високим вхідним опором і малою вхідною ємністю, що утруднює його виявлення (рис. 6.3, *а*). Послідовний адаптер включається у розрив одного із проводів телефонної лінії (рис. 6.3, *б*) і має вхідний опір в кілька сотень Ом і значну вхідну ємність, що полегшує його виявлення.

На рис. 6.4 показано схему паралельного ЗТР, причому роль адаптера виконує реле.

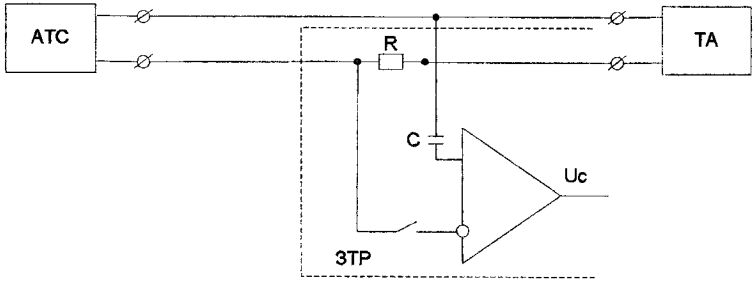



*Рис. 6.4. Використання реле у ролі активатора паралельного ЗТР*

Існує спосіб перехоплення телефонних переговорів, що реалізує випромінювання сигналів з телефонної лінії в ефір з подальшим їх прийманням на радіоприймач.

## 6.2. Найімовірніші місця встановлення телефонних закладок

На рис. 6.5 показано структурно-топологічну схему загроз для абонентської телефонної лінії із зазначенням місць найімовірнішого встановлення телефонних закладок із зазначенням їх типів.

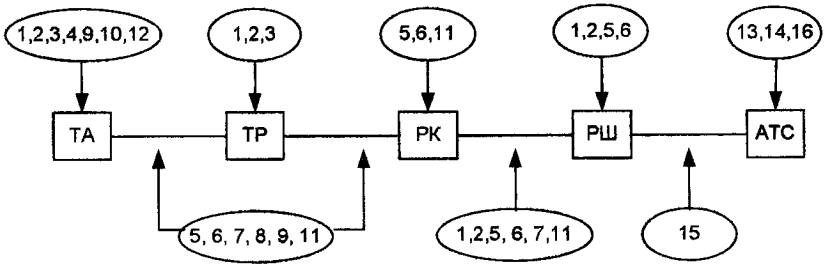



*Рис. 6.5. Структурно-топологічна схема загроз для абонентської телефонної лінії*

На схемі номери означають такі загрози: 1 – радіозакладка паралельного підключення; 2 – радіозакладка послідовного підключення; 3 – комбінована телефонно-акустична радіозакладка; 4 – закладка типу "телефонне вухо"; 5 – низькоомний адаптер; 6 – високоомний адаптер; 7 – безконтактний адаптер; 8 – наводки телефонного сигналу на інші кола; 9 – "мікрофонний ефект"; 10 – ВЧ-випромінювання телефонного сигналу; 11 – високочастотне нав'язування; 12 – радіовипромінювання телефонного продовжувача; 13 – зняття інформації на АТС; 14 – перехоплення інформації по лінії зв'язку; 15 – складна високочутлива апаратура; 16 – витік інформації по лініях відведення від АТС (позавідомча охорона).

## 6.3. Застосування закладок для перехоплення телефонних повідомлень

Конфіденційна інформація дуже часто передається телефонними комунікаціями, що пов'язано з оперативністю і зручністю використання цього виду зв'язку. Тому перехоплення телефонних переговорів дуже результативне з погляду несанкціонованого знімання інформації.

Найпростішим і до того ж найпоширенішим способом перехоплення телефонних переговорів є підслуховування через паралельний телефон. Виявити факт підслуховування із паралельного телефонного апарата також доволі просто, оскільки під час підняття трубки паралельного телефону в лінії додатково спадає напруга та зменшується гучність розмовного сигналу у

трубці основного телефонного апарата. Крім того, можливе стороннє підзвонювання, що викличе підозру користувача штатного телефонного апарата.

Дуже зручним способом перехоплення конфіденційних телефонних переговорів є ***запис на диктофон***. Якщо у диктофоні є режим "акустозапуск", запис відбувається лише в моменти часу, коли у лінії наявний розмовний сигнал. Для під'єднання входу диктофона до телефонної лінії використовується додатковий пристрій – телефонний адаптер.

Найпоширенішим способом перехоплення телефонних розмов є використання телефонних радіозакладок. Паралельні телефонні радіопередавачі підключаються паралельно до телефонної лінії. Включення радіопередавача відбувається під час падіння напруги на лінії, споживаний струм 3...5 мА. Послідовні телефонні радіопередавачі включаються як і послідовний знімач у розрив одного з проводів телефонної лінії. Відрізняються більшою потужністю випромінювання порівняно із паралельними передавачами, але їх легше виявити під час перевірки телефонної лінії пошуковими пристроями.

Телефонні радіопередавачі з індуктивним знімачем належать до групи радіопередавачів з автономним живленням і зустрічаються частіше від інших телефонних радіопередавачів із групи з автономним живленням. Потужність випромінювання та час роботи залежать від елементів живлення.

Комбінований телефонний радіопередавач – це пристрій, який переважно підключається до телефонної лінії паралельно, живиться від телефонної лінії, за покладеної слухавки передається акустична інформація з приміщення, а після підняття слухавки радіопередавач переходить у режим трансляції телефонних повідомлень, що проходять цією лінією.

Радіопередавачі із живленням від телефонної лінії мають фактично необмежений термін служби, але їх легше виявити порівняно із радіопередавачами, що мають автономне живлення, але відповідно обмежений термін роботи.

## 6.4. Способи використання засобів телефонного зв'язку для прослуховування приміщень

### 6.4.1. Перехоплення сигналів "мікрофонного ефекту"

***Мікрофонний ефект*** є побічним явищем, яке проявляється у небажаному паразитному перетворенні акустичних звукових коливань в електричні

сигнали елементами телефонного апарата чи інших технічних засобів. Телефонний апарат містить кілька елементів, здатних перетворювати акустичні коливання в електричні. До них насамперед належать дзвінкове коло, мікрофонна і телефонна капсули. За рахунок акустоелектричних перетворень у цих елементах виникають інформаційні (небезпечні) сигнали. Крім того, корпус апарата є додатковим резонуючим пристроєм.

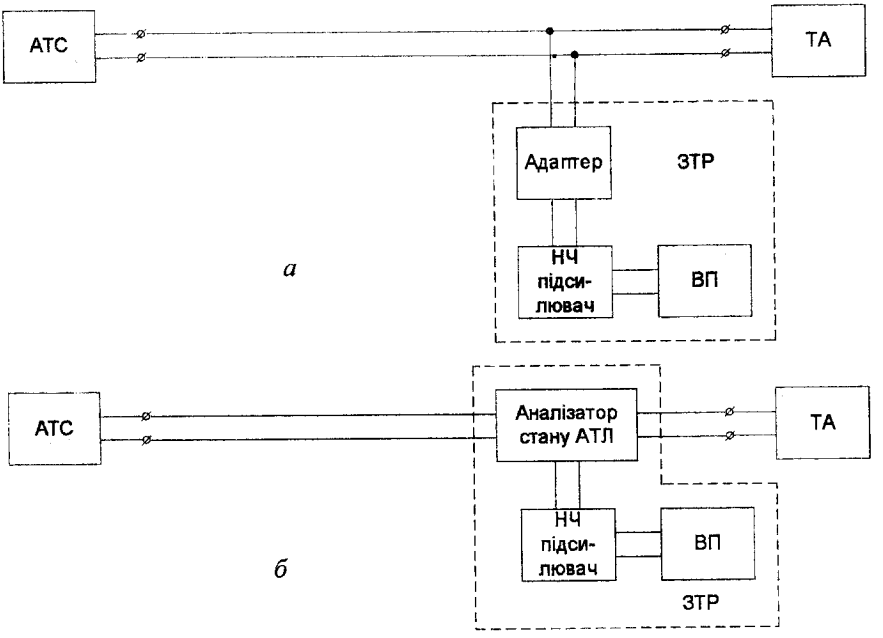



*Рис. 6.6. Варіанти реалізації ЗТР, що використовують "мікрофонний ефект": а – підключення АТЛ через адаптер; б – підключення АТЛ через аналізатор стану АТЛ*

За покладеної трубки до абонентської телефонної лінії підключені лише елементи дзвінкового кола, а телефонна і мікрофонна капсули гальванічно відключені. Отже, в телефонному апараті найвірогіднішим і найнебезпечнішим (з погляду рівня небезпечного сигналу) джерелом мікрофонного ефекту є електромагнітний дзвінок. Такий електромеханічний перетворювач має властивість дуальності, тобто перетворює не лише електричні сигнали у механічні коливання, але й, навпаки, через коливання якоря дзвінка, зумовленого дією

акустичних коливань в його обмотці, розташованій в полі постійного магніту, за законом Фарадея виникає електрорушійна сила електромагнітної індукції. Дослідження показали, що амплітуда ЕРС, що наводиться в лінії, для деяких типів телефонних апаратів може досягати кількох мілівольт.

Перехоплення інформаційних сигналів, що виникають в елементах дзвінкового кола, можливе гальванічним підключенням до телефонної лінії спеціальних високочутливих низькочастотних підсилювачів (рис. 6.6, *а*). Проте внаслідок малої амплітуди сигналів дальність перехоплення інформації, як правило, не перевищує кількох десятків метрів.

Для підвищення дальності перехоплення інформації низькочастотний підсилювач підключають до лінії через пристрій аналізу стану телефонної лінії, що включається у розрив телефонної лінії (рис. 6.6, *б*). Цей пристрій під час покладеної трубки телефонного апарата відключає лінію від АТС (опір розв'язки становить більше 20 МОм), підключає спеціальний низькочастотний підсилювач і переходить у режим аналізу підняття слухавки і наявності сигналів виклику. Під час одержання сигналів виклику або підняття слухавки пристрій відключає спеціальний низькочастотний підсилювач і підключає телефонний апарат до лінії АТС.

Унаслідок відключення телефонного апарата від лінії у момент знімання інформації значно зменшується рівень шумів у лінії, і отже, підвищується дальність перехоплення інформації.

### 6.4.2. Використання високочастотного нав'язування

Для істотного збільшення дальності перехоплення інформації використовують метод ***високочастотного нав'язування***, зміст якого ілюструє рис. 6.7. За високочастотного нав'язування елементи телефонного апарата виконують роль не тільки акустоелектричних перетворювачів, але також і амплітудного модулятора. Джерелом несучого гармонічного коливання (сигналом високочастотного нав'язування) є високочастотний генератор, а демодуляція і виділення інформативного сигналу із відбитого від неузгодженого навантаження здійснюється вузлом опрацювання сигналів. Отже, абонентською телефонною лінією передається не слабкий небезпечний інформативний сигнал, а модульований сигнал, рівень якого достатній для перехоплення у пункті приймання, тому дальність перехоплення інформації під час використання методу

"високочастотного нав'язування" може становити кілька сотень метрів. Частота несучого коливання значно вища від звукового діапазону (від 100 кГц до 1 МГц), тому факт високочастотного нав'язування не вдається встановити на слух.

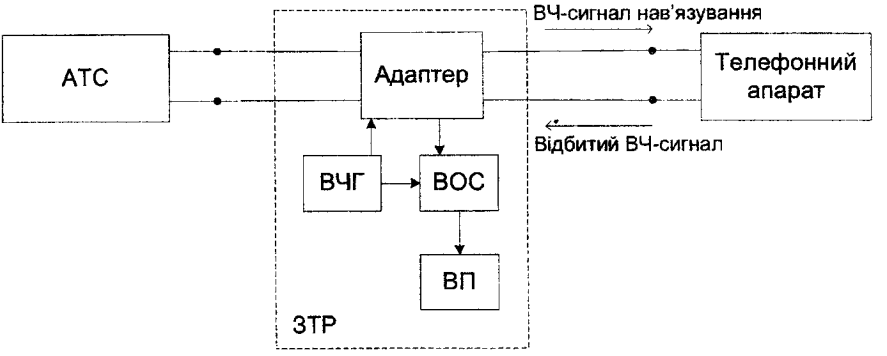



*Рис. 6.7. Схема реалізації методу високочастотного нав'язування*

Існують два варіанти реалізації методу високочастотного нав'язування – послідовний і паралельний. Під час застосування цього методу у послідовному варіанті в один із проводів телефонного кабелю стосовно деякого спільного провідника (наприклад, проводу заземлення чи труби опалення) вводиться високочастотний гармонічний сигнал (рис. 6.8, *а*). Високочастотне коливання, проходячи через елементи дзвінкового кола телефонного апарата, модулюється акустичним сигналом. У такий спосіб електромагнітний дзвінок виконує роль самовільного амплітудного модулятора, а високочастотне коливання – несучої модульованого сигналу. Приймальна частина приладу підключається до іншого проводу телефонного кабелю та спільного провідника. Амплітудний детектор дає змогу отримати низькочастотну огинаючу для подальшого підсилення і запису. Не пов'язані електрично, але близько розташовані елементи конструкції телефонного апарата, за рахунок явища електромагнітної індукції проводять високочастотні сигнали. Для якісної роботи подібного пристрою потрібно зменшувати взаємний індуктивний вплив проводів, тому подача у лінію високочастотного коливання та приймання промодульованого сигналу здійснюються екранованим кабелем.

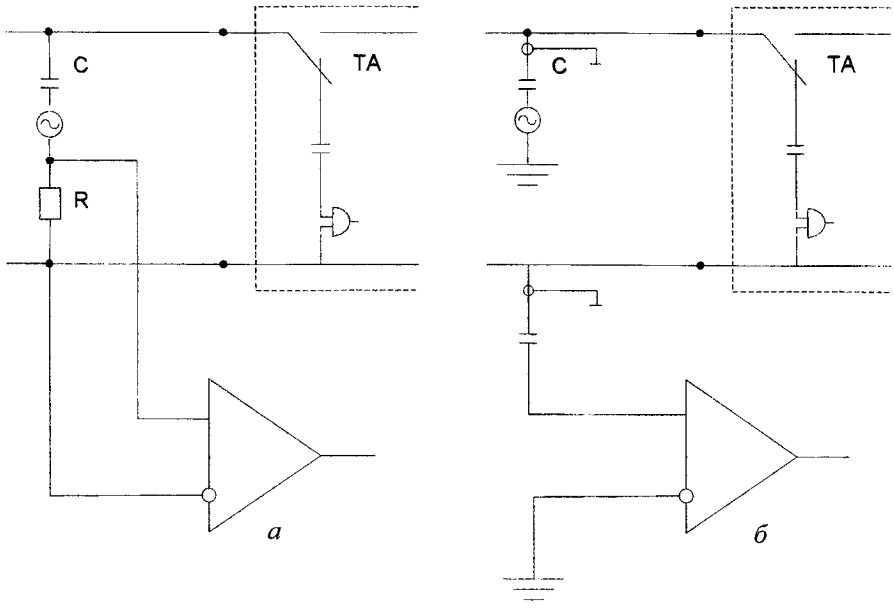



*Рис. 6.8. Реалізація ВЧ-нав'язування у варіанті "накачки"(а) та "підкачки"(б)*

Зміст методу високочастотного нав'язування у паралельному варіанті (високочастотна "накачка") полягає у такому. Завдяки високій частоті сигнал "накачки" може проходити не лише у дзвінкове коло, але й у мікрофонне і телефонне кола та модулюватися інформаційним сигналом, що виникає внаслідок акустоелектричних перетворень. Оскільки нелінійні або параметричні елементи телефонного апарата для високочастотного сигналу, як правило, є неузгодженим навантаженням, промодульований мовним сигналом високочастотний сигнал відбиватиметься від нього і поширюватиметься у зворотному напрямку по лінії. Далі відбитий високочастотний сигнал приймається й опрацьовується спеціальним приймальним пристроєм, що також підключений до телефонної лінії (рис. 6.8, *б*). Пристрій аналізу стану телефонної лінії виконує функції, розглянуті вище.

### 6.4.3. Прослуховування приміщень за допомогою виносних мікрофонів

Поряд із розглянутими електроакустичними каналами витоку інформації для прослуховування розмов у приміщеннях застосовуються спеціальні телефонні закладки, які ще називаються ***виносними мікрофонами***. Зрозуміло, що встановлення таких пристроїв вимагає фізичного доступу у приміщення.

Типовий електронний пристрій перехоплення інформації включає: мікрофон, мікрофонний підсилювач, електронний комутатор і пристрій аналізу стану телефонної лінії (рис. 6.9).

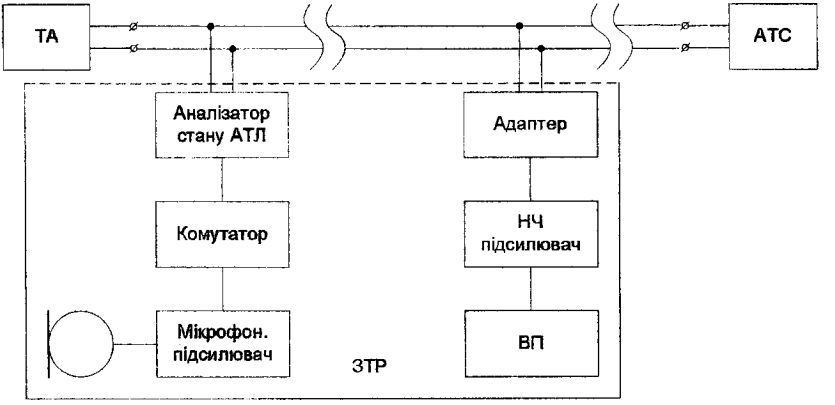



*Рис. 6.9. Схема мікрофонної провідної системи, яка використовує для передачі інформації телефонну лінію*

Телефонні закладки можуть заживлюватися від телефонної лінії або мати автономне живлення. Під час живлення від телефонної лінії термін їхньої служби фактично необмежений, але їх легше знайти через додаткове споживання струму і внесення додаткового опору. Виносні мікрофони з автономним живленням складніше виявляти і вони можуть працювати, крім телефонних ліній, так само на лініях пожежно-охоронної сигналізації, але термін їхньої служби обмежений ємністю елементів живлення.

Принцип роботи виносних мікрофонів простий: якщо на телефонному апараті покладена трубка (на лінії висока напруга), виносний мікрофон сприй-

має акустичні коливання у приміщенні і передає їх на лінію. Приймання сигналу можливе вздовж усієї траси АТЛ від телефону до АТС. Для приймання сигналів можна використати підключений паралельно до телефонної лінії підсилювач з великим вхідним опором. Під час зняття трубки на телефонному апараті чи під час надходження на телефонний апарат сигналу виклику від АТС, виносний мікрофон припиняє передачу сигналів на телефонну лінію й очікує звільнення лінії (відкладення слухавки).

Спільною особливістю виносних мікрофонів є те, що вони передають інформацію телефонними лініями без випромінювання в ефір. Залежно від виду передаваного сигналу розрізняють:

- виносні мікрофони з передачею сигналу у звуковому діапазоні;
- виносні мікрофони, що використовують модуляцію несучої частоти;
- виносні мікрофони, які передають інформацію у кодованому вигляді;
- виносні мікрофони з активацією і використанням телефонної лінії у стандартному режимі.

Виносний мікрофон з передачею сигналу у звуковому діапазоні містить мікрофонний підсилювач, пристрій узгодження з телефонною лінією і модуль перевірки стану телефонної лінії. Якщо на телефонному апараті покладена трубка (на лінії висока напруга) виносний мікрофон сприймає акустичні коливання у приміщенні і після відповідного підсилення безпосередньо передає їх у лінію. Для приймання сигналів достатньо використати підсилювач із великим вхідним опором, підключений паралельно до телефонної лінії. Під час зняття трубки на телефонному апараті, чи під час надходження на телефонний апарат сигналу виклику від АТС, виносний мікрофон припиняє передачу сигналів на телефонну лінію й очікує відновлення стану лінії "трубка покладена".

У виносному мікрофоні з модуляцією несучої частоти сигнал з виходу мікрофонного підсилювача надходить на модулятор з несучою в діапазоні від 20 кГц до 10 Мгц. Може використовуватися амплітудна модуляція або вузькосмугова частотна модуляція як стійкіша до перешкод у каналі поширення. Особливістю цього методу є те, що за паралельного підключення виносного мікрофона акустична інформація з приміщення може передаватися не тільки за покладеної трубки на телефонному апараті, але і під час розмови на цій телефонній лінії.

Особливістю виносних мікрофонів з кодуванням є те, що акустична інформація з виходу мікрофонного підсилювача обробляється за певним алгоритмом, зокрема і перетворенням у цифрову форму, що запобігає її перехопленню прямим прослуховуванням лінії. До цієї самої групи можна зарахувати пристрої, що накопичують інформацію, а потім швидко передають її по команді приймача чи у визначений час.

Найдосконалішими засобами техрозвідки для прослуховування приміщень є виносні мікрофони з активацією і використанням телефонної лінії у стандартному режимі. Такі пристрої ще називають монітором приміщення по телефонній лінії, або "***телефонним вухом***". Встановлюється пристрій між телефонним апаратом і АТЛ, а тому контролює сигнали від АТС. З метою прослуховування приміщення здійснюється активація монітора через телефонну мережу.

Активація пристрою "телефонне вухо" відбувається за таким алгоритмом:

- набір номера телефону абонента, приміщення якого прослуховується;
- утримування АТЛ у режимі виклику обмежене при цьому монітор блокує надходження кількох перших імпульсів виклику (гудків) на телефонний апарат;
- завчасна відмова виклику до піднесення слухавки, наприклад, після трьох гудків;
- поновний набір номера і очікування спрацювання монітора (підключення виносного мікрофона до АТЛ);
- передача звукової інформації на телефон, з якого проводиться активація.

Отже, з погляду роботи АТС робота монітора відбувається у стандартному режимі телефонної розмови. Прослуховування приміщення відбувається через мікрофон монітора з передачею у канал зв'язку, тобто відбувається "віртуальне" підняття слухавки.

Монітор є "прозорим" для звичайних дзвінків, хоча привносить певну затримку на етапі встановлення з'єднання внаслідок "проковтування" кількох перших імпульсів виклику. Практика показує, що такий алгоритм забезпечує високий рівень маскування монітора і ускладнює виявлення факту його встановлення.

## 6.5. Перехоплення побічних електромагнітних сигналів випромінювання і наведень

Конструктивно-технологічною особливістю будови симетричних телефонних кабелів є попарна скрутка ізольованих проводів між собою з подальшим повивом таких пар для безпосереднього упакування проводів у зовнішні кабельні ізоляційно-захисні шари.

Навколо скрученої пари лінії створюється магнітне поле, а напрям силових ліній визначається за правилом "правого гвинта". Якщо силові лінії магнітного поля замкнути через сердечник з котушкою (рамкою), то на кінцях котушки виникне електрорушійна сила (рис. 6.10).

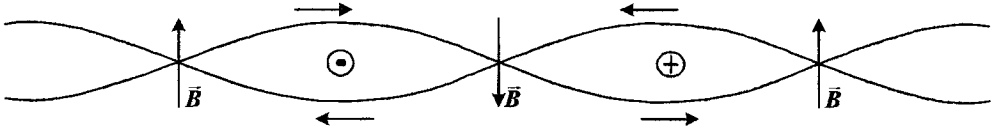



*Рис. 6.10. Скрутка однієї пари проводів телефонного кабелю*

Для ефективного наведення ЕРС магнітопровід з котушкою доцільно розташувати вздовж скрученої лінії, причому довжина магнітопроводу має дорівнювати половині кроку скрутки лінії ***L***, а для наближення полюсів магнітопроводу до лінії доцільно використати сердечник П-подібної форми (рис. 6.11).

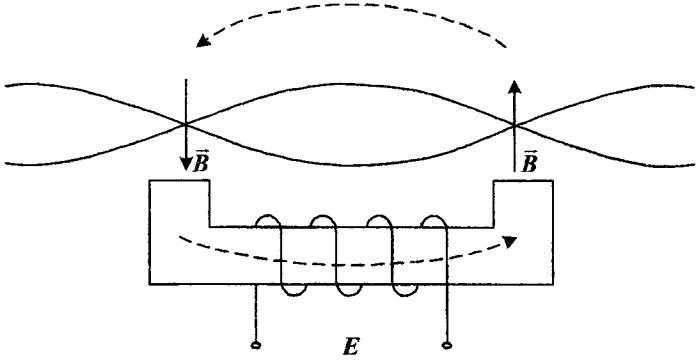



*Рис. 6.11. Узгодження довжини магнітопроводу з кроком скрутки*

Для підвищення чутливості та завадостійкості використовують диференціальну схему індуктивного давача (рис. 6.12).

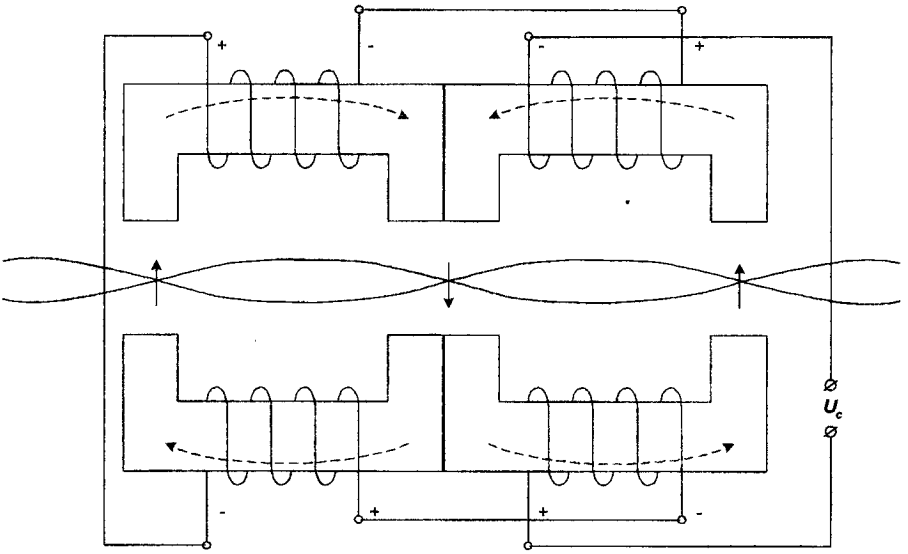



*Рис. 6.12. Схема індуктивного давача для дослідження побічного електромагнітного випромінювання витоку телефонних кабелів*

Як випливає із рисунка, напрям вектора магнітної індукції змінюватиметься на протилежний з інтервалом ***L/2*** і тому розташовану поряд котушку слід увімкнути зустрічно-послідовно. За такого включення ЕРС двох котушок від магнітного поля, створеного витою парою, додається тоді, як ЕРС, зумовлена дією завад, буде взаємно компенсуватися, що позитивно позначається на завадостійкості давача. Для збільшення рівня сигналу давача на протилежному боці кабелю використано додаткове плече давача, що замикає магнітні силові лінії. Котушки нижньої частини давача є дзеркальним відображенням верхньої.

## Питання для самоконтролю:

**1.** Опишіть узагальнену структуру засобів технічної розвідки, що призначені для використання на АТЛ.

**2.** Наведіть класифікацію телефонних закладок із зазначенням класифікаційних критеріїв.

**3.** Охарактеризуйте можливі способи використання перехоплених сигналів у телефонних закладках.

**4.** Які принципи можуть бути використані для продовження терміну роботи та підвищення скритності телефонних закладок?

**5.** Вкажіть на специфіку підключення до АТЛ паралельних, послідовних та безконтактних телефонних закладок і проілюструйте це відповідними схемами.

**6.** Покажіть на схемі, як можна використати реле як активатор паралельної телефонної закладки.

**7.** Наведіть найімовірніші місця встановлення телефонних закладок.

**8.** Опишіть варіанти застосування телефонних закладок для перехоплення телефонних повідомлень.

**9.** Охарактеризуйте технічні канали витоку інформації на основі "мікрофонного ефекту" та "високочастотного нав'язування".

**10.** Чому збільшується дальність прослуховування приміщення під час використання "високочастотного нав'язування"?

**11.** Дайте порівняльну характеристику та наведіть схеми для реалізації високочастотного нав'язування у варіанті "накачки" та "підкачки".

**12.** Охарактеризуйте способи прослуховування приміщень за допомогою виносних мікрофонів.

**13.** Опишіть алгоритм активації телефонних закладок типу "телефонне вухо" для прослуховування приміщень.

**14.** Поясніть фізичні засади та технічну реалізацію пристроїв, що здійснюють перехоплення телефонних повідомлень через побічні електромагнітні випромінювання.

**15.** Поясніть, як у диференціальній схемі індуктивного давача досягається підвищення чутливості та завадостійкості.

# Розділ 7

# ЗАСОБИ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ МІСЦЬ КОНТАКТНИХ ПІДКЛЮЧЕНЬ ЗАСОБІВ ТЕХНІЧНОЇ РОЗВІДКИ У ТЕЛЕФОННИХ ЛІНІЯХ

Загрози інформаційній безпеці абонентів телефонних мереж загального користування найчастіше реалізуються через контактні підключення засобів технічної розвідки до абонентських телефонних ліній. Подібне підключення змінює параметри АТЛ, що можна використати до виявлення факту несанкціонованих підключень чи сторонніх впливів на лінію. Хоча засоби виявлення і локалізації місць несанкціонованих підключень не є самодостатніми для захисту засобів і каналів телефонного зв'язку, але ознайомлення з принципами їх роботи та технічними характеристиками є корисним для глибшого розуміння проблематики інформаційної безпеки у телефонії.

У результаті вивчення цього розділу студент повинен знати:

- основні методи і засоби, які можуть бути використані для виявлення і локалізації засобів технічної розвідки на ділянці абонентської телефонної лінії;
- моделі АТЛ для постійного струму у режимі "Очікування" та "Розмова", співвідношення, що описують роботу пристроїв контролю напруги живлення АТЛ та струму короткого замикання;
- зміст методу контролю навантажувальної характеристики АТЛ та принцип дії пристроїв контролю сигналів у телефонній лінії та радіоефірі;
- повну та спрощену електричні схеми заміщення знеструмленої "чистої" абонентської телефонної лінії, а також еквівалентні схеми, що відображають різні способи підключення телефонних закладок;
- зміст методів та принцип дії пристроїв контролю вольт-амперної характеристики, Лісажа-характеристики, перехідної характеристики;
- принципи роботи імпульсних рефлектомірів та їх застосування для виявлення та локалізації несанкціонованих підключень до АТЛ.

## 7.1. Класифікація методів виявлення несанкціонованих підключень до абонентських телефонних ліній

Методи виявлення несанкціонованих підключень до абонентських телефонних ліній ґрунтуються на тому, що безпосереднє підключення до них

сторонніх пристроїв (засобів технічної розвідки, "піратських" телефонних апаратів тощо) викликає зміну електричних параметрів ліній, насамперед напруги, струму, а також імпедансу. Крім того, працюючі телефонні закладки передають телефонними лініями чи випромінюють в ефір сигнали, тому можна використовувати методи, які забезпечують їх виявлення та ідентифікацію.

На рис. 7.1 показано класифікацію методів, які придатні для виявлення несанкціонованих підключень до АТЛ. Ці методи доцільно поділити на дві групи:

- які контролюють параметри АТЛ у робочому стані;
- які вимагають відключення АТЛ від АТС (знеструмлення АТЛ).


*Рис. 7.1. Класифікація методів, що використовуються для виявлення несанкціонованих підключень до АТЛ*

## 7.2. Контроль абонентських телефонних ліній у робочому стані

Засоби контролю АТЛ у робочому стані можуть бути виконані як "сторожові" (працюють увесь час), так і "пошукові" (застосовуються лише під час пошукових робіт).

Абонентська телефонна лінія у робочому стані може перебувати у двох режимах – "Очікування" (розімкнений шлейф) та "Розмова" (замкнений шлейф). На рис. 7.2 показано еквівалентні електричні схеми АТЛ на постійному струмі для двох зазначених режимів.

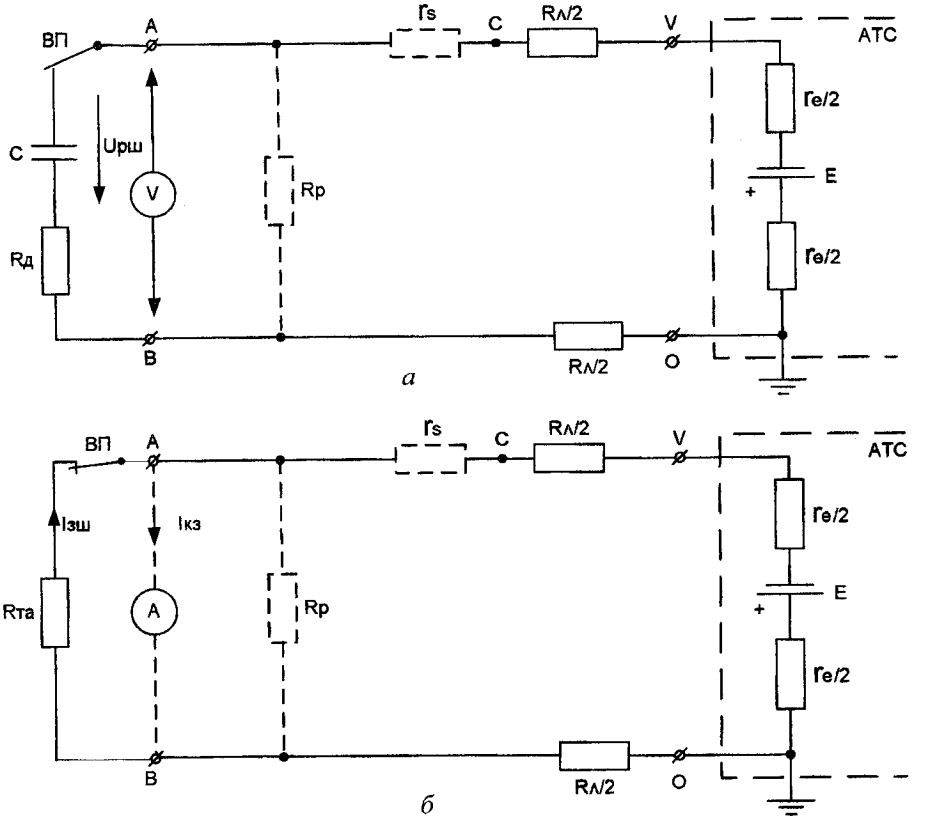



*Рис. 7.2. Модель АТЛ для постійного струму у режимі "Очікування" (а) та "Розмова" (б)*

Опір абонентської телефонної лінії залежить від її довжини та діаметра жил. Як типове можна прийняти значення опору АТЛ на постійному струмі 2 кОм. На тлі опору лінії $R_L$ можна знехтувати внутрішнім опором центральної батареї АТС $r_E << R_L$. Оскільки опір розмовної частини телефонного апарата $R_{TA}$ становить приблизно 500 Ом, а напруга центральної батареї – 60 В, то струм замкненого шлейфу – 25 мА.

На рис. 7.2 пунктиром показано підключення паралельної телефонної закладки (опір $R_P$) та послідовної телефонної закладки (опір $r_S$).

### 7.2.1. Контроль напруги живлення АТЛ

Найінформативнішим і легко вимірюваним параметром телефонної лінії є напруга живлення: для більшості міських АТС – це 60 В за покладеної трубки та 8–12 В (залежно від моделі телефонного апарата) – за знятої. Але ці параметри можуть змінюватися через стан атмосфери, пори року, погані контакти тощо.

Пристрої, які реалізують цей метод, визначають факт підключення до АТЛ за зміною напруги живлення, порівняно із деяким "еталонним" значенням, одержаним на "чистій" лінії (за відсутності пристроїв несанкціонованого знімання інформації).

У пошуковому режимі роботи телефонний апарат відключається, а АТЛ навантажується на еталонний резистор, на якому вимірюється спад напруги. Якщо зміна напруги на цьому опорі, зумовлена несанкціонованим підключенням, перевищує встановлений пороговий рівень, пристрій видає сигнал тривоги (звуковий чи світловий).

У сторожовому режимі здійснюється неперервне вимірювання напруги живлення на затискачах "А" і "В" телефонної розетки (рис. 7.2).

Напруга на "чистій" лінії у режимі "Очікування":

$$U_{AB} = U_{PШ} \approx E = 60\,B,$$

а в режимі "Розмова":

$$\bar{U}_{AB} = U_{ЗШ} = E\frac{R_{TA}}{R_L + R_{TA}} = 12\,B.$$

За наявності паралельного підключення пристрою з опором $R_P = 10\ кОм$ напруга на затискачах "А" і "В" у режимі "Очікування":

$$U^*_{AB} = U_{РШ} = E\frac{R_P}{R_L + R_P} = \frac{E}{1 + R_L/R_P} = 50\ В,$$

а в режимі "Розмова":

$$\bar{U}^*_{AB} = U_{ЗШ} = E\frac{R_{TA} \| R_P}{R_L + R_{TA} \| R_P} = \frac{E}{1 + R_L\left(1 + R_{TA}/R_P\right)/R_{TA}} = 11{,}5\ В.$$

Підключення паралельних телефонних закладок зумовлює зміну напруги на затискачах "А" і "В" у режимі "Очікування":

$$\Delta U_{AB} = U^*_{AB} - U_{AB} = -10\ В \text{ (зменшення на 17 \%)},$$

а в режимі "Розмова":

$$\Delta \bar{U}_{AB} = \bar{U}^*_{AB} - \bar{U}_{AB} = -0{,}5\ В \text{ (зменшення на 4,2 \%)}.$$

За наявності послідовного підключення пристрою з опором $r_S = 100\ Ом$ напруга на затискачах "А" і "В" в режимі "Очікування":

$$U^*_{AB} = U_{РШ} = E = 60\ В,$$

а в режимі "Розмова":

$$\bar{U}^*_{AB} = U_{ЗШ} = E\frac{R_{TA}}{R_L + r_S + R_{TA}} \approx 11{,}5\ В.$$

Отже, підключення послідовних телефонних закладок зумовлює зміну напруги на затискачах "А" і "В" в режимі "Очікування":

$$\Delta U_{AB} = U^*_{AB} - U_{AB} \approx 0 \text{ (без змін)},$$

а в режимі "Розмова":

$$\Delta \bar{U}_{AB} = \bar{U}^*_{AB} - \bar{U}_{AB} = -0{,}5\ В \text{ (зменшення на 4,2 \%)}.$$

Як бачимо, метод контролю напруги живлення АТЛ у режимі "Очікування" дає змогу виявляти лише паралельні телефонні закладки, а в режимі "Розмова" – паралельні та послідовні.

Основними недоліками засобів контролю, що реалізують цей метод, є:

- потреба налаштування приладу під час першого підключення на "чистій" лінії для реєстрації "еталонного" значення напруги (перевірка на "чистоту" потребує використання інших методів контролю);

- вимога перелаштування пристрою, що працює у сторожовому режимі, під час заміни телефонного апарата;
- висока вірогідність помилкових спрацьовувань пов'язана із дрейфом параметрів абонентських телефонних ліній.

Пристрої контролю напруги живлення АТЛ, що працюють у сторожовому режимі, називаються ***індикаторами***, або ***аналізаторами*** стану телефонних ліній. До сертифікованих в Україні пристроїв цього класу належить аналізатор "Скеля 1А". Деякі пристрої захисту телефонних розмов ("Барьер-3", "Аккорд-200" та ін.) постійно висвітлюють значення напруги в лінії, а різка її зміна повинна насторожувати.

### 7.2.2. Контроль струму короткого замикання АТЛ

У телефонних лініях можливе вимірювання струму короткого замикання. Для цього затискачі "А" і "В" з'єднуються між собою і амперметром вимірюється струм шлейфа $I_{КЗ}$.

Струм короткого замикання на "чистій" лінії дорівнює

$$I_{КЗ} = \frac{E}{R_L} = 30\ мА,$$

а на лінії із послідовно включеною закладкою:

$$I^*_{КЗ} = \frac{E}{R_L + r_S} \approx 28{,}5\ мА.$$

Зміна струму, зумовлена таким підключенням, становить

$$\Delta I = I^*_{КЗ} - I_{КЗ} = -1{,}5\ мА \text{ (зменшення на 5 \%)}.$$

Отже, метод контролю струму короткого замикання придатний до використання у сторожовому режимі для виявлення лише послідовних телефонних закладок.

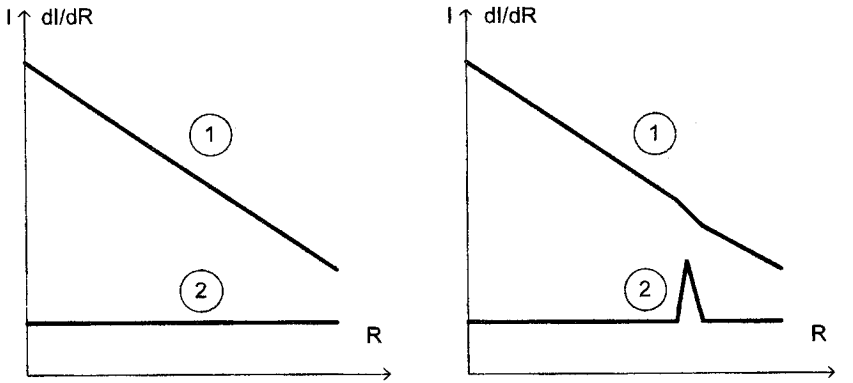
Варіантом контролю струму короткого замикання є вимірювання опору шлейфа, оскільки

$$R_{Ш} = \frac{E}{I_{КЗ}}.$$

### 7.2.3. Контроль навантажувальної характеристики

Деякі телефонні закладки, призначені для перехоплення телефонних повідомлень, підключаються до АТЛ лише у режимі "Розмова", тобто під час замикання шлейфа. Метод контролю навантажувальної характеристики призначений для виявлення саме такого типу закладок.

***Навантажувальна характеристика*** – це залежність струму в АТЛ від опору навантаження, під'єднаного до затискачів "А" і "В". Типове зображення навантажувальної характеристики "чистої" міської телефонної лінії показано на рис. 7.3, *а* (крива 1).




*а* *б*

*Рис. 7.3. Вигляд навантажувальних та диференційних навантажувальних характеристик "чистої" лінії (а) та із підключеною закладкою (б), що активується замиканням шлейфа*

У разі наявності на АТЛ закладки, яка підключається за умови перевищення порогового значення струму $I_П$ (наприклад, струму спрацювання реле), навантажувальна характеристика має вигляд, зображений на рис. 7.3, *б* (крива 1). У момент спрацювання реле спостерігається стрибкоподібна зміна струму споживання, зумовлена підключенням додаткового опору закладки $R_P$.

Інформативнішою є так звана диференціальна навантажувальна характеристика (криві 2 на рис. 7.3). Для "чистої" лінії диференціальна навантажувальна характеристика є горизонтальною прямою, а про наявність несанкціонованого підключення свідчить імпульсний підйом.

### 7.2.4. Виявлення сторонніх сигналів у АТЛ та радіоефірі

Принцип дії пристроїв контролю сигналів у телефонній лінії ґрунтується на виявленні та аналізі наявних сигналів мовного і позамовного діапазону частот. Пристрої цієї групи мають високу чутливість (на рівні 20 мкВ) у широкому частотному діапазоні від кількох десятків Гц до кількох десятків МГц і розпізнають тип модуляції сигналу. За допомогою цих пристроїв можна:

- прослуховувати НЧ-сигнал у лінії, виявляючи його зв'язок з акустичним сигналом у приміщенні (наявність підключених мікрофонів, пристроїв, що мають мікрофонний ефект тощо);
- виявити наявність так званих сигналів ВЧ-зондування;
- виявити наявність модуляції зондувального ВЧ-сигналу, що пов'язана із акустичним сигналом у приміщенні.

На рис. 7.4 показано схеми, що ілюструють джерела сигналів високочастотного нав'язування, які виявляють цим методом.

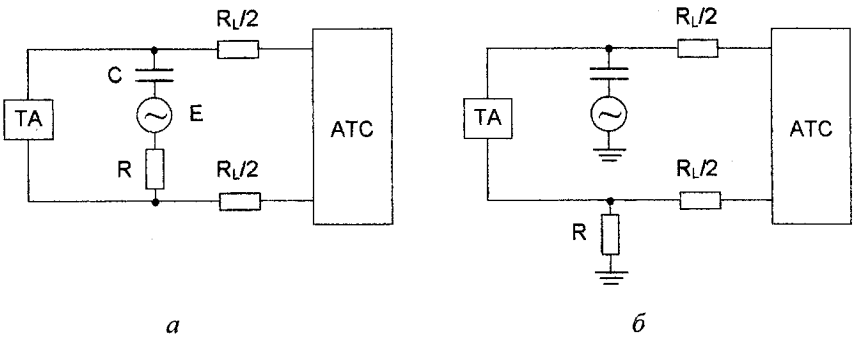



*Рис. 7.4. Симетрична (а) і несиметрична (б) схеми включення джерел сигналів високочастотного нав'язування*

Для виявлення підключених мікрофонних закладок або сигналів високочастотного нав'язування контроль сигналів здійснюється між проводами АТЛ (рис. 7.4, *а*), а у разі високочастотної накачки – стосовно точки заземлення (рис. 7.4, *б*).

Телефонні закладки цього типу використовують телефонну лінію лише як джерело живлення і небезпечного сигналу, а інформацію передають радіоканалом.

Для передачі перехопленої мовної інформації можуть застосовуватися телефонні ретранслятори, що є комбінацією сенсора для знімання сигналів з телефонної лінії і радіопередавача для трансляції радіосигналів на заданій частоті. Такі пристрої використовують АТЛ не лише як джерело живлення, але також проводять високочастотний промодульований сигнал у лінію. Для виявлення подібних пристроїв контролюють радіоефір у самому приміщенні, де розташований телефонний апарат, або на ділянці абонентської проводки, оскільки АТЛ виконує роль випромінювальної антени.

Найпростішими і найдоступнішими пристроями контролю ефіру є ***детектори поля***, які реагують на джерело радіосигналу, що знаходиться на невеликій віддалі від антени детектора. Такі пристрої мають світлову і звукову індикацію, яка сигналізує про наближення до джерела сигналу. Прикладами детекторів поля є вироби D-006 фірми "Смерш Технікс" ($160), а також РТ-2 фірми "НОВО" ($500), що поєднує в собі функції детектора поля і радіочастотоміра.

Для виявлення радіозакладок найефективнішими є портативні широкосмугові радіоприймачі – ***сканери***. Один із найпопулярніших і найдоступніших сканерів AR-8200 японської фірми AOR Ltd є на кафедрі "Захисту інформації". Якщо використовувати сканувальний приймач разом з комп'ютером і спеціальним програмним забезпеченням, можна досягти найбільшої ефективності контролю радіоефіру у приміщенні.

До недоліків цього методу можна зарахувати потребу активації закладних пристроїв під час пошукових робіт і тривалий час контролю ефіру.

## 7.3. Контроль параметрів знеструмлених абонентських телефонних ліній

Арсенал методів і засобів виявлення знеструмлених АТЛ значно ширший і загалом забезпечує потенціально вищу достовірність. Знеструмлення АТЛ (відключення від АТС) найдоцільніше здійснювати у розподільній шафі, оскільки, з одного боку, підключення на абонентській та розподільній ділянках є найімовірнішим, а з іншого, – протяжна міська ділянка АТЛ переважно вносить додаткові завади. Зрозуміло, що ці методи контролю застосовуються лише під час виконання пошукових робіт, а їх спільною особливістю є потреба у використанні зовнішніх джерел різного роду зондувальних сигналів.

На рис. 7.5 показано повну (а) та спрощену (б) електричні схеми заміщення знеструмленої "чистої" абонентської телефонної лінії, а на рис. 7.6 – еквівалентні схеми, що враховують різні способи підключення телефонних закладок: а – резистивну ланку, що відображає безпосереднє підключення кола живлення телефонної закладки, б – ємнісно-резистивну ланку знімання/ передачі інформації, в – діодно-мостову схему живлення закладки.

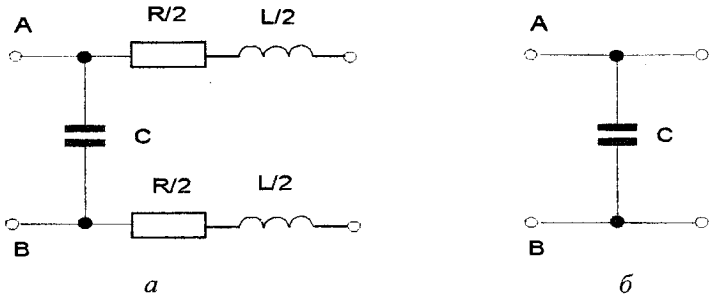



*Рис. 7.5. Повна (а) та спрощена (б) схеми заміщення знеструмленої "чистої" абонентської телефонної лінії*

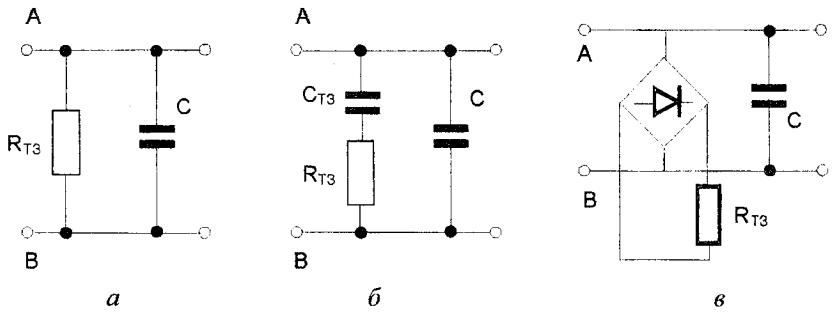



*Рис. 7.6. Еквівалентні схеми з різними способами підключень телефонних закладок*

### 7.3.1. Вимірювання опору шлейфа, омічної асиметрії та параметрів імпедансу абонентських телефонних ліній

Засоби контролю нормалізованих параметрів ліній виявляють відмінності нормалізованих параметрів ліній за наявності та відсутності підключення до

них. Основна маса засобів контролю – це пасивні вимірювачі величин опорів, ємностей, індуктивностей, напруг, струмів, які адаптовані до вимірювань у провідних лініях (оснащені відповідними засобами комутації, автоматизації, інтерпретації показів тощо).

Здатність таких засобів до виявлення підключень, особливо тих, які контролюють чинні лінії, що не відключаються у процесі контролю, не перевищує природного розкиду параметрів реальних ліній. Виявлення підключень до ліній полягає у виявленні відмінності вимірюваних параметрів від середньостатистичних значень "чистих" ліній чи від вимірюваних раніше значень для конкретних ліній.

Вимірювання опору шлейфа та омічної асиметрії переважно здійснюють мостовим методом на постійному струмі. Для вимірювання опору одиничного проводу абонентського шлейфа до одного із затискачів моста приєднується вимірюваний провід з опором $R_L$, заземлений на протилежному кінці (на АТС), а до іншого затискача – заземлення (рис. 7.7). Значення опорів заземлень *r1* і *r2* у абонента на станції мають бути відомі, оскільки входять у плече вимірюваного опору.

Із рівняння зрівноваженого моста

$$R_L + r1 + r2 = \frac{R_A}{R_B} R_O$$

одержують значення опору проводу відніманням від показу моста опорів заземлень.

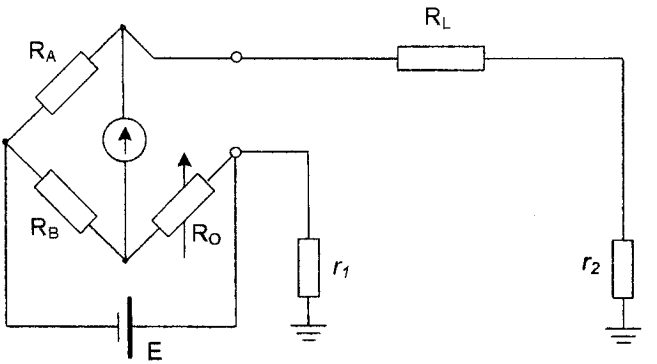



*Рис. 7.7. Схема вимірювання опору шлейфа*

Імпеданс АТЛ визначається так званими первинними параметрами $R, L, C$, які наведені у довідниках. Імпеданс "чистої" знеструмленої і ненавантаженої АТЛ представлений лише ємністю (рис. 7.5, *а*). Вимірювання опору $R$ та індуктивності $L$ АТЛ можна виконати мостом змінного струму за умови замикання лінії на віддаленому кінці.

### 7.3.2. Контроль вольт-амперної характеристики

Вольт-амперна характеристика (ВАХ) – це залежність струму у лінії від лінійно зростаючої напруги. За допомогою ВАХ можна візуально оцінити наявність у контрольованій лінії компонентів з нелінійними характеристиками, насамперед напівпровідникових елементів. Як відомо, кола знімання інформації із АТЛ містять напівпровідникові елементи, а тому характеризуються значною нелінійністю вхідного імпедансу.

Вимірювання вольт-амперної характеристики відбувається за схемою, показаною на рис. 7.8. Джерело лінійно зростаючої напруги може бути на постійному струмі (DC – direct current) або на змінному струмі (AC – alternating current).

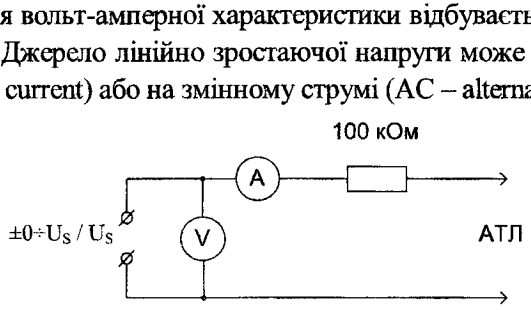



*Рис. 7.8. Схема вимірювання вольт-амперної характеристики АТЛ*

На рис. 7.9 показано приклади вольт-амперних характеристик чистої лінії (а) та з різними видами підключень: (б) – резистивним, (в) – ємнісно-резистивним, (г) – діодно-мостовим.

Іншим методом визначення нелінійностей на АТЛ є нелінійна локація. Нелінійні локатори провідних ліній – це пристрої, дія яких полягає у виявленні в досліджуваному сигналі лінії вищих гармонійних складових, які зумовлені нелінійними спотвореннями гармонічного зондувального сигналу, підключеними до лінії пристроїв з нелінійним імпедансом.

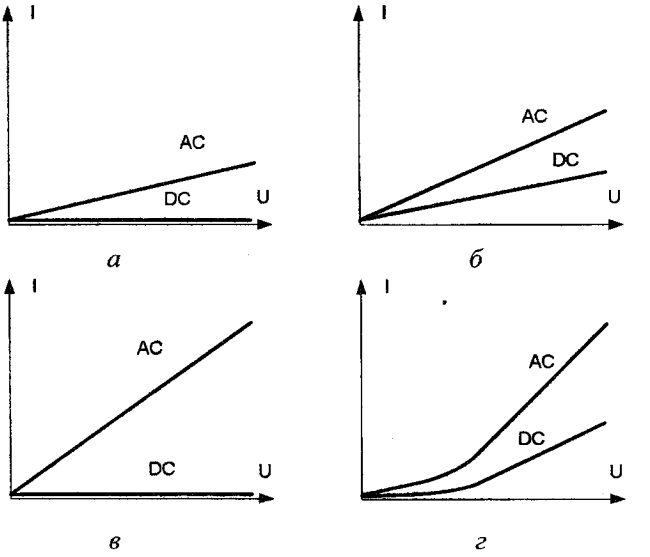



*Рис. 7.9. Приклади вольт-амперних характеристик АТЛ*

### 7.3.3. Контроль Лісажа-характеристики

Лісажа-характеристика – це параметрична залежність струму, що протікає в лінії, під час її збудження синусоїдальною напругою. За допомогою ЛХ можна візуально оцінити фізичні параметри телефонної лінії та виявити наявність підключень з нелінійними характеристиками.

На рис. 7.10 показано приклади Лісажа-характеристик чистої лінії (а) та з різними видами підключень: (б) – резистивним, (в) – ємнісно-резистивним, (г) – діодно-мостовим.

### 7.3.4. Контроль перехідної характеристики

Перехідна характеристика (ПХ) – це реакція АТЛ на дію високовольтної стрибкоподібної напруги. Перехідна характеристика має високу інформативність, оскільки оцінка таких візуальних її параметрів, як монотонність, тривалість, форма, дають змогу із високим ступенем ймовірності визначати наявність та ідентифікувати можливі несанкціоновані підключення до АТЛ.

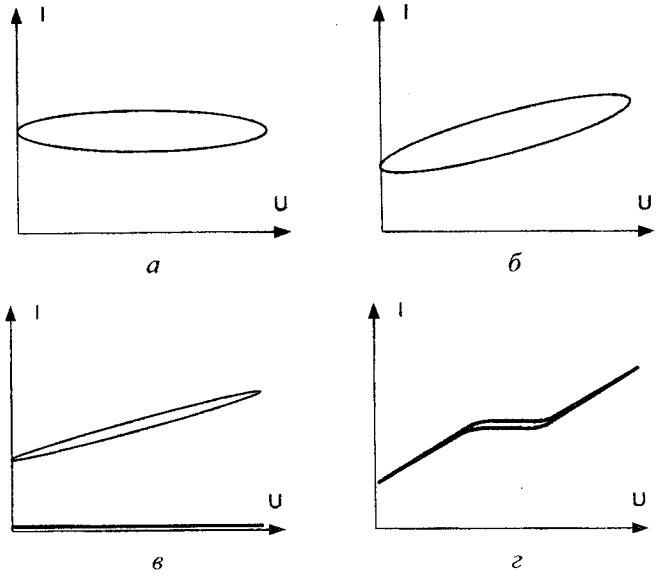



*Рис. 7.10. Приклади Лісажа-характеристик*

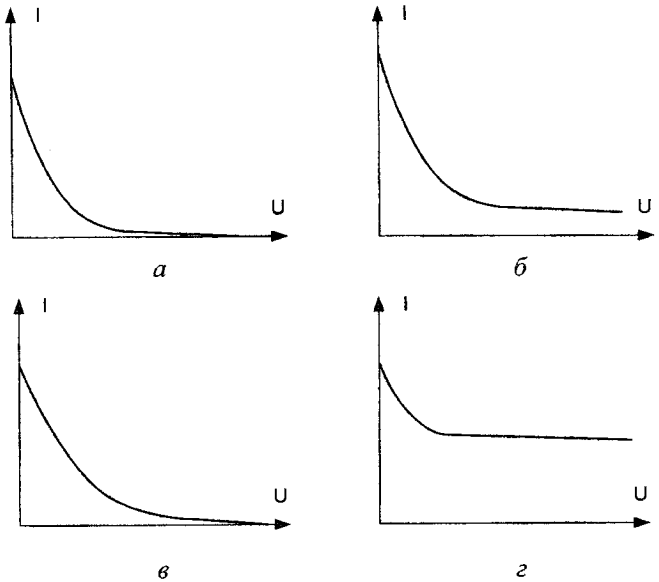



*Рис. 7.11. Приклади перехідних характеристик*

На рис. 7.11 показано приклади перехідних характеристик чистої лінії (а) та з різними видами підключень: (б) – резистивним, (в) – ємнісно-резистивним, (г) – діодно-мостовим.

### 7.3.5. Визначення віддаленості місця несанкціонованого підключення до АТЛ за неоднорідністю

Неоднорідність абонентської телефонної лінії зумовлюється неузгодженістю хвильових імпедансів її окремих елементів чи ділянок. За допомогою імпульсної рефлектометрії можна визначити не лише факт підключення неузгодженого навантаження, але і віддаленість до неоднорідності, що є істотною перевагою методу.

Принцип дії імпульсних рефлектомірів (інша назва "кабельні радари") ґрунтується на подачі у лінію імпульсного сигналу і прийманні відбитого від неоднорідності лінії відгуку. За запізненням відбитого сигналу можна визначити відстань до неоднорідності ("дефекту" лінії). Як відомо, коефіцієнт відбиття від неоднорідності визначається за виразом

$$\Gamma = \frac{Z_X - Z_W}{Z_X + Z_W}, \tag{7.1}$$

де $Z_W$ і $Z_X$ – відповідно хвильовий опір "чистої" лінії та у місці неоднорідності.

На рис. 7.12 показано рефлектограми, що відповідають підключенням до телефонної лінії телефонних закладок паралельного (а) та послідовного (б) типу.

Підключення до телефонної лінії паралельної закладки із опором $R_P$ зумовлює зміну хвильового опору до значення

$$Z_X = \frac{Z_W R_P}{Z_W + R_P}. \tag{7.2}$$

Коефіцієнт відбиття $\Gamma_P$ може змінюватися у межах від 0 (відбитого сигналу немає), за умови "чистої" лінії ($R_P = \infty$), до -1 (повне відбиття сигналу із зміною полярності), що відповідає короткому замиканню ($R_P = 0$). Значення опору телефонної закладки $R_P$ лежить між двома граничними значеннями (нулем і нескінченністю), тому і амплітуда відбитого сигналу за заданих умов буде тим більша, чим менший опір паралельної телефонної закладки (рис. 7.12, *а*).

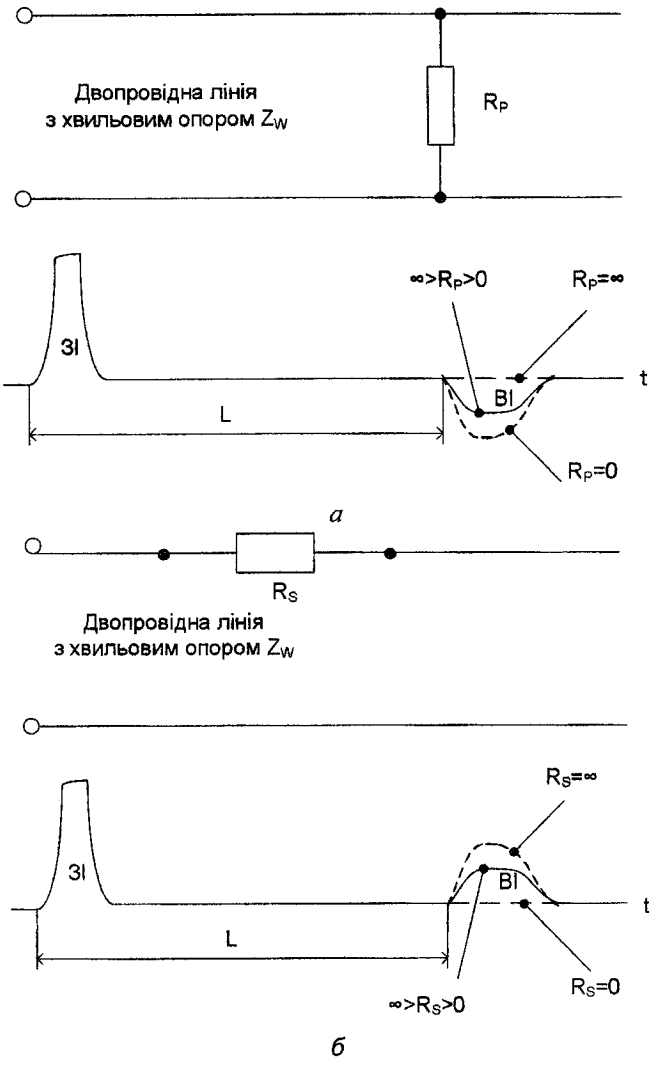



*Рис. 7.12. Рефлектограми під час підключення паралельних (а) і послідовних (б) телефонних закладок*

Підключення до телефонної лінії послідовної закладки із опором $R_S$ зумовлює зміну хвильового опору до значення

$$Z_X = Z_W + R_S . \tag{7.3}$$

У цьому випадку коефіцієнт відбиття $\Gamma_S$ може змінюватися у межах від 0 (відбитого сигналу немає), за умови "чистої" лінії ($R_S = 0$), до +1 (повне відбиття сигналу без зміни полярності), що відповідає розриву лінії ($R_S = \infty$). Значення опору телефонної закладки $R_S$ лежить між цими двома граничними значеннями (нулем і нескінченністю), тому і амплітуда відбитого сигналу за заданих умов буде тим більша, чим більший опір послідовної телефонної закладки (рис. 7.12, *б*).

Виявляючі можливості рефлектомірів обмежені їх чутливістю, згасанням імпульсного сигналу, яке вносить лінія, а також впливом зовнішніх адитивних завад. З огляду на відмінність хвильового опору різних типів ліній, на практиці кожна конкретна лінія вимагає калібрування приладу.

Застосування імпульсних рефлектомірів є ефективним за наявності результатів вимірювання "чистої" лінії. Для цього телефонна лінія спочатку візуально перевіряється на предмет відсутності на ній засобів знімання інформації, потім до неї підключається прилад і за результатами вимірювання складається паспорт лінії, в якому вказується номер неоднорідності (відведення до паралельного телефону, стик від нарощування кабелю тощо) і відстань до неї за показами рефлектоміра. Під час проведення планового контролю чи пошукових робіт прилад знову підключається до лінії і здійснюється перевірка на предмет появи нових неоднорідностей.

## 7.4. Комплексні системи моніторингу телефонних ліній

Сьогодні для виявлення, локалізації та нейтралізації засобів техрозвідки, зокрема і на аналогових телефонних лініях, широко використовуються автоматизовані пошукові системи, які завдяки застосуванню різних методів контролю та сучасних цифрових засобів оброблення сигналів забезпечують поглиблені дослідження стану інформаційної безпеки, підвищують ефективність пошукових робіт та достовірність результатів моніторингу.

Одним із прикладів пристроїв цього класу є універсальний лінійний аналізатор "ULAN-2" (Росія), призначений для виявлення фактів несанкціонованого підключення у різних проводових комунікаціях, таких як телефонні

лінії, електричні електромережі змінного струму, комп'ютерні мережі, лінії охоронно-пожежної сигналізації тощо.

Прилад дає можливість виявити факт підключення до телефонних ліній кіл живлення фактично усіх відомих пристроїв знімання і передачі інформації, без відключення цих ліній від АТС, тобто у робочому стані. Рішення щодо виявлення гальванічних підключень не потрібує наявності апріорної інформації про параметри "чистої" лінії. Прилад здатний не лише виявити та ідентифікувати виявлені пристрої, але, використовуючи метод імпульсної рефлектометрії, визначати відстань до місця несанкціонованого підключення.

Універсальний лінійний аналізатор "ULAN-2" є на кафедрі захисту інформації, а його основні технічні характеристики наведені у Додатку 2.

Іншим прикладом пошукових пристроїв, які використовують комплексні дослідження телефонних ліній, є портативний аналізатор ССТА-1000 (фірма CCS, США). Він уможливлює проведення шести типів контрольних перевірок телефонних ліній. Вимірюється напруга, струм, опір і ємність лінії в автоматичному і ручному режимах. Передбачена також антена для виявлення пристроїв підслуховування з радіопередавачами.

## Питання для самоконтролю:

**1.** На чому ґрунтується робота засобів виявлення несанкціонованих підключень до абонентських телефонних ліній?

**2.** Перерахуйте методи, які придатні для виявлення несанкціонованих підключень до АТЛ, що знаходиться у робочому режимі або у знеструмленому стані.

**3.** У чому полягає різниця між пристроями виявлення несанкціонованих підключень до АТЛ, що працюють у сторожовому і пошуковому режимах?

**4.** Наведіть модель АТЛ для постійного струму у режимі "Очікування" та "Розмова".

**5.** Наведіть співвідношення, що використовуються у роботі пристроїв контролю напруги живлення АТЛ, та вкажіть основні недоліки цих засобів контролю.

**6.** Для виявлення яких телефонних закладок придатні пристрої контролю струму короткого замикання? Наведіть співвідношення, які описують роботу цих пристроїв.

**7.** Охарактеризуйте зміст методу контролю навантажувальної характеристики. Чому інформативність диференціальної навантажувальної характеристики вища?

**8.** На чому ґрунтується принцип дії пристроїв контролю сигналів у телефонній лінії та радіоефірі?

**9.** Наведіть моделі, що ілюструють симетричне і несиметричне включення джерел сигналів високочастотного нав'язування.

**10.** Які телефонні закладки виявляються за допомогою детекторів поля і сканерів радіоефіру?

**11.** Наведіть повну та спрощену електричні схеми заміщення знеструмленої "чистої" абонентської телефонної лінії, а також еквівалентні схеми, що враховують різні способи підключення телефонних закладок.

**12.** Опишіть методи вимірювання опору шлейфа, омічної асиметрії та параметрів імпедансу абонентських телефонних ліній.

**13.** Розкрийте зміст методів та принцип дії пристроїв контролю вольт-амперної характеристики, Лісажа-характеристики та перехідної характеристики.

**14.** На чому ґрунтується принцип дії імпульсних рефлектомірів? Наведіть вираз для коефіцієнта відбиття від неоднорідності.

**15.** Наведіть типові рефлектограми під час підключення паралельних і послідовних телефонних закладок.

**16.** Дайте характеристику комплексним системам моніторингу телефонних ліній на прикладі універсального лінійного аналізатора "ULAN-2".

# Розділ 8

# ЗАХИСТ АБОНЕНТСЬКИХ ТЕЛЕФОННИХ ЛІНІЙ ВІД ПРОСЛУХОВУВАННЯ

Оскільки АТС є режимними об'єктами із відомчою охороною, а перехоплення телефонних повідомлень на ділянках магістральних ліній систем передачі ускладнене через мультиплексацію потоків групових сигналів, то абонентська телефонна лінія є найнезахищенішим, а відтак найуразливішим елементом телефонної мережі. Це зумовлює високу ймовірність застосування засобів технічної розвідки несанкціонованим підключенням до АТЛ. Тому можна вважати, що захист абонентських телефонних ліній є важливим, а в деяких випадках і самодостатнім завданням у загальній проблематиці захисту засобів і каналів телефонного зв'язку.

У результаті вивчення цього розділу студент повинен знати:

- різновиди та зміст завдань забезпечення конфіденційності на ділянці АТЛ із застосуванням технічних засобів захисту;
- суть та можливості методів обмеження фізичного доступу до АТЛ та знищення гальванічно підключених телефонних закладок;
- принципи роботи та доцільні випадки застосування пасивних і активних засобів технічного захисту АТЛ у режимі очікування;
- особливості застосування технічних засобів захисту від перехоплення телефонних повідомлень на ділянці АТЛ;
- перелік сертифікованих в Україні засобів технічного захисту АТЛ.

## 8.1. Характеристика завдань забезпечення конфіденційності на ділянці АТЛ

Забезпечення конфіденційності на об'єктах інформаційної діяльності із телефонним зв'язком є актуальним під час виконання завдань захисту інформації (рис. 8.1):

- закриття телефонних повідомлень, які передаються телефонною мережею загального користування;
- запобігання витоку мовної інформації абонентською телефонною лінією із приміщень, де розміщені телефонні апарати.

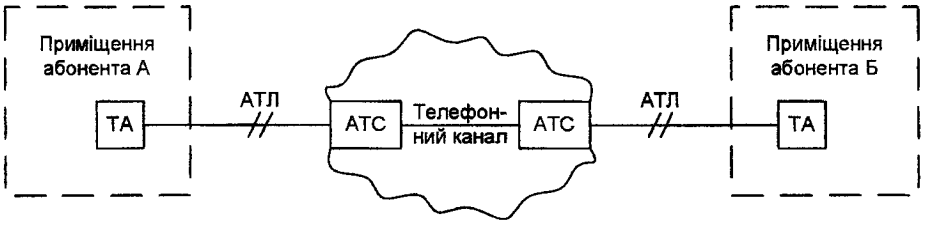



*Рис. 8.1. Модель телефонного зв'язку для аналізу конфіденційності*

У табл. 8.1 подано порівняльну характеристику згаданих завдань захисту інформації.

*Таблиця 8.1*

**Порівняльна характеристика завдань захисту інформації**

| Завдання захисту | Закриття телефонних повідомлень | Запобігання прослуховуванню приміщення |
|---|---|---|
| Стан АТЛ | Замкнений шлейф (телефонна трубка піднята) | Розімкнений шлейф (телефонна трубка покладена) |
| Джерела загроз | Телефонні повідомлення, побічні електромагнітні випромінювання і наведення | Акустоелектричний канал витоку мовної інформації |
| Шляхи реалізації загроз | Контактні та безконтактні телефонні закладки | Засоби техрозвідки контактного типу |

Як зазначалося у розділі 5, загрози конфіденційності здійснюються через підключення до АТЛ засобів технічної розвідки, причому найімовірнішим таке підключення є до відкритих ділянок абонентської проводки, телефонної розетки, телефонного апарата, розподільної коробки чи шафи. Абонентська телефонна лінія може бути не лише ділянкою телефонного тракту під час проведення телефонних переговорів, але й елементом технічного каналу витоку мовної інформації із приміщення. АТЛ може перебувати в одному із двох станів: розімкнений шлейф (трубка покладена) або замкнений шлейф (трубка піднята).

Для запобігання використанню АТЛ для прослуховування приміщень та підслуховування телефонних повідомлень використовуються як однакові, так і відмінні методи. Крім власне методів забезпечення конфіденційності за вже підключених до АТЛ телефонних закладок, важливими є методи і засоби, націлені на запобігання встановленню телефонних закладок, виявлення факту їх підключення до АТЛ та фізичного знищення усіх несанкціоновано підключених до АТЛ пристроїв.

## 8.2. Методи обмеження фізичного доступу до АТЛ та знищення гальванічно підключених телефонних закладок

Оскільки загрози конфіденційності найчастіше здійснюються підключенням до АТЛ телефонних закладок, то доцільно застосовувати методи захисту, що ґрунтуються як на ***обмеженні фізичного доступу*** до засобів телефонного зв'язку (запобігання встановленню телефонних закладок), так і на ***фізичному знищенні*** вже встановлених телефонних закладок контактного типу, наприклад, електричним випалюванням.

Обмеження фізичного доступу до АТЛ передбачає унеможливлення або хоча б ускладнення:

- безпосереднього підключення зловмисником розвідувальної апаратури до телефонних апаратів чи окремих ділянок АТЛ;
- візуальної розвідки та отримання зловмисником допоміжної інформації про обладнання та організацію зв'язку на об'єкті, що у подальшому полегшить несанкціоноване підключення до АТЛ;
- використання зловмисником для перехоплення інформації електромагнітних полів у навколишньому просторі та наведень у колах живлення і заземлення, що знаходяться у межах контрольованої зони.

Цілком очевидно, що застосування цього методу можливе лише у межах контрольованої зони, при цьому на основній протяжності (ділянка міського телефонного кабелю) телефонна лінія знаходиться поза зоною адміністративного контролю. Крім того, застосування заходів обмеження фізичного доступу, як правило, є нереальним для абонента, що працює у "блукаючому" режимі. У цьому випадку потрібно застосовувати методи та засоби захисту телефонного зв'язку, що розглядаються нижче.

Метод ***"випалювання"*** реалізується подачею в лінію високовольтних імпульсів, напругою понад 1500 В, що приводять до знищення вхідних каскадів електронних пристроїв перехоплення інформації та їх блоків живлення, гальванічно підключених до телефонної лінії. Використовуючи цей метод, телефонний апарат від лінії відключається, а подача імпульсів у лінію здійснюється два рази:

- перший – за розімкненої телефонної лінії для "випалювання" паралельно під'єднаних пристроїв;
- другий – за закороченої (як правило, у центральному розподільному щитку будинку) телефонної лінії для "випалювання" послідовно під'єднаних пристроїв.

У Додатку 3 наведені основні технічні характеристики деяких пристроїв фізичного знищення телефонних закладок на АТЛ.

## 8.3. Запобігання прослуховуванню приміщень через АТЛ

Прослуховування приміщень відбувається у режимі очікування, тобто за покладеної слухавки. Це загалом спрощує реалізацію цієї функції захисту порівняно із забезпеченням конфіденційності телефонних переговорів. Серед пристроїв захисту цієї категорії розрізняють пасивні та активні, а їх роботу в узагальненому вигляді можна описати рівнянням

$$r(t) = s(t) * h(t) + \xi(t),$$

де $r(t)$ – сигнал на вході засобу технічної розвідки; $s(t)$ – небезпечний сигнал; $h(t)$ – імпульсна характеристика пасивного засобу захисту; $\xi(t)$ – захисний шум активних пристроїв захисту.

Елементами технічного (електроакустичного) каналу витоку мовної інформації з приміщень є абонентська телефонна лінія, а джерелами небезпечного сигналу – телефонний апарат або телефонна закладка.

### 8.3.1. Пасивні засоби захисту: нелінійні розв'язувальні пристрої, загороджувальні фільтри та електронні комутатори

***Пасивні*** засоби захисту мають за мету послабити рівень небезпечного сигналу у АТЛ. Дія пасивних засобів захисту АТЛ передбачає:

- ***блокування*** небезпечних сигналів від елементів телефонного апарата внаслідок так званого "мікрофонного ефекту";
- ***фільтрацію*** небезпечних сигналів від пристроїв високочастотного нав'язування;
- ***відключення*** джерел (перетворювачів) небезпечних сигналів, наприклад, акустичних закладок, які передають інформацію телефонною лінією у режимі покладеної трубки.

Для блокування низькорівневих сигналів від "мікрофонного ефекту" використовуються **нелінійні розв'язувальні пристрої**, дія яких ґрунтується на нелінійних властивостях p-n-переходів напівпровідникових елементів, переважно діодів. На рис. 8.2, *а* показано типову вольт-амперну характеристику кремнієвого діода. Такі діоди мають великий опір (сотні кОм) для струмів малої амплітуди

$$R_{НС} = \frac{\Delta U_{НС}}{\Delta I_{НС}}$$

й одиниці Ом і менше – для струмів великої амплітуди (корисних сигналів виклику або розмовних):

$$R_{РС} = \frac{\Delta U_{РС}}{\Delta I_{РС}}.$$

Велике значення опору p-n-переходу для інформативних сигналів малої амплітуди унеможливлює їх проникнення у телефонну лінію і фактично не впливає на проходження через діоди корисних сигналів.

У схемі нелінійних розв'язувальних пристроїв використовуються два зустрічно увімкнені діоди, які включаються послідовно у лінію дзвінка (рис. 8.2, *б*), або безпосередньо у кожну з телефонних ліній (рис. 8.2, *в*). Це виключає проходження через діоди у телефонну лінію небезпечних сигналів малої амплітуди від "мікрофонного ефекту" і фактично не впливає на проходження корисних сигналів під час телефонної розмови.

Для захисту телефонних апаратів від "високочастотного нав'язування" застосовуються **загороджувальні фільтри**, які встановлюють між телефонним апаратом і АТЛ. Амплітудно-частотна характеристика таких фільтрів має забезпечувати "прозорість" в інтервалі каналу тональної частоти (300–3400 Гц) і якомога більше згасання сигналів на частотах позазвукового діапазону.

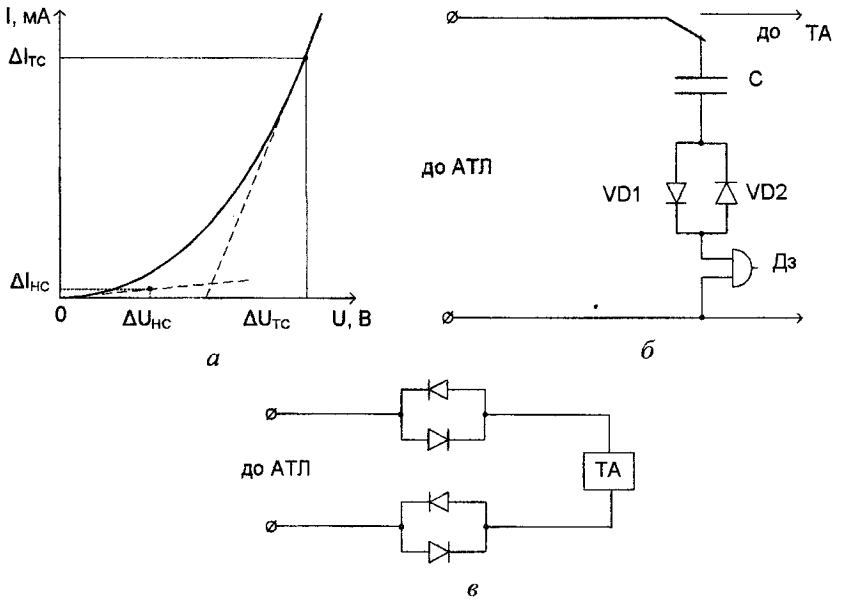



*Рис. 8.2. Вольт-амперна характеристика діода (а) та схеми включення діодних обмежувачів для захисту кола дзвінка (б) чи телефонного апарата загалом (в)*

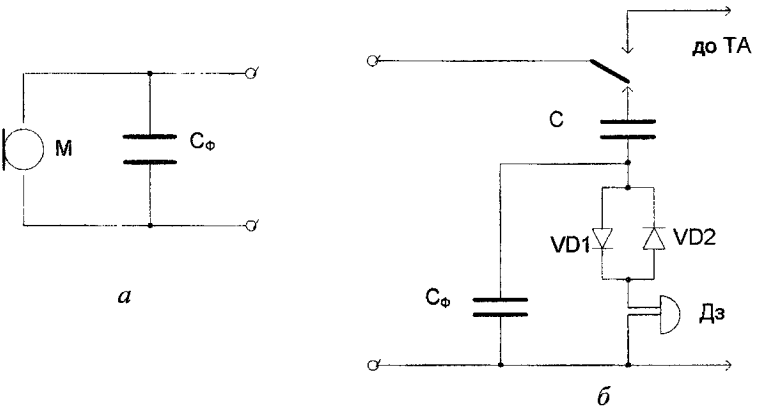



*Рис. 8.3. Схеми захисту мікрофона (а) і дзвінкового кола (б) телефонного апарата*

Найпростішим варіантом загороджувального фільтра є конденсатор, встановлений у мікрофонне коло телефонного апарата або у коло електромеханічного дзвінка виклику (рис. 8.3). Ємність конденсаторів вибирається так, щоб зашунтувати зондувальні сигнали високочастотного "нав'язування" і до того ж істотно не впливати на корисні сигнали. Переважно для установки у мікрофонне коло використовуються конденсатори ємністю 0,01 – 0,05 мкФ, а для установки в дзвінкове коло – 1 мкФ. Складніший фільтрувальний пристрій являє собою багатоланковий фільтр нижніх частот на LC-елементах.

Для захисту телефонних апаратів, як правило, використовуються пристрої, що поєднують фільтр і обмежувач (рис. 8.4). Ці пристрої вмикаються у розрив кола (між телефонним апаратом та АТЛ) і забезпечують придушення небезпечного сигналу малого рівня від "мікрофонного ефекту" більш ніж на 80 дБ і вносять згасання для сигналів "високочастотного нав'язування" у смузі частот від 30 кГц до 30 МГц більше 70 дБ.

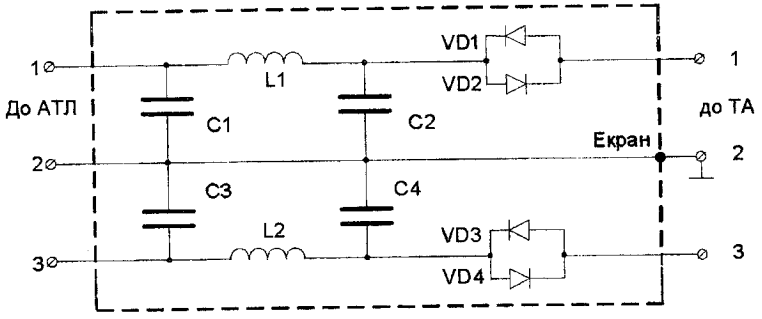



*Рис. 8.4. Схема пристрою захисту телефонних апаратів типу "Гранит-8"*

Відключення телефонних апаратів або встановлених телефонних закладок від АТЛ під час ведення в приміщенні конфіденційних розмов є найефективнішим методом захисту інформації. Найпростіший спосіб реалізації цього методу захисту полягає в установці у корпусі телефонного апарата або телефонної лінії ***звичайного тумблера***, що вмикається і вимикається вручну. Зручнішою в експлуатації є установка в телефонній лінії спеціального пристрою захисту – ***електронного комутатора***, який автоматично (без участі оператора) відключає телефонний апарат від лінії за покладеної слухавки.

До типових пристроїв, що реалізують цей метод захисту, належить комутатор телефонних ліній "Скеля-1К". Пристрій має такі режими роботи: "Чекання", "Виклик" і "Розмова". У режимі чекання (за покладеної слухавки) телефонний апарат гальванічно відключений від лінії й пристрій знаходиться у режимі аналізу підняття слухавки та наявності сигналів виклику. При цьому послаблення сигналу витоку мовної інформації становить не менше 120 дБ.

За наявності у лінії сигналів виклику пристрій підключає телефонний апарат до абонентської лінії лише на час дії сигналів виклику. Під час підняття слухавки пристрій переходить у робочий режим і телефонний апарат підключається до лінії.

Електронний комутатор встановлюється у розрив телефонної лінії при виході її із виділеного приміщення або в розподільному щитку, що знаходиться у межах контрольованої зони.

### 8.3.2. Активні засоби захисту. Генератори маскувальних сигналів

Дія ***активних*** засобів полягає у накладанні захисного шуму на небезпечний сигнал. Розрізняють ***низькочастотні маскувальні сигнали*** у діапазоні від 100 Гц до 10 кГц та ***високочастотні широкосмугові*** – від 20 кГц до 30 МГц. Унаслідок ефекту маскування не вдається засобами технічної розвідки виділити інформативні параметри сигналів витоку.

Активні засоби блокування технічних каналів витоку абонентськими телефонними лініями часто називають засобами лінійного зашумлення, а їх дія ґрунтується на створенні й "закачуванні" в лінію за покладеної трубки шумового сигналу. Генератори шуму (ГШ) підключаються у розрив телефонної лінії і монтуються, як правило, безпосередньо у корпусі телефонного апарата (рис. 8.5). Шумовий сигнал подається в лінію у режимі, коли телефонний апарат не використовується (трубка покладена). За підняття трубки телефонного апарата подача в лінію шумового сигналу припиняється.


*Рис. 8.5. Схема підключення засобів лінійного зашумлення*

Низькочастотна маскувальна перешкода застосовується для:

- створення перешкод роботі виносних мікрофонів, що використовують телефонну лінію для передачі інформації;
- активації (вмикання на запис) диктофонів, які підключені до АТЛ за допомогою адаптерів або індукційних датчиків, що призводить до змотування плівки у проміжках між телефонними розмовами у режимі запису шуму (тобто за відсутності корисного сигналу);
- маскування сигналів, що виникають від "мікрофонного ефекту".

Пристрої захисту, що реалізують метод високочастотної маскувальної завади, забезпечують захист від сигналів високочастотного нав'язування чи накачки, а також використовують для запобігання передачі сигналів виносних мікрофонів з модуляцією чи кодуванням. До сертифікованих в Україні пасивних засобів захисту, що поєднують фільтр і обмежувач, належить пристрій "Скеля-1Ф", а активні засоби лінійного зашумлення представлені пристроєм "Скеля-1Г". Технічні характеристики пристрою технічного захисту інформації "Скеля-1" наведені у Додатку 3.

## 8.4. Методи захисту від підслуховування телефонних повідомлень на ділянці абонентських телефонних ліній

Для захисту телефонних повідомлень від підслуховування на ділянці АТЛ використовуються такі методи:

- ***накладання маскувальних перешкод*** (синфазної низькочастотної або високочастотної) у режимі піднятої трубки з метою запобігання перехопленню телефонних повідомлень;
- ***порушення функціонування (придушення) електронних пристроїв перехоплення інформації*** за допомогою маніпуляції із напругою живлення АТЛ (підвищення її рівня чи зміни полярності).

### 8.4.1. Накладання маскувальних перешкод

Суть методу ***синфазної низькочастотної маскувальної перешкоди*** полягає у подачі під час розмови у кожний провід телефонної лінії стосовно єдиної системи заземлення апаратури АТС і захисного заземлення електромережі абонента узгоджених за амплітудою та фазою перешкоджальних сигналів, спектральна густина потужності яких зосереджена у тональному діапазоні

(300 – 3400 Гц). Ефективність маскування досягається лише для послідовних телефонних закладок, оскільки у паралельних закладках, як і у телефонному апараті, такі перешкоджальні сигнали компенсують один одного, не створюючи завад для сигналу мовлення.

За методом ***високочастотної маскувальної перешкоди*** під час розмови у телефонну лінію подається білий шум або псевдовипадкові імпульсні послідовності із надтонального 6 – 20 кГц та ультразвукового (понад 20 кГц) діапазонів. Параметри перешкоджальних маскувальних сигналів підбираються так, щоб ці сигнали, з одного боку, не погіршували якість телефонних розмов, а з іншого, – після проходження селективних кіл адаптера телефонних закладок їх рівень виявився достатнім для маскування корисного сигналу. Негативний вплив перешкод на телефонний апарат усувається спеціальним низькочастотним фільтром із граничною частотою в 3,4 кГц. Встановлені на міських АТС смугові фільтри виконують аналогічну роль, а от подібна фільтрація у телефонних закладках ускладнюється габаритами низькочастотних фільтрів.

Цей метод використовується для придушення фактично усіх типів електронних пристроїв перехоплення мовної інформації як контактного (послідовного і паралельного) підключення до лінії, так і безконтактного підключення до лінії з використанням індукційних датчиків різноманітного типу. Проте ефективність придушення засобів знімання інформації з підключенням до лінії за допомогою індукційних датчиків (особливо тих, що не мають попередніх підсилювачів) значно нижча, ніж засобів із гальванічним підключенням до лінії.

### 8.4.2. Придушення електронних засобів технічної розвідки

Для захисту телефонних розмов використовуються методи активного впливу на працездатність електронних пристроїв перехоплення інформації, до яких належать:

- метод підвищення напруги;
- метод зміни полярності напруги живлення.

Метод ***підвищення напруги живлення*** використовується для погіршення якості функціонування телефонних закладок під час розмови за рахунок переведення їхніх каскадів підсилення та передачі у нелінійний режим роботи під час підняття напруги у лінії до 18÷24 В. Метод є ефективним як для паралельних, так і для послідовних телефонних радіозакладок.

Метод ***зміни полярності напруги живлення*** передбачає подачу під час розмови у лінію постійної напруги, що відповідає напрузі у лінії за піднятої слухавки, але оберненої полярності. Цей метод використовується для порушення функціонування електронних пристроїв перехоплення інформації з контактним підключенням до телефонної лінії, що використовують її як джерело живлення. До таких пристроїв належать паралельні телефонні апарати і телефонні радіозакладки.

## Питання для самоконтролю:

**1.** Наведіть модель телефонного зв'язку для аналізу конфіденційності та дайте порівняльну характеристику завданням конфіденційності на об'єктах із телефонним зв'язком.

**2.** Як застосовуються пристрої випалювання для знищення паралельних та послідовних телефонних закладок?

**3.** Дайте узагальнений опис роботи пасивних і активних пристроїв захисту АТЛ у режимі очікування.

**4.** Які три принципи можна застосувати для реалізації роботи пасивних пристроїв з метою послаблення небезпечного сигналу?

**5.** Для усунення якої загрози застосовуються нелінійні розв'язувальні пристрої і який механізм їх дії?

**6.** Для усунення якої загрози застосовуються загороджувальні фільтри і який механізм їх дії?

**7.** Наведіть схему пристрою захисту телефонних апаратів типу "Гранит-8" та поясніть призначення її окремих елементів.

**8.** Опишіть роботу пристроїв блокування АТЛ у режимі очікування.

**9.** Для яких цілей застосовують генератори низькочастотних маскувальних перешкод?

**10.** Які пасивні та активні технічні засоби захисту АТЛ сертифіковано в Україні?

**11.** У чому полягає специфіка застосування засобів зашумлення для захисту телефонних повідомлень від підслуховування на ділянці АТЛ?

**12.** Які методи застосовуються для захисту телефонних повідомлень від підслуховування на ділянці АТЛ?

**13.** Розкрийте суть методу синфазної низькочастотної маскувальної перешкоди.

**14.** Які особливості роботи пристроїв створення високочастотних маскувальних перешкод та доцільні випадки їх застосування?

**15.** Поясніть, як відбувається придушення електронних засобів технічної розвідки під час використання методів підвищення напруги живлення та зміни її полярності.

# Розділ 9

# ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПІД ЧАС ПЕРЕДАЧІ МОВНИХ ПОВІДОМЛЕНЬ КАНАЛАМИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Забезпеченя конфіденційності телефонних переговорів має свою специфіку, зумовлену передусім аналоговою природою повідомлень. Цей аспект, з одного боку, ускладнює застосування криптографічних засобів для шифрування телефонних повідомлень, а з іншого, – розширює арсенал засобів приховування семантичного змісту цих повідомлень, які не доступні для захисту даних у комп'ютерних мережах. У цьому розділі розглядаються методи і засоби забезпечення кофіденційності повідомлень впродовж усього телефонного тракту, які можуть бути застосовані абонентами телефонних мереж загального користування.

У результаті вивчення цього розділу студент повинен знати:

- специфіку завдань забезпечення конфіденційності мовної інформації та застосовувані методи захисту від перехоплення телефонних повідомлень упродовж усього телефонного тракту;
- принцип роботи і модель односторонніх маскіраторів телефонних повідомлень, а також переваги та недоліки застосування цих пристроїв для забезпечення конфіденційності;
- зміст і особливості частотних та часових перестановок для приховування семантичних телефонних повідомлень, а також чинники, що обмежують гарантований рівень їх закриття;
- необхідні перетворення, яким піддаються телефонні повідомлення, для застосування сучасних алгоритмів шифрування;
- структуру захищеного телефонного апарата і перебіг службових сигналів, що використовуються для встановлення захищеного режиму.

## 9.1. Класифікація і характеристика методів забезпечення конфіденційності телефонних повідомлень

Відомі три основні методи захисту від перехоплення телефонних повідомлень впродовж усього телефонного тракту:

- ***одностороннє маскування*** накладанням на телефонне повідомлення з боку одержувача маскувальних перешкод із подальшою їх компенсацією;
- ***скремблювання*** (часочастотні перетворення) мовних сигналів;
- ***шифрування*** стиснених телефонних повідомлень.

Кожен із цих методів має свої переваги і недоліки, а їх зміст та особливості розкрито нижче. Так, методи маскування і скремблювання забезпечують захист телефонних повідомлень на нижньому сигнальному рівні, тоді як шифрування пов'язане із криптографічними перетвореннями мовної інформації, представленої у формі даних на вищому рівні інтерпретації.

Метод маскування передбачає адитивне накладання на аналоговий телефонний сигнал спеціальних перешкод, рівень яких забезпечує надійне енергетичне маскування телефонних повідомлень упродовж усього телефонного тракту. Отже, йдеться про зменшення відношення "сигнал/шум" до значень, за яких стає вже неможливим виділення зловмисником інформаційного сигналу засобами техрозвідки.

Особливістю методу скремблювання є такі перетворення форми сигналів мовлення, їх часових і частотних характеристик, у результаті яких спотворюється семантичний зміст телефонних повідомлень, що унеможливлює (чи, принаймні, ускладнює) сприйняття зловмисником інформації. До того ж зміна форми сигналів є відновлювана для абонентів, які володіють значеннями параметрів алгоритмів (ключем), застосованими у процесі скремблювання.

Методи шифрування також забезпечують захист телефонних повідомлень на семантичному рівні, але мають свою специфіку, зумовлену насамперед вразливістю телефонних повідомлень до затримок у часі, а також значною кореляцією вибірок мовного сигналу.

На рис. 9.1 показано класифікацію сучасних методів закриття телефонних сигналів на семантичному рівні. Під час захисту мовного обміну вирішальне значення має вид сигналу мовлення у каналі зв'язку (аналоговий чи цифровий).

Захист інформації на семантичному рівні досягається застосуванням часо-частотних та криптографічних перетворень і спрямований на унеможливлення її одержання (виділення), навіть під час перехоплення зловмисником сигналів. Перетворення повинно надавати інформації вигляд, що унеможливлює її сприйняття під час використання апаратури, стандартної для цього каналу зв'язку. Використовуючи спеціальну апаратуру відновлення первинного

виду інформації, необхідно витрачати такі затрати часу і засобів, щоб втручання зловмисника в інформаційний процес втратило сенс.

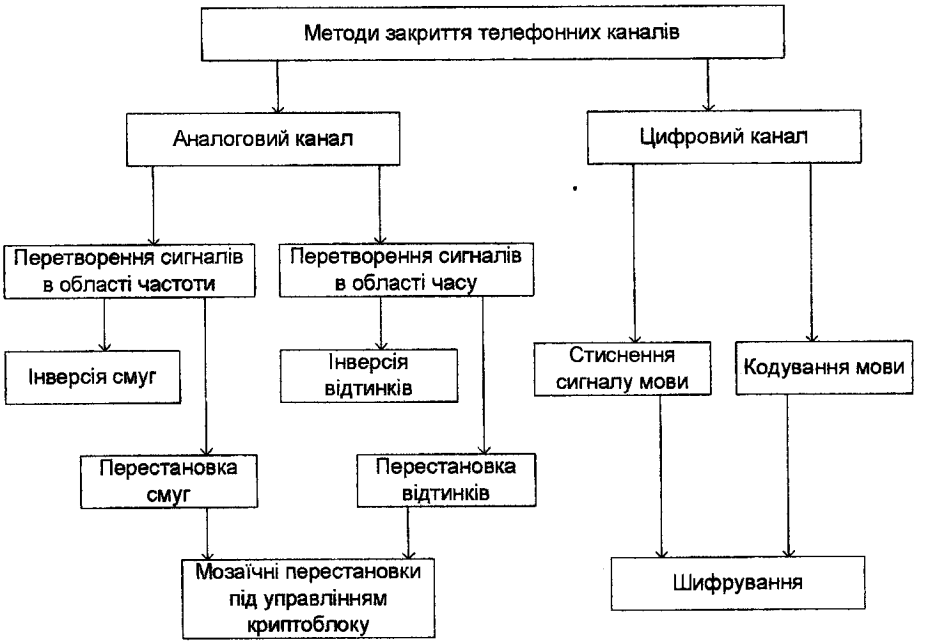



*Рис. 9.1. Класифікація методів закриття мовної інформації у телефонних каналах*

Незважаючи на істотно різні рівні захисту, наявність на ринку "ніші" для кожного типу перетворювачів сигналу зумовлена різноманітністю вимог користувачів.

## 9.2. Захист від перехоплення телефонних повідомлень на енергетичному рівні. Метод одностороннього маскування

Застосовуючи маскувальні перешкоди до приховування мовних повідомлень, потрібно зважати на такі обставини:

1. Мовний обмін у природних умовах піддається впливові різноманітних завад, тому у процесі еволюції артикуляційний (мовотворчий) і перцепційний

(слуховий) апарати людини сформували прекрасно зв'язану і винятково завадостійку систему. Тому, якщо у технічних системах придушення стійкого прийому сигналу переважно спостерігається за відношення "шум/сигнал" у кілька десятків відсотків, то для людини втрата семантичного (змістового) сприйняття мови відбувається за відношення "шум/сигнал" у кілька сотень відсотків, а придушення ознак мови (неможливість фіксації факту розмови) досягається за відношення "шум/сигнал", близького до 10. Крім того, прослуховування зашумленої мови впродовж тривалого часу, а тим паче багатократне прослуховування такої мови у записі, завдяки адаптаційним властивостям людського слуху стають зрозумілими фрагменти мови, що були не сприйняті під час короткочасної оцінки.

У випадках, коли маскувальний шум містить значну детерміновану складову, яка після перехоплення може бути відфільтрована, для досягнення стійкого захисту необхідно збільшувати рівень шуму.

2. Стійкий маскувальний ефект забезпечується лише під час накладання на корисний сигнал шуму, що є насправді випадковим процесом і за частотним діапазоном повністю перекриває мовний сигнал. До того ж багато відомих і часто використовуваних способів формують псевдошумовий сигнал, який за своїми частотними і часовими параметрами близький до справжнього шумового, але значною мірою є детермінований із значними внутрішніми кореляційними зв'язками. Такий сигнал можна використовувати як захисний шум, якщо перехоплення ведеться на слух. Проте під час застосування методів кореляційної обробки такий "шум" може бути ефективно придушений.

3. Мовний сигнал і маскувальний шум по-різному розповсюджуються у просторі, тому забезпечити повну ідентичність їх розподілу і накладання вкрай складно. Потрібно враховувати, що застосування багатоканального прийому з кількох спеціально вибраних точок може послабити маскувальний ефект шумового поля.

Виключити можливість застосування зловмисником методів багатоканального прийому можна, повністю сумістивши шляхи розповсюдження корисного сигналу і маскувального шуму. До того ж забезпечити захищений телефонний зв'язок між двома легальними абонентами можна було б формуванням ідентичних шумових сигналів на передавальному і на приймальному боці. При цьому на передавальному боці шум накладався б із корисним сиг-

налом, а на приймальному – розділявся. Та незважаючи на здавалося б простоту такого рішення, його практична реалізація ускладнюється впливом нестабільності передавальної характеристики каналу зв'язку, що виявляється у неповній компенсації маскувальної перешкоди, а відтак у зниженні якості зв'язку. Але найістотнішими обмеженнями такого варіанта маскування телефонних повідомлень на енергетичному рівні є:

- неможливість незалежного формування справді випадкового маскувального сигналу на передавальному і приймальному боці;
- потреба у синхронізації апаратури захисту на передавальному і приймальному боці.

Тому на практиці застосовується інший варіант компенсаційного методу – ***метод одностороннього маскування.*** Його суть полягає у подачі в телефонну лінію маскувальної перешкоди $\xi(t)$ у вигляді випадкового цифрового або аналогового сигналу із спектром, що перекриває діапазон мовного сигналу. Ця перешкода утворюється за допомогою спеціального генератора маскувальної перешкоди (ГМП) у абонента, який приймає конфіденційне повідомлення (рис. 9.2). На протилежному кінці телефонного тракту (у слухавці абонента, що передає конфіденційне повідомлення) діятиме послаблена проходженням телефонного тракту маскувальна перешкода:

$$r_1(t) = h(t) * \xi(t),$$

де $h(t)$ – імпульсна характеристика телефонного тракту.

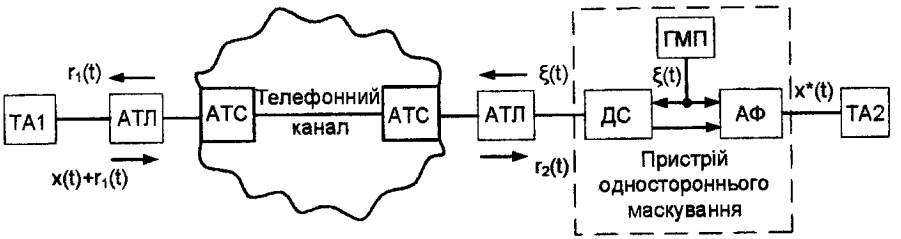



*Рис. 9.2. Закриття телефонних повідомлень за методом одностороннього маскування*

Конфіденційне повідомлення $x(t)$, створюване мікрофоном телефонного апарата ТА1, передається на тлі маскувальної перешкоди $r_1(t)$, причому її рівень має бути достатнім, щоб захистити від перехоплення телефонне повідомлення на віддаленій АТЛ. На прийомі за допомогою диференціальної схеми ДС виділяється адитивна суміш корисного сигналу і перешкоди, які послаблені проходженням через телефонний тракт:

$$r_2(t) = h(t) \cdot \left[ x(t) + h(t) \cdot \xi(t) \right].$$

Ця суміш подається на один із входів двоканального адаптивного фільтра (АФ), на інший вхід якого надходить маскувальний сигнал у "чистому" вигляді $\xi(t)$. Адитивний фільтр компенсує (придушує) шумову складову і виділяє корисний сигнал $x^*(t)$, що подається на телефонний апарат.

Слід зазначити, що практична реалізація методу одностороннього маскування стала можливою лише в останнє десятиріччя завдяки розвитку та вдосконаленню алгоритмів і засобів цифрового оброблення сигналів, зокрема застосуванню швидкодіючих сигнальних процесорів, що уможливлюють забезпечення швидкої і точної адаптації до характеристик каналу зв'язку.

Перевагою застосування пристроїв одностороннього маскування є відсутність потреби синхронізації та додаткового часу на створення захищеного каналу. Проте істотним обмеженням таких пристроїв є їх одностороння дія. За потреби захищеного обміну телефонними повідомленнями обидва абоненти повинні мати пристрої одностороннього маскування, не обов'язково однакові, та використовувати їх по черзі у режимі прийому. Це створює певні незручності у користуванні, тому застосування пристроїв одностороннього маскування може виявитися доцільним лише для фрагментарного захисту інформації, що передається із будь-яких джерел, зокрема із таксофонів чи стільникових апаратів.

Сьогодні серійно випускаються кілька моделей пристроїв одностороннього маскування, серед них вироби "Щит" і "Туман".

## 9.3. Приховування семантичного змісту телефонних повідомлень часо-частотними перетвореннями

### 9.3.1. Інверсія та перетворення спектра телефонних сигналів

Найпростішим, але і не дуже стійким до розкриття методом захисту телефонних повідомлень, що належить до цього класу, є інверсія спектра мовного сигналу. Процес інверсії спектра сигналу при передачі та його відновлення під час приймання ілюструється рис. 9.3.

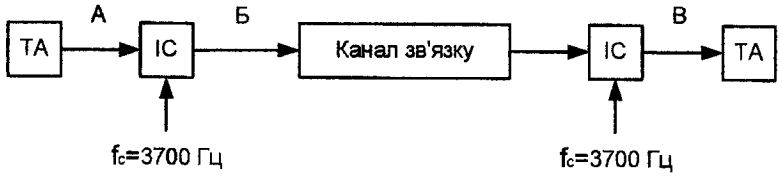
Схему застосування інвертора спектра для закриття телефонних повідомлень показано на рис. 9.3, *а*. Сам інвертор спектра ІС є балансним змішувачем, що, як відомо, здійснює амплітудну модуляцію із подавленою несучою. На частоті несучої $f_C$, що дорівнює сумі граничних частот телефонного сигналу $F_H = 300$ Гц та $F_B = 3400$ Гц, тобто

$$f_C = F_H + F_B = 3700 \text{ Гц},$$

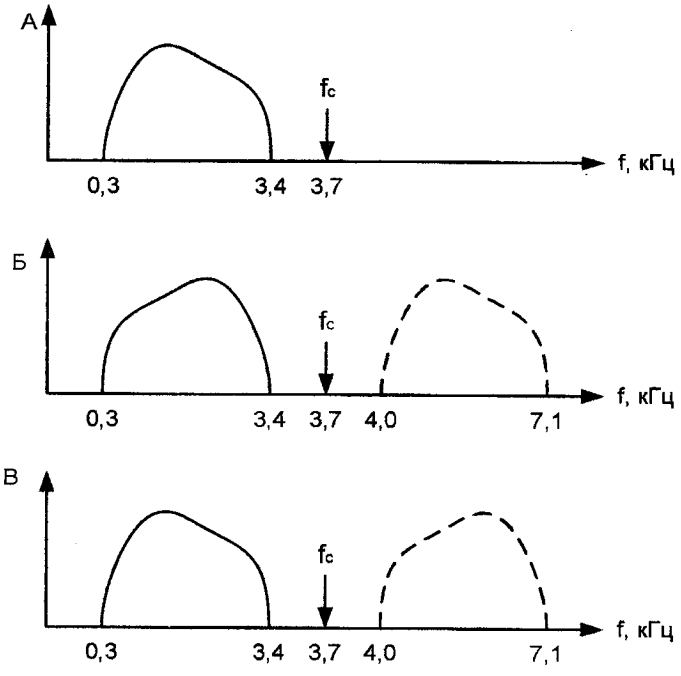
нижня бічна смуга частот модульованого сигналу відтворюється у початковій смузі частот, тобто у смузі каналу тональної частоти, але в інвертованому вигляді. На прийомі проводиться повторна інверсія і початковий сигнал відновлюється (рис. 9.3, *б*). Як на передачі, так і під час приймання, верхня бічна смуга, яка знаходиться поза КТЧ, відфільтровується (пунктирні лінії).

Якість відновленої мови залежить від досконалості змішувачів і фільтрів, що обмежують спектр вхідного сигналу і виділяють нижню бічну смугу частот перетвореного сигналу, а також від корегування на приймальному боці частотних спотворень каналу, вплив яких також позначається інверсно: загасання каналу у верхній частині спектра під час приймання позначається у низькочастотній частині сигналу, і навпаки.

Під час перехоплення сигнал з інвертованим спектром може бути легко відновлений будь-яким аналогічним апаратом (не обов'язково однотипним), а за відповідного тренування – сприйнятий людиною безпосередньо. Для підвищення стійкості захисту деякі виробники використовують багатосмугову інверсію із фіксованими перестановками спектральних компонент мовного сигналу.




*а*




*б*

*Рис. 9.3. Інвертор спектра (а) та спектр сигналів у різних точках (б)*

Оскільки основна частина енергії мовного сигналу зосереджена у невеликій області низькочастотного спектра, то вибір варіантів змішування його частотних компонент є обмежений. Смуга частот тонального каналу (300–3400 Гц) становить 3,5 октави. Смугові фільтри, що розділяють сигнал на частотні смуги, мають скінченну крутизну амплітудно-частотної характерис-

тики, внаслідок чого на границях частотних інтервалів відбувається помітне невідновне змішування різних компонент сигналу. Формуючи три смуги (по 1,2 октави на кожну смугу) і використовуючи фільтри 8-го порядку (наростання згасання близько 48 дБ/октаву), згасання всередині сусідньої смуги становитиме не більше 30 дБ, що зумовлює низьку якість відновленої мови. Істотне збільшення порядку фільтрів настільки ускладнює апаратуру, що вона втрачає переваги перед іншими варіантами перетворювачів. До того ж кількість можливих перестановок із трьох смуг – усього лише шість, з чотирьох смуг – 24, тобто підбір потрібної підстановки не становить труднощів навіть в умовах прямого перехоплення, не кажучи вже про аналіз запису у спецлабораторіях.

Найбільшою перевагою перетворювачів спектра є їхня автономність, тобто відпадає потреба взаємної синхронізації передавального і приймального пристроїв і відповідно відсутність затримки зв'язку для синхронізації і можливих зривів захищеного режиму через зниження якості каналу. Якщо вдалося встановити зв'язок у відкритому режимі після включення партнерами інвертувань, буде реалізований і захищений режим. Перехід у захищений режим відбувається за взаємною домовленістю абонентів після встановлення з'єднання натисканням відповідної клавіші.

Під час розмови у лінії прослуховується характерний сигнал, що за структурою повторює передавану мову. Відновлений сигнал має високу якість. Наявність сторонніх шумів у приміщенні, з якого ведеться передавання, позначається на якості відновленого сигналу так само, як у відкритому режимі, і майже не впливає на стійкість захисту.


*Рис. 9.4. Схема частотних перестановок телефонного сигналу на основі швидкого перетворення Фур'є*

Апаратура може включатися між телефонним апаратом і лінією у стандартний двопроводовий стик. Можливий варіант виконання перетво-

рювачів спектра у вигляді накладки на мікротелефонну трубку з акустичною передачею перетвореного сигналу. До переваг перетворювачів спектра також можна зарахувати низьку ціну (порядку 30–50 USD).

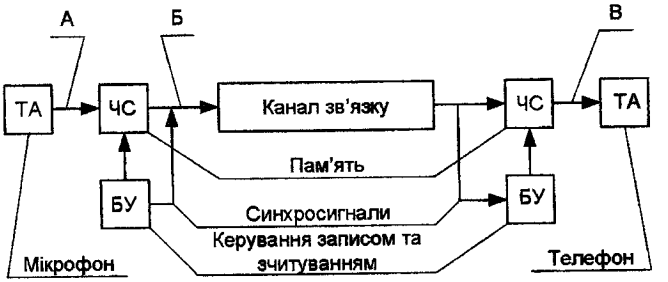
Основним недоліком перетворювачів спектра є низький рівень захисту. Дещо підвищити ступінь закриття телефонних повідомлень можна, застосовуючи швидке перетворення Фур'є, оскільки кількість допустимих перемішувань частотних смуг при цьому значно збільшується (рис. 9.4). Однак значна кореляція спектральних компонент мовного сигналу також обмежує можливості цього методу.

### 9.3.2. Часові перестановки фрагментів телефонних сигналів

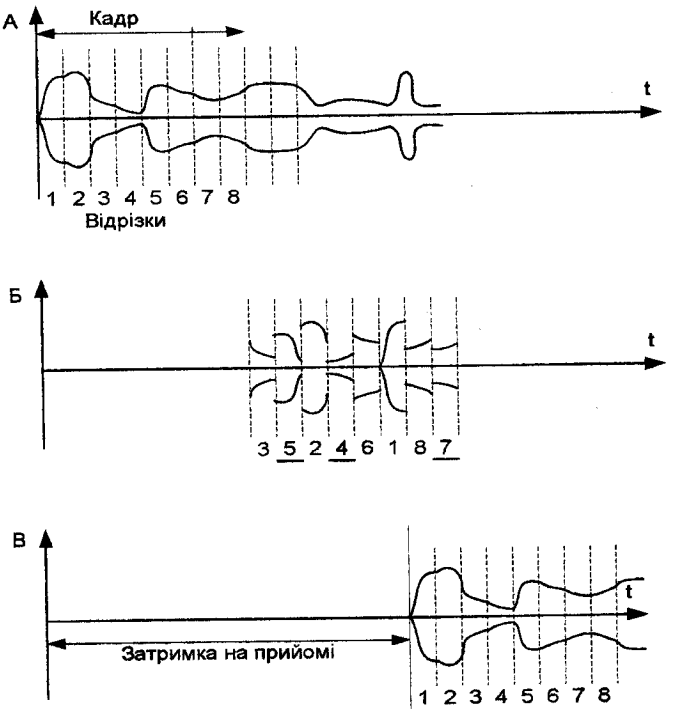
Принцип часових перестановок (часового скремблювання) передбачає поділ мовного сигналу на послідовність часових сегментів та подальше їх перемішування. Робота часових скремблерів ЧС за своїм принципом вносить затримку через потребу запам'ятовування деякої кількості сегментів мовного сигналу з метою їх подальшого зчитування у тій чи іншій послідовності. Отже, часовий скремблер вимагає наявності у своєму складі блока запам'ятовування із керованим доступом до запису і зчитування окремих сегментів сигналу. Крім того, для коректної роботи часових скремблерів на обох кінцях захищеного телефонного тракту вимагається синхронізація їх роботи. Структуру часового скремблера та процеси перетворення сигналу показано на рис. 9.5.

Для мовного сигналу кількість варіантів часових перестановок є обмеженою. Дослідження показали, що тривалість сегментів, на які розбивається початковий мовний сигнал, не повинна перевищувати тривалості одного елементарного звука мови (10–20 мс). Збільшення кількості змішуваних сегментів (збільшення глибини перестановки) також обмежене зростанням затримки відновлюваного під час приймання сигналу. Наприклад, часові перестановки на інтервалі 100 мс із урахуванням зворотного перетворення вимагають щонайменше 200 мс, що є межею допустимої затримки сигналу у телефонії. Затримка під час діалогу більш ніж на 300 мс викликає помітні незручності, а за затримки понад 1 с діалог стає неможливим. Зазначені чинники визначають глибину часових перестановок на рівні 15–30 елементарних відрізків мови.

Під час передачі скрембльованого у часі сигналу через обмежену частотну смугу каналу тональної частоти виникають крайові спотворення відрізків сигналу. За відновлення мови під час приймання це призводить до появи "зшивань", які погіршують якість відновленого сигналу (рис. 9.5, *б*).




*а*




*б*

*Рис. 9.5. Принцип часового скремблювання: а – структурна схема телефонного каналу із часовим скремблюванням; б – вигляд сигналів у різних точках схеми*

Можна підвищити захисний ефект, якщо до одержаних часових перестановок сигналів додатково застосувати ще й часову інверсію фрагментів мовного сигналу. Часова інверсія досягається відтворенням у зворотному напрямі запису часових фрагментів сигналу (такі інтервали на рис. 9.5, *б* підкреслено).

Комбінування часових перестановок з часовою інверсією за правильного вибору параметрів перестановок унеможливлює безпосереднє прослуховування мови у телефонному каналі. Але під час аналізу запису статична перестановка, яка повторюється із кадру в кадр, розкривається за спектральними і амплітудними зв'язками відрізків сигналу. Оскільки із застосуванням нескладної апаратури (комп'ютер із аудіокартою) мовна інформація може бути відновлена, тому сьогодні для захисту телефонних повідомлень застосовуються скремблери зі змінними перестановками. Алгоритм, за яким відбувається зміна порядку часових перестановок, задається криптоблоком.

Застосування змінних перестановок значно утруднює відновлення початкової мови із перехопленого сигналу. За вдалого криптоалгоритму розкриття перестановки на одному інтервалі ніяк не сприяє підбору перестановок на подальших інтервалах. Крім того, введення криптоалгоритму із індивідуальним ключем унеможливлює використання однотипного апарата для перехоплення.

### 9.3.3. Часо-частотне скремблювання телефонних повідомлень

Використовуючи комбінацію часового і частотного скремблювання, можна значно підвищити ступінь закриття мови. Сучасні комбіновані скремблери використовують перетворення і перемішування одночасно як частотних, так і часових параметрів сигналів за певним алгоритмом, причому для підвищення рівня захисту параметри алгоритму змінюються під управлінням криптоблока (рис. 9.6).

Мовний сигнал $x(t)$ оцифровується аналогово-цифровим перетворювачем (АЦП). Із використанням ковзаючого часового вікна $\tau$ швидким перетворенням Фур'є із сегмента вибірок $x(n)$ формується спектрограма, тобто представлення енергії мовного сигналу на площині частоти і часу (рис. 9.7). Далі у блоці цифрового оброблення під дією генератора псевдовипадкових

чисел ГПЧ відбувається перемішування фрагментів сигналу у часо-частотній площині (мозаїчні перестановки). Варіант перестановок задається криптографічним ключем. У результаті зворотного швидкого перетворення Фур'є формується скрембльований цифровий сигнал $y(n)$, який за допомогою цифро-аналогового перетворювача ЦАП перетворюються в аналоговий сигнал $y(t)$, придатний для передачі на АТС абонентською телефонною лінією. Під час приймання відбуваються зворотні часо-частотні перетворення над оцифрованою версією скрембльованого сигналу та відновлення аналогового сигналу, наближеного до оригінального $x'(t) \approx x(t)$.

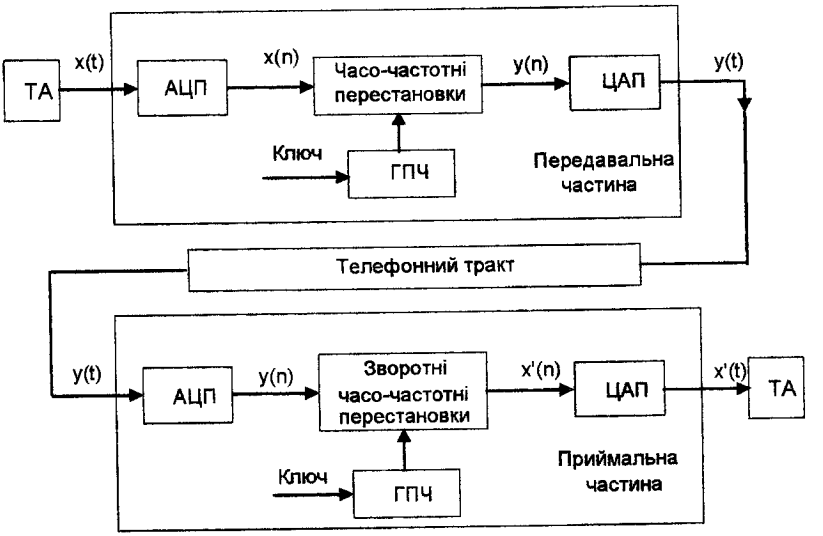



*Рис. 9.6. Схема комбінованого часо-частотного скремблера*

Оскільки принцип роботи апаратури за методами часо-частотних перетворень пов'язаний із руйнуванням на передачі і подальшим відновленням на прийомі мозаїчної картини сигналу, поданої у вигляді спектрограми, це зумовило появу іншої назви скремблерів – апаратури мозаїчних перетворень.

Основною перевагою часо-частотного сремблювання є поєднання доволі високого ступеня захисту телефонних повідомлень зі збереженням смуги

частот, унаслідок чого скрембльований сигнал може бути переданий безпосередньо по АТЛ без застосування додаткових пристроїв, наприклад, модемів.

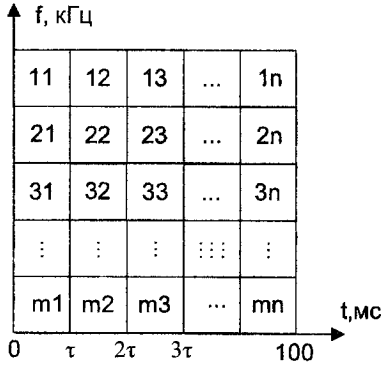



*Рис. 9.7. Спектрограма мовного сигналу*

Обов'язковим етапом робочого процесу є початкова синхронізація взаємодіючих скремблерів і їх подальша підсинхронізація. Під час переходу в захищений режим за домовленістю абонентів виникає інтервал переривання мовного зв'язку, який синхронізує і встановлює взаємодію криптоблоків. У багатьох виробах у цей самий час абонент, використовуючи тастатуру телефонного апарата або тастатуру скремблера, повинен ввести ключ. У результаті перехід у захищений режим може займати близько 10–20 с. При цьому треба враховувати, що за поганої якості каналу синхронізація і перехід у захищений режим можуть не відбутися взагалі, хоча зв'язок у відкритому режимі, нехай й за поганої якості, підтримується.

Наявність часової затримки під час передачі сигналу двопроводовою лінією неминуче призводить до виникнення "еха". У сучасній апаратурі зв'язку, зокрема у високошвидкісних модемах, відпрацьовані досконалі алгоритми компенсації еха. Проте людське вухо реагує на рівні ехо-сигналів, які явно неістотні для модемів. Тому навіть у найвдаліших моделях скремблерів придушення еха до непомітного рівня досягається тільки за випадково вдалого поєднання параметрів лінії зв'язку.

Криптоблок, що керує процесом перестановок, може використовувати як симетричну, так і несиметричну ключову систему, яка має відомі переваги. Враховуючи, що за найдосконалішого криптоалгоритму передавана мова може

бути відновлена із перехопленого лінійного сигналу за залишковими ознаками взаємного розташування елементарних відрізків, застосування у скремблерах дуже сильних криптоалгоритмів і дуже довгих ключів не виправдане. Цілком достатньою є довжина ключа до 10 цифр (30 бітів) у симетричній ключовій системі і 30 цифр (близько 100 бітів) – у несиметричній ключовій системі.

Перевагами скремблерів як апаратури закриття телефонних повідомлень є:

- порівняно висока стійкість захисту передаваного мовного сигналу, що виключає його безпосереднє прослуховування і вимагає для відновлення повідомлення значних затрат часу із використанням спеціалізованих вимірювально-обчислювальних комплексів;
- можливість безпосередньої передачі скрембльованого сигналу абонентською телефонною лінією (без застосування модемів);
- порівняно низька вартість та простота експлуатації.

До недоліків цього класу апаратури можна зарахувати:

- затримку відновленого сигналу на приймальному боці, що вимагає деякого звикання і ускладнює діалог;
- наявність еха, рівень якого залежить від параметрів телефонного тракту;
- затримку зв'язку на час проходження процесу синхронізації апаратів;
- можливість зриву синхронізації у разі погіршення якості каналу.

За сукупністю параметрів скремблери є найприйнятнішим варіантом для використання у корпоративних захищених телефонних системах під час обміну мовною інформацією оперативного характеру, що не вимагає тривалого періоду секретності.

Для забезпечення доброї розбірливості відновленого сигналу та високого рівня закриття телефонних повідомлень використовуються доволі складні алгоритми цифрового оброблення сигналів, що переважно реалізуються на основі сигнальних процесорів. На ринку України найвідомішими є такі типи скремблерів: Орех-II, Грот-С, GUARD-BASE, SCR-M1.2.

## 9.4. Оцифровування і стиснення мови з подальшим шифруванням

Альтернативним до скремблювання методом закриття телефонних повідомлень є шифрування мовних сигналів, попередньо перетворених у цифрову

форму. Відомо, що комерційна якість оцифрованого телефонного повідомлення вимагає швидкості 64 кбіт/с, що перевищує пропускну здатність аналогових абонентських телефонних ліній під час використання модемів. Тому метод закриття телефонних повідомлень шифруванням обов'язково передбачає стиснення телефонних повідомлень за одним із двох методів, які відрізняються обчислювальною складністю та вимагають різної швидкості передачі:

- ***кодування форми сигналу*** (***waveform coding***) – невисока складність алгоритму та швидкість передачі мови у кілька десятків кбіт/с;
- ***кодування параметрів мовного сигналу*** (***voice coder***) – висока складність алгоритму за швидкості передачі порядку десять кбіт/с або нижче.

### 9.4.1. Шифрування стиснених телефонних повідомлень

Найвідомішим стандартом стиснення часових перебігів мовного сигналу є алгоритм адаптивної різницевої імпульсно-кодової модуляції ADPCM (Adaptive Differential Pulse Code Modulation), який забезпечує комерційну якість передачі телефонного повідомлення на швидкості 32 кбіт/с. Цей клас апаратури закриття телефонних повідомлень є перспективним для каналів абонентського доступу, що забезпечують стійкий модемний зв'язок на швидкості 32 кбіт/с.

Для входження у режим захищеного зв'язку взаємодіючим апаратам потрібен деякий час для синхронізації криптоблоків та обміну ключовою інформацією. Проте за швидкості обміну 32 кбіт/с необхідний для цього час не перевищує 1 с. Якість відновленої мови після розшифрування лінійного сигналу не поступається якості відкритої мови, а затримка фактично відсутня. Стійкість захисту повністю визначається використаним алгоритмом шифрування та надійністю криптографічних ключів. Сигнал у телефонному каналі не несе жодних ознак мовного сигналу, а сприймається на слух, як звичайний сигнал модему.

На рис. 9.8 показано структуру системи криптографічного закриття стиснених телефонних повідомлень. На передачі послідовно виконуються такі перетворення:

- стиснення телефонного сигналу за алгоритмом ADPCM;
- шифрування потоку за одним із криптографічних алгоритмів;
- передача зашифрованих даних телефонним трактом за допомогою модемів.

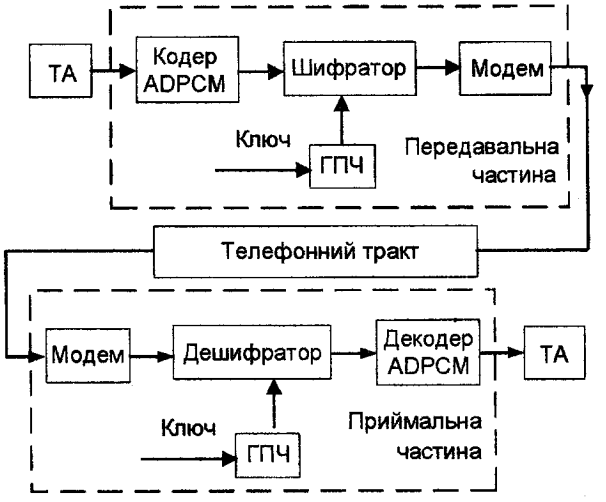



*Рис. 9.8. Структура системи криптографічного закриття стиснених телефонних повідомлень*

На приймальному боці виконуються зворотні перетворення і у зворотному порядку.

### 9.4.2. Кодування параметрів мовного сигналу із подальшим шифруванням цифрового потоку

Апаратура закриття цього типу становить основу державних систем захищеного мовного зв'язку у багатьох країнах світу. Принцип роботи ґрунтується на визначенні за допомогою вокодерів, необхідних для синтезу параметрів мови та їх передачі у шифрованому вигляді.

Сьогодні відомо багато різних методів побудови вокодерів (див. розділ 2). Наприклад, один із перших вокодерів з лінійним передбачуванням за алгоритмом LPC-10 на швидкості 2,4 кбіт/с забезпечує прийнятний рівень розбірливості мови, але недостатню натуральність звучання та розпізнавальність, натомість алгоритм MP-MLQ забезпечує високу якість синтезу мови на швидкості 8 кбіт/с.

Дослідження структури звука людського голосу показало, що для передачі не тільки тексту, але й індивідуальності голосу, його інтонацій,

тембру достатньо швидкості цифрового потоку 2–5 кбіт/с, а за деякої втрати якості – навіть 1 кбіт/с. Передача цифрового потоку на такій швидкості забезпечується фактично будь-яким каналом телефонного зв'язку. Це робить апаратуру захисту телефонних каналів із вокодерним перетворенням мови винятковою, оскільки забезпечується організація захищеного мовного зв'язку із будь-яким абонентом, який має відкритий телефонний зв'язок, а шифрування цифрового потоку дає змогу забезпечити будь-яку задану стійкість захисту.

Структуру системи захищеного вокодерного зв'язку показано на рис. 9.9. Системи, зображені на рис. 9.8 і 9.9, відрізняються лише різними підходами до кодування (стиснення) телефонного сигналу.

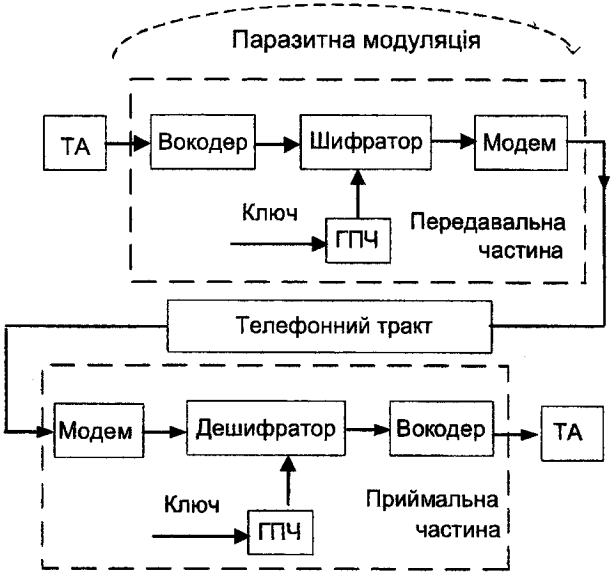



*Рис. 9.9. Структура системи захищеного вокодерного зв'язку*

З особливостей такої апаратури можна відзначити таке. Процес аналізу мови на передачі принципово вимагає інтервалу часу порядку 10–30 мс, тому на прийомі відновлена мова дещо затримується, але ця затримка на порядок менша, ніж у скремблерів. Оскільки алгоритм аналізу оптимізований на звучання деякого середньостатистичного людського голосу, під час вимовляння

незвично високих звуків і деяких звукосполучень процес кодування може порушуватися і у відновленій на приймальному боці мові виникають спотворення. Саме тому шуми довкілля (зокрема, й інші голоси) на передачі істотно знижують якість мови на прийомі. Вокодер усі звуки намагається подати як компоненти мови, тому, якщо, наприклад, на мікрофон діє шум вітру, після кодування і декодування він може перетворитися на цілком мовоподібний сигнал. Це накладає певні обмеження на умови використання вокодерної апаратури.

Для шифрування стиснених телефонних повідомлень можна використати струменеві алгоритми, наприклад RC4, або блокові алгоритми (DES, ГОСТ 28147-89 тощо) у потоковому режимі. У завданнях з захисту інформації у каналах зв'язку вибір системи формування, розподілу та переховування криптографічних ключів може виявитися важливішим за вибір алгоритму шифрування. У симетричних системах секретні ключі поширюються суто конфіденційними каналами, що зумовлює проблему їх розподілу між багатьма територіально віддаленими абонентами. У несиметричних системах розподіл відкритих ключів спирається на технологію цифрових сертифікатів, що спрощує їх використання.

З-поміж доступних на ринку України можна виділити насамперед такі телефонні шифратори, як "Орех-4131" та "VoiceCoder-2400". Слід зазначити, що шифратори, як і скремблери, не захищають телефонну лінію від отримання акустичної інформації з приміщення у перервах між телефонними переговорами. Крім того, існує загроза технічного каналу витоку відкритої мовної інформації через паразитну модуляцію лінійного цифрового сигналу (рис. 9.9).

### 9.4.3. Алгоритм встановлення шифрованого телефонного зв'язку у телефонній мережі загального користування

Встановлення шифрованого зв'язку у телефонній мережі загального користування складається із таких етапів (рис. 9.10):

1. ***Встановлення з'єднання*** у комутованій телефонній мережі загального користування (на схемі часові інтервали **Набір** і **Виклик**).

2. ***Телефонна розмова у відкритому режимі,*** коли абоненти домовляються про перехід у закритий режим (інтервал **Відкритий зв'язок**).

**3.** ***Запотребування послуг закритого зв'язку*** ініціюється абонентами набором відповідних кодів у формі тонального набору DTMF (інтервали **A** і **B**).

**4.** ***Встановлення цифрового каналу*** – це сесія конфігурації модемів, що передбачає тестування параметрів телефонного каналу, узгодження протоколів, швидкості передачі.

**5.** ***Узгодження параметрів шифрування*** – це погодження вибору алгоритмів та процедура автентифікації й генерування криптографічних ключів сеансу зв'язку (інтервали **C**, **D** і **E**).

**6.** ***Закритий зв'язок*** – передача телефонних повідомлень у шифрованому вигляді.

**7.** ***Роз'єднання абонентів*** – ліквідація телефонного каналу у телефонній мережі.

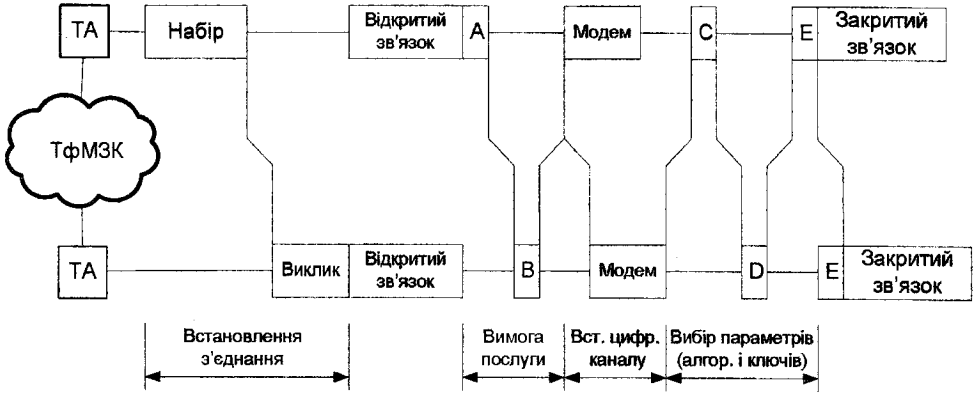



*Рис. 9.10. Алгоритм встановлення шифрованого зв'язку*

Структуру захищеного телефонного апарата показано на рис. 9.11.

На початку перемикачі на ТА та мережевому інтерфейсі пристрою знаходяться у лівому положенні, чим забезпечується пряме підключення телефонного апарата до абонентської телефонної лінії. У звичайний спосіб забезпечуться встановлення телефонного з'єднання та розмова абонентів у відкритому режимі.

Після взаємної домовленості абоненти переходять у захищений режим натисненням відповідних кодових комбінацій на клавіатурі. Перемикачі на ТА

та мережевому інтерфейсі переводяться у праве положення (як показано на рис. 9.11). Після автоматичної конфігурації модемів, що передбачає тестування параметрів телефонного каналу, узгодження протоколів та швидкості передачі у телефонному тракті встановлюється цифровий канал, готовий до обміну даними, подібно як під час з'єднання комп'ютерів через dial-up модеми.

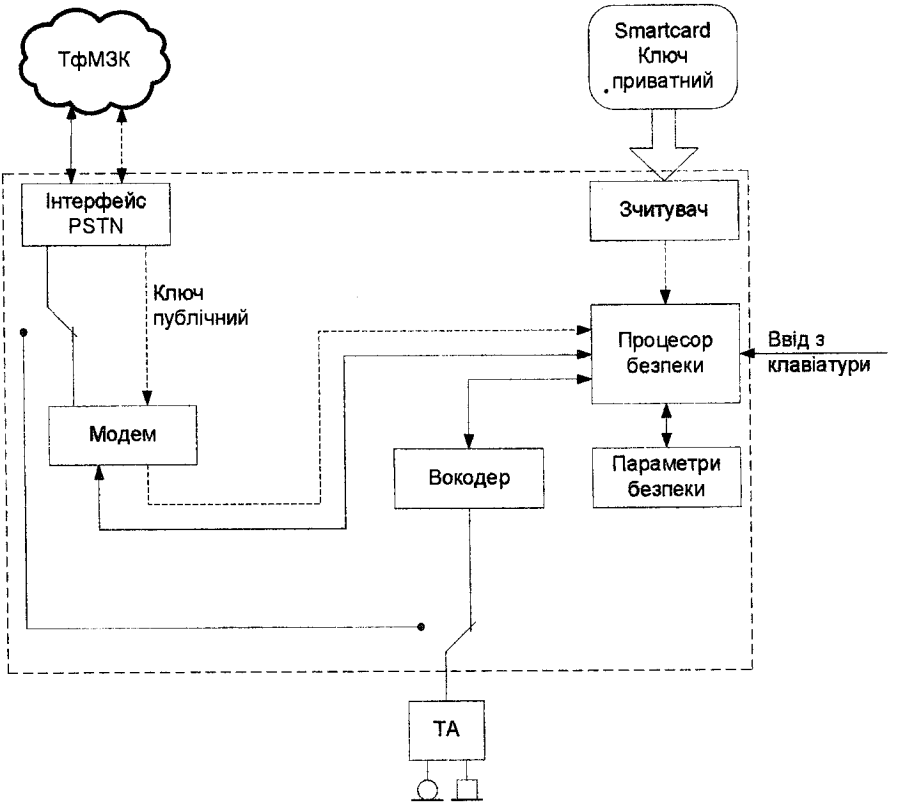



*Рис. 9.11. Структура захищеного телефонного апарата*

Наступний етап передбачає погодження алгоритмів шифрування та формування спільного сеансового криптографічного ключа. Для цього переважно використовуються асиметричні алгоритми, наприклад, Діффі–Хелмана. Необхідні параметри ключів зчитуються із смарт-карти абонентів. Додатковий

захист від несанкціонованого доступу передбачає введення відповідного PIN-коду із клавіатури.

Факт готовності захищеного телефонного тракту сповіщається абонентам синтезованим голосовим повідомленням. З цього моменту телефонна розмова абонентів відбувається у захищенному форматі, який передбачає на передачі компресію телефонних повідомлень та їх шифрування за симетричним алгоритмом у потоковому режимі, а на прийомі – відповідне розшифрування та декомпресію. Компресію-декомпресію виконує вбудований вокодер, а шифрування-розшифрування – процесор безпеки.

## Питання для самоконтролю:

**1.** Охарактеризуйте специфіку мовного сигналу як об'єкта шифрування.

**2.** Подайте класифікацію методів забезпечення конфіденційності телефонних переговорів.

**3.** Наведіть схему та опишіть принцип закриття телефонних повідомлень за методом одностороннього маскування.

**4.** Опишіть зміст перетворень та структуру інвертора спектра телефонних сигналів.

**5.** Вкажіть причину обмежень використання перестановок частотних інтервалів у завданнях захисту телефонних розмов.

**6.** Опишіть зміст методу часових перестановок для захисту телефонних повідомлень від перехоплення. Які чинники обмежують глибину часових перестановок у скремблерах телефонних повідомлень?

**7.** Що спільне та відмінне у роботі частотних та часових скремблерів телефонних повідомлень?

**8.** Які чинники мають дестабілізуючий вплив на якість частотного та часового скремблювання?

**9.** Обґрунтуйте переваги і недоліки цифрових скремблерів.

**10.** Що потрібно розуміти під терміном "проблема останньої милі"?

**11.** Дайте класифікацію методів компресії мовних сигналів. У чому полягає різниця вокодерів і кодерів форми сигналів?

**12.** Обґрунтуйте послідовність використання шифрування і компресії мовного сигналу.

**13.** Опишіть алгоритм встановлення шифрованого телефонного зв'язку у телефонній мережі загального користування.

**14.** Опишіть структуру захищеного ТА.

**15.** Дайте порівняльну оцінку скремблерів і вокодерів у завданнях забезпечення конфіденційності телефонного зв'язку.

# Розділ 10

# ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ВИКОРИСТАННЮ РЕСУРСІВ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

З великою ймовірністю можна стверджувати, що ще на початку XX ст., фактично одночасно із розгортанням перших загальнонаціональних телефонних мереж, знаходилися люди, що намагалися користуватися телефоном безкоштовно. Проте система абонентської плати, що за відсутності щохвилинного обліку розмов накладалася на власників окремих номерів, не завдавала їм істотних фінансових збитків. Лише із автоматизацією телефонних станцій та введенням погодинної оплати за телефонні послуги проблема телефонного шахрайства надзвичайно загострилася. Можливість майже безперешкодного підключення до абонентської лінії з метою одержання доступу до міжміського та міжнародного зв'язку на тлі високих тарифів призвела до того, що проблема фінансової безпеки неабияк загострилася. У періодичній пресі описано чимало випадків, коли дії махінаторів призводили до значних фінансових втрат.

Варто зазначити, що розробка схем протидії несанкціонованому використанню чужих абонентських телефонних ліній не вимагає такого обережного підходу, як у випадку виготовлення виробів зі збирання та захисту інформації. Обмеження у вигляді ліцензування та сертифікації визначаються лише Міністерством зв'язку України подібно до того, як і для звичайних телефонних пристроїв. У цьому розділі розглядаються принципи, технічні засоби та організаційні заходи блокування послуг телефонного зв'язку для неавторизованих осіб.

У результаті вивчення цього розділу студент повинен знати:

- способи, які застосовуються для запобігання несанкціонованому використанню ресурсів телефонного зв'язку;
- принцип роботи та схему індикатора стану АТЛ, блокаторів неавторизованого доступу до АТС і АМТС;
- перелік та зміст пропонованих ВАТ "Укртелеком" організаційно-технічних засобів захисту від стороннього підключення.

## 10.1. Технічні аспекти, що застосовуються для боротьби із телефонним шахрайством

Для запобігання несанкціонованому використанню ресурсів телефонного зв'язку, зокрема телефонному шахрайству, використовуються такі способи:

- сигналізація про нелегальні підключення;
- блокування нелегальних підключень;
- заборона набору номера;
- кодування доступу до телефонної лінії;
- контроль тривалості використання телефонних послуг.

Одержання інформації про нелегальне підключення до АТЛ є ключовим у роботі як пасивних пристроїв технічного захисту, які лише сигналізують про факт такого підключення, так і для пристроїв активного захисту, що використовують таку інформацію для блокування телефонної лінії з метою унеможливлення набору номера із піратського телефонного апарата.

Основні технічні способи одержання інформації про стороннє підключення до лінії ґрунтуються на таких ознаках:

- відсутність напруги у телефонній лінії;
- зниження у 3–4 рази напруги живлення в лінії за покладеної трубки телефонного апарата;
- піддзвонювання телефонного апарата, зумовлене імпульсами набору номера із піратського ТА;
- наявність частотних посилок DTMF коду за покладеної трубки ТА;
- непроходження виклику із АТС на телефонний апарат.

Складніші способи виявлення несанкціонованого підключення ґрунтуються на контролі за резонансним включенням пристроїв до абонентського шлейфа. Під резонансним настроюванням телефонного апарата розуміють роботу обладнання АТС із конкретним телефонним апаратом. У разі підключення телефону з іншими параметрами, чи приєднання в іншому місці шлейфа "АТС–абонент", відбувається неузгодженість (непотрапляння в резонанс), що призводить до спрацьовування індикатора нерезонансного підключення.

Параметри, що характеризують стан узгодження, можуть бути такими:

- еквівалентний опір ТА за піднятої трубки;
- еквівалентний опір за покладеної трубки;

- індивідуальні параметри номеронабирача;
- комплексний опір розмовної частини;
- струм споживання під час виклику;
- струм споживання у розмовному режимі;
- інші параметри (розподіл зарядів, зміна хвильового опору двопровідної лінії під час включення ТА тощо).

## 10.2. Сигналізація про нелегальні підключення

Сигналізація про паралельні підключення здійснюється пристроями пасивного типу, так званими ***індикаторами стану*** телефонної лінії. Принцип роботи індикатора ґрунтується на контролі рівня напруги АТЛ.

Функціональну схему індикатора стану телефонної лінії показано на рис. 10.1. До складу пристрою належать такі функціональні вузли: телефонна розетка ТР для підключення телефонного апарата, діодний міст, компаратор напруги КН, фільтр виклику ФВ, генератор імпульсів ГІ, звуковий індикатор ЗІ, джерело живлення ДЖ.

Діодний міст забезпечує підключення індикатора до телефонної лінії без урахування полярності. Компаратор напруги відстежує поточне значення напруги у телефонній лінії і спрацьовує у разі зниження рівня напруги внаслідок підняття телефонної трубки чи розриву лінії. Фільтр виклику повинен запобігати спрацюванню індикатора під час надходження сигналів виклику із АТС. Генератор імпульсів формує сигнал звукового діапазону, який за спрацювання індикатора подається на звуковий індикатор.

Принцип роботи індикатора стану телефонної лінії полягає у такому. Якщо рівень напруги перевищує, наприклад, 40 В, то компаратор напруги перебуває у нормальному стані, блокуючи роботу генератора імпульсів. Якщо ж на якійсь ділянці лінії була знята трубка або відбувся розрив більш ніж на 1 с, компаратор напруги спрацьовує, запускаючи генератор імпульсів. У результаті звуковипромінювач подає неперервний звуковий сигнал, що сигналізує про використання абонентської телефонної лінії або її розрив. Під час повернення телефонної лінії у стан очікування (напруга, більша за 40 В) індикатор знову переходить у початковий стан.

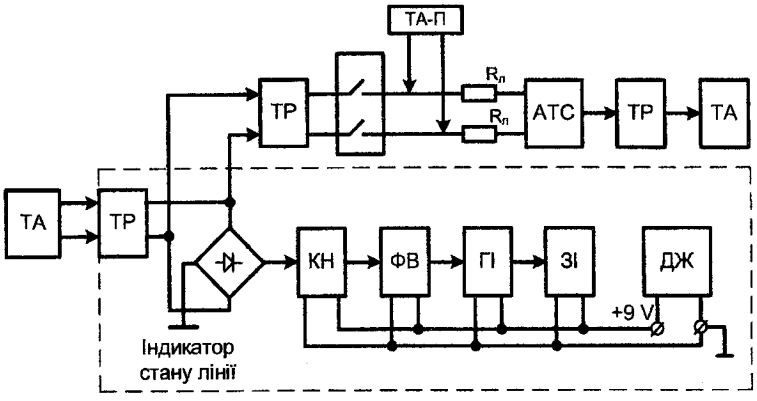



*Рис. 10.1. Функціональна схема індикатора стану телефонної лінії*

Для підвищення зручності та забезпечення можливості ретроспективного аналізу подій, що відбулись у контрольованій телефонній лінії, потрібно використати деякий запам'ятовувальний пристрій. Якщо, наприклад, з'єднати схему індикатора стану лінії і електронний годинник, можна одержати простий лічильник часу розмови, що дасть змогу оцінити часу піратського підключення за відсутності власника телефону. Якщо годинник не обнулювати, то лічильник часу підсумує час усіх розмов (до 24-х годин). Лічильник часу може бути також застосований для аналізу частоти використання телефонного апарата.

## 10.3. Блокування нелегальних підключень

Активний технічний захист телефонної лінії від самовільного підключення на відміну від пасивного передбачає не лише сигналізацію (звукову чи світлову) про цю подію, але й безпосереднє втручання у процес встановлення і проведення зв'язку з піратського апарата з метою запобігання реальним фінансовим втратам.

Залежно від призначення розрізняють такі пристрої активного захисту від піратських підключень:

- ***блокатор типу "заглушка"***, що унеможливлює будь-яке використання телефонної лінії;

- ***блокатор паралельного підключення***, що запобігає спробам ведення розмов із паралельного телефонного апарата.

Пристрої активного захисту абонентських телефонних ліній можуть встановлюватися як на вихідних клемах АТС, так і на вході абонентських термінальних пристроїв. Місце установки блоків захисту визначається необхідністю виконання тих чи інших завдань протидії.

Перевагою установки захисних пристроїв на кросі АТС є охорона шлейфа "АТС-абонент" по усій його довжині, навіть за його розриву. Недоліком є неможливість абонентом самостійно визначати тактику захисту.

До переваг індивідуальної установки пристроїв захисту можна зарахувати можливість вибору типу пристроїв, оперативність реагування на усі випадки самовільних підключень, а також, що важливо, невтручання до протоколу роботи АТС. Недолік полягає у неможливості контролювати усю довжину шлейфа, особливо під час його розриву.

Саме тому під час проектування апаратури активного захисту визначальною є постановка завдання протидії. Найреальніше для більшості користувачів АТС завдання формулюється у такий спосіб: у разі самовільних підключень фінансові збитки необхідно звести до мінімуму, по можливості, до нуля.

Існує два ступені ефективності застосування активних засобів захисту:

- зрив піратського підключення – 100 % уникнення фінансових збитків;
- створення перешкод під час піратського підключення – зниження розміру фінансових збитків.

Втручання у процес зв'язку має на меті реалізацію функції заборони набору номера за одним із таких способів:

**1.** Короткочасний розрив лінії з метою встановлення апаратури АТС у вихідний стан (лінія вільна). Йдеться про розрив одного з лінійних проводів на час, більший за 400–800 мс (за ДСТУ 7153).

**2.** Шунтування лінії резистивно-ємнісною ланкою. У цьому випадку за допомогою резистора обмежується амплітуда імпульсів набору номера, що не дає змоги АТС визначити номер і здійснити з'єднання, а ємність призначена для придушення посилок тонового (частотного чи DTMF) набору, а також для послаблення мовного сигналу, якщо з'єднання все ж таки відбулося.

**3.** Перешкоди імпульсному і частотному набору номера. Йдеться про спотворення форми імпульсів набору, зменшення їхньої кількості тощо, що унеможливлює однозначне визначення номера і встановлення зв'язку.

### 10.3.1. Блокатор типу "заглушка"

У разі невикористання абонентом телефонного апарата впродовж тривалого часу (відрядження, відпустка тощо) рекомендується використовувати активні засоби захисту лінії від паралельного підключення (тобто без розриву шлейфа "АТС-абонент").

Такі пристрої повинні виконувати дві основні функції:

- за спроби набору номера з паралельно підключеного апарата здійснити заборону набору методом шунтування лінії;
- під час приймання посилань виклику від АТС (100 В, 25 Гц) пристрій не повинен шунтувати лінію (система заборони не включається).

Функціональну схему блокатора типу "заглушка" показано на рис. 10.2.

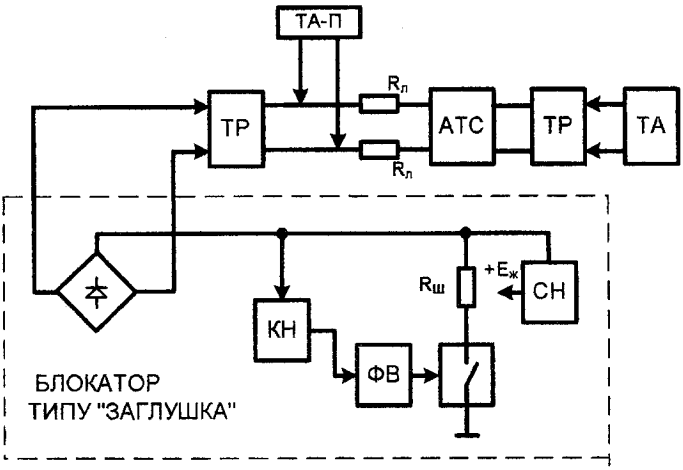



*Рис. 10.2. Функціональна схема блокатора типу "заглушка"*

До складу пристрою зараховують діодний міст, компаратор напруги КН, фільтр виклику ФВ, а також шунтувальний резистор $R_Ш$ із ключем та стабілізатор напруги СН, що здійснює живлення усіх елементів схеми. Пристрій оснащений роз'ємом, що включається у телефонну розетку замість основного ТА (тобто виконується у вигляді "заглушки").

У вихідному стані, коли на лінії присутня напруга понад 40 В, ключ розімкнений і лінія не шунтується опором $R_Ш$. За спроби набору номера з запізненням близько 2 с заряджається RC-ланка фільтра виклику, зумовлюючи спрацювання ключа та шунтування телефонної лінії опором $R_Ш$, що унеможливлює прийом АТС сигналів абонентської сигналізації (заборона подальшого набору). Значення опору $R_Ш$ підібране так, щоб під час відключення від лінії піратського телефону зростання напруги призвело до спрацювання компаратора напруги, тобто розмикання ключа і скасування шунтування лінії опором $R_Ш$ (зняття заборони набору номера).

### 10.3.2. Блокатор паралельних телефонних апаратів

За потреби експлуатації блока захисту разом із штатним телефонним апаратом він повинен виконувати такі функції, як:

- заборона набору номера у разі паралельного набору;
- відсутність шунтування лінії під час приймання посилань виклику з АТС;
- автоматичне відключення системи заборони набору номера за підняття трубки штатного ТА.

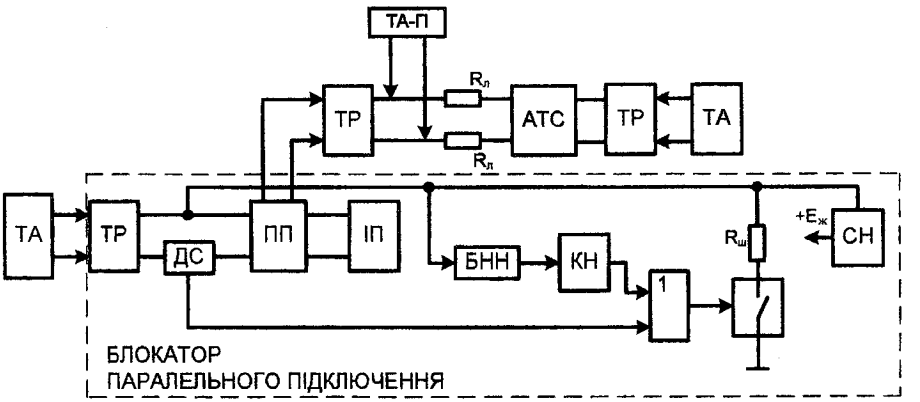



*Рис. 10.3. Функціональна схема блокатора паралельного підключення*

Функціональну схему блокатора паралельного підключення показано на рис. 10.3, яка містить такі вузли: телефонну розетку (ТР), датчик струму (ДС) для відстеження підняття трубки на штатному (ТА), перемикач та індикатор полярності (ПП) та (ІП) для забезпечення необхідної полярності, блокатор несанкціонованого набору (БНН), компаратор напруги (КН), пристрій, що реалізує функцію АБО для сигналів керування ключем шунтування лінії, опір шунтування $R_Ш$, стабілізатор напруги СН.

Блок захисту підключається у розрив телефонної лінії з дотриманням полярності та встановлюється поблизу ТА, наприклад, у телефонній розетці.

## 10.4. Запобігання доступу до міжміської автоматичної телефонної станції

### 10.4.1. Блокування цифри "0"

На вітчизняних телефонних мережах доступ до ресурсів автоматичного міжміського і міжнародного зв'язку здійснюється через набір цифри "0". Якщо необхідно заборонити лише міжміський зв'язок, звичайний блок захисту від паралельного набору не годиться – він не має вибірковості.

На рис. 10.4 показано функціональну схему блокатора цифри "0", до якої належать телефонна розетка (ТР), діодний міст, компаратор напруги (КН), схема запуску лічильника (СЗЛ), лічильник імпульсів (СТ), схема включення заборони (СВЗ), ключ шунтування лінії з опором шунтування $R_Ш$, стабілізатор напруги (СН).

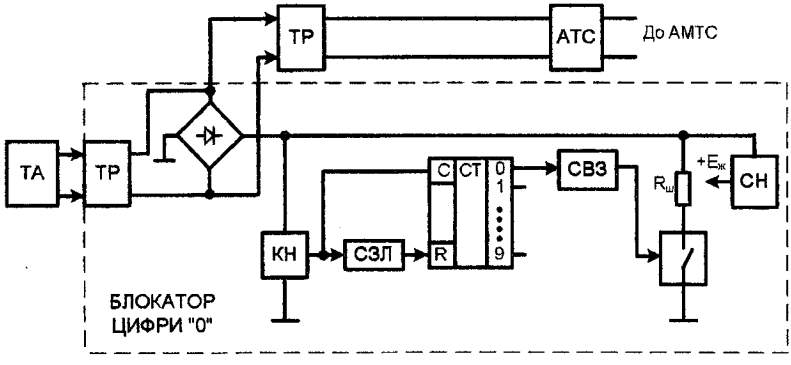



*Рис. 10.4. Функціональна схема блокатора цифри "0"*

### 10.4.2. Обмеження формату набору

Альтернативний спосіб заборони доступу до засобів міжміського зв'язку полягає в обмеженні кількості цифр у номері, який набирається. Практика показує, що здебільшого максимальна кількість цифр номера міського зв'язку не перевищує восьми (5–7-значний номер плюс одна цифра відомчої АТС, найчастіше "9"). Тоді вихід на міжміський зв'язок має таку послідовність набору: "0" + код міста (мінімум три цифри) + номер абонента (мінімум п'ять цифр), що в сумі становить дев'ять цифр і більше. Отже, якщо обмежити номер вісьмома цифрами, можна застрахувати себе від дорогих міжміських і тим більше міжнародних розмов.

Функціональну схему обмежувача формату набору показано на рис. 10.5. Вона містить такі вузли: телефонну розетку (ТР), датчик струму, перемикач та індикатор полярності (ІПП) та (ІП), формувач рахункових імпульсів (ФРІ), фільтр виклику (ФВ), лічильник імпульсів (СТ), пристрій, що реалізує функцію АБО для сигналів обнулення лічильника, схему блокування лічильника (СБЛ), обмежувач часу заборони (ОЧЗ), ключ і опір шунтування $R_{Ш}$, пристрій АБО для сигналів керування ключем шунтування, стабілізатор напруги (СН).

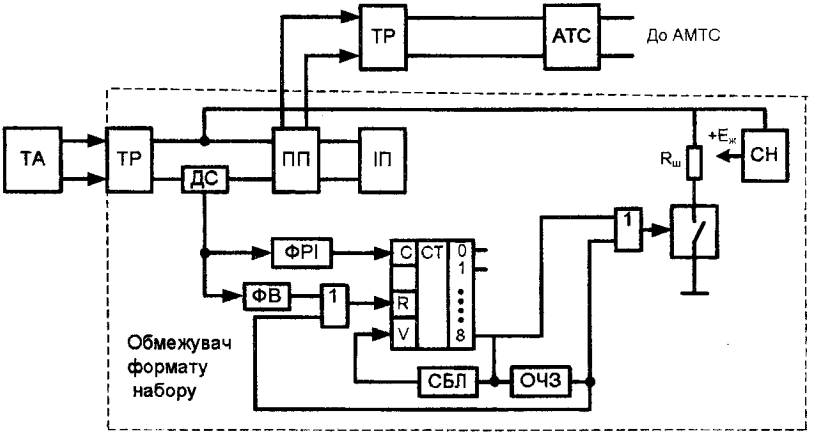



*Рис. 10.5. Функціональна схема обмежувача формату набору*

Захисний ефект досягається тим, що на усіх міжміських АТС, через їхнє велике завантаження, скорочено час очікування кожної цифри номера. Якщо

під час набору міжміського коду виникне пауза між цифрами більше 8–10 с, АТС дає відбій у лінію. Крім того, за самовільного підключення абонент може не припинити подальший набір номера (він не знає, що лінія зашунтована), і відповідно дев'ята і наступна цифри номера набираються впусту, тому що АТС їх не сприймає. Після того, як трубка була покладена на апарат, через заданий час схема повернеться у вихідний стан.

Під час експлуатації такої схеми ті абоненти, які використовуватимуть звичайні внутрішньоміські номери, повинні робити обов'язкову 2–4-секундну паузу між наборами різних номерів, щоб унеможливити включення заборони.

Існують також пристрої, які запобігають несанкціонованому використанню послуг телефонного зв'язку у спосіб кодування доступу до телефонної лінії. На підприємствах ефективним може виявитися принцип захисту, що ґрунтується на контролі використання службових телефонів фіксуванням тривалості чи архівації телефонних розмов.

## 10.5. Рекомендовані ВАТ "Укртелеком" організаційно-технічні засоби захисту від стороннього підключення

Для уникнення випадків несанкціонованого використання послуг і засобів зв'язку оператори місцевих телефонних мереж під час укладання договорів з абонентами повідомляють їх про можливість:

- обмеження виходу на міжміську та міжнародну телефонну мережу встановленням відповідної категорії АВН. Для цього потрібно звернутися з письмовою заявою про відключення свого номера телефону від автоматичного виходу на міжміську (чи міжнародну) телефонну мережу. При цьому у абонента залишається можливість замовити таку розмову через оператора зв'язку;
- користування додатковими послугами АТС, які забезпечують вихід на міжміську та міжнародну телефонну мережу за паролем.

З метою захисту інтересів абонентів та мережі оператори міжміської (міжнародної) телефонної мережі можуть, за наявності необхідних програмних та технічних засобів, проводити оперативний контроль користування послугами з кожного телефону (моніторинг). Під час виявлення різких відхилень

(суми, видів послуг тощо) оператор вживає заходи щодо з'ясування їхніх причин (можливого стороннього підключення, неузгодженого користування телефоном тощо). Залежно від характеру виявлених відхилень у користуванні послугами оператор може застосовувати такі заходи:

- попередження абонента за допомогою автоматизованої інформаційної системи;
- продзвонювання абонента;
- виставлення термінового рахунку.

Для запобігання випадкам несанкціонованого користування послугами міжміського та міжнародного телефонного зв'язку абонент може:

- присвоїти номеру телефону категорію АВН, яка відповідає реальним потребам абонента у послугах міжміського та міжнародного телефонного зв'язку і у платних інтелектуально-довідкових послугах;
- провести роз'яснювальну роботу серед осіб, які мають доступ до користування телефоном (абонентським пристроєм), щодо порядку користування послугами, особливо послугами з високими тарифами;
- контролювати доступ зі свого телефону до послуг міжміського та міжнародного телефонного зв'язку, платних інтелектуально-довідкових послуг типу "0-900" за наявності технічної можливості (наприклад, на цифрових АТС) користуватися паролем доступу. Вартість цієї послуги незначна;
- при здачі квартири (приміщення) з телефоном в оренду проконсультуватися з відповідними службами оператора зв'язку стосовно методів захисту від несанкціонованого користування телефоном і контролювати оплату за послуги з цього телефону. Здаючи квартиру в найм, можна проводити переоформлення телефону на орендаря, оскільки після цього уся відповідальність за проведення оплати за послуги зв'язку на час оренди лягає на орендаря. Зворотне переоформлення проводиться безкоштовно;
- виконувати вимоги безпечного користування абонентськими пристроями, щоб запобігти сторонньому підключенню. Не використовувати несертифіковані апарати (абонентські пристрої), зокрема з радіопродовжувачем. Користуючись телефонним апаратом з радіопродовжувачем, стежити, щоб телефонна трубка у режимі чекання знаходилась на базовому апараті;
- скористатись послугою "Термінова довідка", завдяки якій ви матимете можливість двічі на добу отримувати інформацію про проведені з вашого телефону міжміські та міжнародні телефонні розмови, та вчасно на це реагувати;

- негайно звертатися до оператора місцевої телефонної мережі або до оператора міжміської та міжнародної телефонної мережі у разі появи ознак стороннього підключення і виконувати їх рекомендації.

ВАТ "Укртелеком" проводить такі заходи із покращання захищеності абонентських ліній від несанкціонованих підключень:

- влаштовує розподільні шафи (РШ) місцевих телефонних мереж, які замкнено на замки;
- РШ обладнує охоронною сигналізацією, яка виводиться на ПЕОМ диспетчера підприємства електрозв'язку, а в багатьох підприємствах – на пульт органів МВС;
- укладає договір з фірмою НВФ "ІНТЕГДІФ" на розробку "Системи виявлення несанкціонованих підключень до абонентських телефонних ліній" (шифр "Бар'єр"). Сьогодні система проходить сертифікаційні випробування у ДКЗіУ;
- проводить роз'яснювальну роботу з ЖЕКами про необхідність зачинення підвальних приміщень та розподільних ніш у будинках.

## Питання для самоконтролю:

1. Які принципи можуть бути використані для роботи пристроїв контролю санкціонованого використання послуг телефонного зв'язку?
2. Які ознаки визначають одержання інформації про стороннє підключення до лінії?
3. Назвіть параметри, що характеризують стан узгодження з'єднання "абонент-АТС".
4. Наведіть функціональну схему та поясніть роботу індикатора стану телефонної лінії.
5. Які способи заборони набору номера можуть бути використані під час створення блокаторів доступу до АТС?
6. Для чого використовується блокатор типу "заглушка"? Наведіть функціональну схему та поясніть роботу цього пристрою.
7. Які функції повинен виконувати блокатор паралельних телефонів? Наведіть функціональну схему та поясніть роботу цього пристрою.

**8.** У чому полягає особливість пристроїв блокування міжміського телефонного зв'язку? Які принципи можуть бути закладені в системи контролю доступу до автоматичної міжміської телефонної станції?

**9.** Наведіть функціональну схему та поясніть роботу блокатора цифри "0".

**10.** Наведіть функціональну схему та поясніть роботу обмежувача формату набору.

**11.** Розкрийте зміст рекомендацій ВАТ "Укртелекому" для протидії телефонному шахрайству.

**12.** Які організаційно-технічні засоби, запропоновані ВАТ "Укртелекому", може застосувати абонент для запобігання випадкам несанкціонованого користування послугами міжміського та міжнародного телефонного зв'язку?

# ЛІТЕРАТУРА


1. Абалмазов Э.И. Новая технология защиты телефонных разговоров // Специальная техника. – 1998. – № 1. – С. 4–8.

2. Абубакиров Б.А., Гудков К.Г., Нечаев Э.В. Измерение параметров радиотехнических цепей / под ред. В.Г. Андрущенко, Б.П. Фетеева. – М.: Радио и связь, 1984. – 284 с.

3. Балахничев И.Н., Дрик А.В., Крупа А.И. Борьба с телефонным пиратством. – Минск: ОМО "Наш город", 1998. – 116 с.

4. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.:ООО "ТИД ДС", 2001. – 698 с.

5. Беллами Дж. Цифровая телефония / пер. с англ. – М.: Радио и связь, 1986. – 544 с.

6. Берлик Б.З., Брискер А.С. и др. Справочник. Городская телефонная связь. – М.: Радио и связь, 1987. – 280 с.

7. ГОСТ 7153-85. Аппараты телефонные общего применения. Общие технические условия.

8. Дворянкин С.В., Клочкова Е.Н., Калужин Р.В. Маскирование речевых сообщений на основе современных компьютерных технологий // Специальная техника. – 2001. – № 3. – С. 37–45.

9. Дикмарова Л.П., Павлюк Р.П. Электромагнитное поле скрученной в группу и в повив двухпроводной линии // Электросвязь. – 1984. – № 3.

10. Дикмарова Л.П., Ничога В.А. Особенности паразитных излучений коаксиальных линий связи: матер. Междунар. науч.-техн. конф. "Повышение эффективности систем защиты информации" ("Защита-97"). – К., 1997. – С. 130–135.

11. ДСТУ 2621-94. Зв'язок телефонний. Загальні поняття. Телефонні мережі. Терміни та визначення.

12. Назаров М.В., Прохоров Ю.Н. Методы цифровой обработки и передачи речевых сигналов. – М.: Радио и связь, 1985.

13. НД ТЗІ 4.7-001-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань.

14. НД ТЗІ 2.3-002-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.

15. НД ТЗІ 2.3-003-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.

16. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах.– М.: Энергоатомиздат, 1996. – 304 с.

17. Лысов А.В., Остапенко А.Н. Телефон и безопасность (Проблемы защиты информации в телефонных сетях). – СПб.: Политехника, 1997.

18. Кащеев В.И. Мониторинг телефонной сети. – М., 1995. – 52 с.

19. Кизлюк А.И. Справочник по устройству и ремонту телефонных аппаратов зарубежного и отечественного производства. – М.: Антелеком, 1998.

20. Кравченко В.Б. Защита речевой информации в каналах связи // Специальная техника. – 1999. – № 4.

21. Обзор активных технических средств защиты // Защита информации. – 1997. – № 6. – С. 61–63.

22. ОСТ 45.36-97. Линии кабельные, воздушные и смешанные городских телефонных сетей. Нормы электрические эксплуатационные // http://1gost.net.ru/doc-33032.html.

23. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика: учеб. Пособ. – 3-е изд., испр. и доп. – М.: Радио и связь, 2004. – 504 с.

24. Попугаев Ю.И. Телефонные переговоры: способы защиты. – М., 1995. – 84 с.

25. Сайт Державної служби спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua.

26. Сайт ВАТ "Укртелекому" http://ukrtelecom.ua.

27. Системы и сети передачи информации: учеб. пособ. для вузов / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. – М.: Радио и связь, 2001. – 336 с.

28. Сударев И.В. Криптографическая защита телефонных сообщений // Специальная техника. – 1998. – № 2. – С. 47 – 55.

29. Телекоммуникационные системы и сети: учеб. пособ.: в 3-х т. – Т.1: Современные технологии / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов; под ред. В.П. Шувалова. – 3-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2005. – 647 с.

30. Хома В.В. Інформаційна безпека абонентів стаціонарних телефонних мереж // Вісник Нац. ун-ту "Львівська політехніка". – 2008. – № 608. – С. 74–85.

31. Хома В.В. Методи і засоби технічного захисту інформації на абонентських телефонних лініях // Вісник Нац. ун-ту "Львівська політехніка". – 2009. – № 639. – С. 87–94.

32. Хома В.В. Методи та засоби забезпечення конфіденційності телефонних повідомлень // Сучасна спеціальна техніка. – 2009. – № 3(18). – С. 50–59.

33. Хома В.В. Основи збору, передачі та оброблення інформації: навч. посіб. – Серія "Дистанційне навчання". – № 43. – Львів: Вид-во Національного університету "Львівська політехніка", 2007. – 312 с.

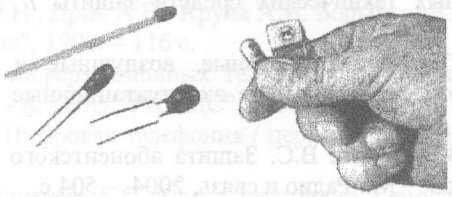
34. Хорев А.А. Способы и средства защиты информации: учеб. пособ. – М.: МО РФ, 2000. – 316 с.

35. Хорн Д. Усовершенствуй свой телефон / пер. с англ. – М.: БИНОМ, 1995.

# ДОДАТКИ

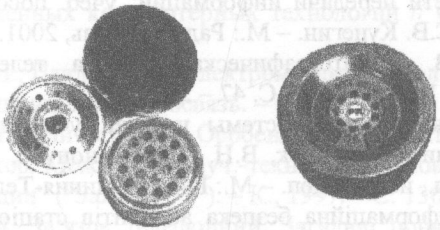
*Додаток 1*

**Приклади конструктивного виконання телефонних закладок**
(за матеріалами сайту www.analitic.info)



*а* *б*

*Рис. Д.1. Телефонні закладки, виконані у вигляді конденсаторів:*
*а – РК-130; б – РК-130-S*



*а* *б*

*Рис. Д.2. Телефонні закладки, виконані у вигляді мікротелефонних капсул:*
*а – РК-110-S; б – РК-155*

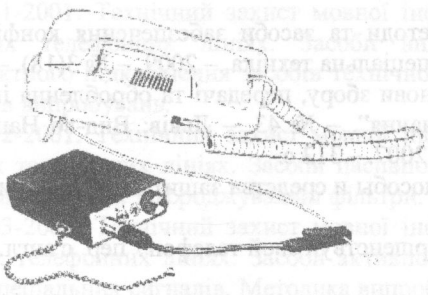


*Рис. Д.3. Безконтактне знімання інформації із телефонної лінії за допомогою індуктивного адаптера SNG-4525 Paslm*

*Додаток 2*

**Призначення та основні технічні характеристики універсального аналізатора проводових комунікацій "ULAN-2"**

Універсальний лінійний аналізатор "ULAN-2" (рис. Д.4) призначений для виявлення фактів несанкціонованих підключень у таких проводових комунікаціях, як:

- телефонні лінії;
- електричні електромережі змінного струму;
- комп'ютерні мережі;
- лінії охоронно-пожежної сигналізації.

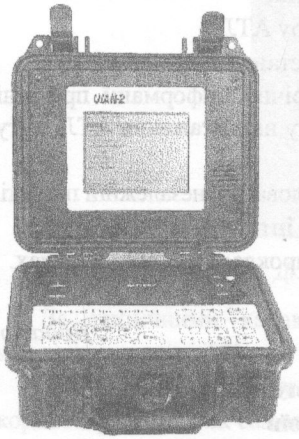


*Рис. Д.4. Зовнішній вигляд приладу "ULAN-2"*

Основні технічні характеристики приладу "ULAN-2":

I. Прилад "ULAN-2" допомагає виявляти:

1. У телефонних лініях (без відключення від АТС і без наявності попередньої інформації):

- послідовні підключення з еквівалентним опором більше 30 Ом;
- паралельні підключення у режимі із струмом споживання більше 0,1 мА;
- високочастотні сигнали у лінії в діапазоні 0,02 – 30 Мгц напругою більше 10 мВ за симетричного і несиметричного підключень;
- низькочастотні сигнали у діапазоні 20 – 20000 Гц напругою понад 10 мВ.

2. У лініях електромережі змінного струму під напругою:

- "сторожові пристрої" із струмом споживання більше 0,1 мА;
- високочастотні сигнали у діапазоні 0,02 – 30 МГц з напругою понад 10 мВ.

3. У знеструмлених лініях:

- паралельні підключення із активним опором до 200 МОм;
- послідовні підключення із активним опором більше 1 Ом;
- паралельні підключення через конденсатор із сталою часу понад 100 мкс;
- наявність елементів з вираженою нелінійністю від 5 % і вище в діапазоні напруг 0–100 В;
- наявність реактивних елементів з ємністю понад 100 пФ і індуктивністю більше 10 мГн (без урахування власних параметрів лінії).

4. У будь-яких лініях (зокрема без відключення від напруги) за наявності заздалегідь отриманої рефлектограми:

- послідовні підключення з еквівалентним опором більше 1 Ом;
- паралельні підключення з еквівалентною ємністю більше 5 пФ;
- паралельні відгалуження будь-якої протяжності;
- відновлені порушення цілісності лінії (розриви з подальшим скручуванням);
- порушення лінії, пов'язані з установкою безконтактних магнітних знімачів;
- порушення ізоляції проводів.

II. Окрім того, прилад "ULAN-2" можна використовувати для:

- вимірювання напруги постійного і змінного струмів у лінії;
- вимірювання опору, ємності та індуктивності лінії;
- вимірювання струму короткого замикання і опору АТЛ;
- прослуховування аудіосигналів у лінії із використанням навушників;
- виведення на екран вбудованого дисплея графічної інформації про лінію: вольт-амперну і перехідну характеристики, характеристику навантаження АТЛ, фігури Лісажа, імпульсні рефлектограми ліній;
- зберігання числових і графічних результатів вимірювань у незалежній пам'яті;
- передавання її на комп'ютер високошвидкісним інтерфейсом USB;
- спільно із адаптером UP-7 простежувати трасу прокладання лінії у стінах.

*Додаток 3*

**Основні характеристики засобів фізичного знищення телефонних закладних пристроїв**

| Назва характеристик | Тип пристрою | | |
|---|---|---|---|
| | "Кобра" | КС-1300 | КС-1303 |
| Напруга на виході, В | 1600 | – | – |
| Потужність імпульсу, ВА | – | 15 | 50 |
| Режими роботи | Автоматичний, Ручний | Автоматичний, Ручний | Ручний |
| Час неперервної роботи в автоматичному режимі | 20 с | 24 години | – |
| Час неперервної роботи в ручному режимі | 10 хв | – | – |
| Часові інтервали, встановлювані таймером | – | від 10 хв до 2 діб | – |
| Габаритні розміри, мм | 65× 170×185 | 170×180×70 | 170×180×70 |
| Напруга живлення, В | 220 | 220 | 220 |
| Кількість під'єднуваних телефонних ліній | 1 | 2 | 2 |

*Додаток 4*

## Призначення та характеристика приладу технічного захисту інформації абонентів телефонної мережі "СКЕЛЯ-1"

Прилад "СКЕЛЯ-1" (рис. Д.5) призначений для захисту кінцевих пристроїв абонентів від просочування інформації лініями телефонної мережі.

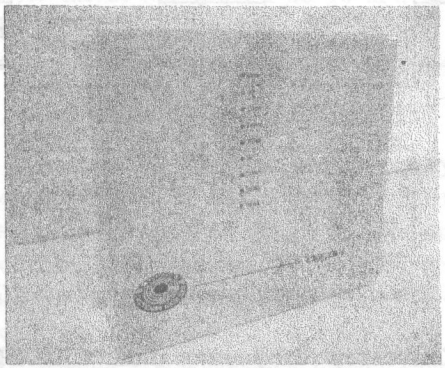


*Рис. Д.5. Зовнішній вигляд приладу "СКЕЛЯ-1"*

За технічними характеристиками прилад відповідає чинним нормативним документам у галузі ТЗІ.

До складу приладу "СКЕЛЯ-1" входять чотири пристрої, які можуть використовуватися і як самостійні (рис. Д.6):

- аналізатор телефонної лінії "СКЕЛЯ-1А";
- комутатор телефонних ліній "СКЕЛЯ-1К";
- фільтр телефонних ліній "СКЕЛЯ-1Ф";
- генератор шуму "СКЕЛЯ-1Г".

### 1. Аналізатор стану телефонної лінії "СКЕЛЯ-1А"

Аналізатор стану призначений для контролю аналогової телефонної лінії від несанкціонованого паралельного підключення у режимах "Чекання" і "Розмова". Підключається в абонентську мережу автоматичних телефонних станцій паралельно до кінцевого пристрою абонента. Електроживлення аналізатора забезпечується від АТС.

Аналізатор забезпечує:

- контроль абонентської лінії від несанкціонованого паралельного підключення у режимі "Чекання" пристроєм, внутрішній опір якого знаходиться у межах 0,3–150 кОм і час підключення не менший за 0,5 с;

- контроль абонентської лінії від несанкціонованого паралельного підключення у режимі "Розмова" пристроєм, внутрішній опір якого знаходиться у межах до 5 кОм і час підключення, не менший за 0,5 с;
- контроль абонентської телефонної лінії від обриву одного або двох проводів зразу з боку АТС у режимі очікування.

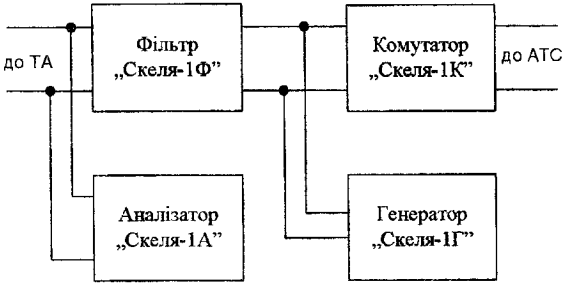



*Рис. Д.6. Схема включення компонентів приладу "Скеля-1"*

## 2. Комутатор телефонних ліній "СКЕЛЯ-1К"

Комутатор призначений для автоматичного включення або відключення кінцевих абонентських пристроїв від ліній аналогової телефонної мережі. Підключається в абонентську мережу автоматичних телефонних станцій послідовно до кінцевого пристрою абонента. Електроживлення забезпечується від мережі змінного струму з номінальною напругою 220 В і частотою 50 Гц.

Комутатор забезпечує:

- автоматичну комутацію каналу телефонної мережі;
- повну гальванічну розв'язку кінцевого абонентського пристрою від телефонної лінії у режимі "Чекання" (телефонна трубка на пристрої покладена);
- послаблення сигналу витоку мовної інформації у режимі "Чекання" не менше 120 дБ;
- автоматичне підключення кінцевих абонентських пристроїв ліній аналогової телефонної мережі у режимі "Виклик".

## 3. Загороджувальний фільтр телефонних ліній "СКЕЛЯ-1Ф"

Фільтр призначений для захисту мовної інформації від витоку абонентськими телефонними лініями зв'язку у режимі чекання виклику. Підключається в абонентську мережу автоматичних телефонних станцій послідовно до кінцевого пристрою абонента. Електроживлення фільтра забезпечується від АТС.

Фільтр забезпечує:

- послаблення сигналу в активному режимі не більше 1 дБ;
- захист абонентських пристроїв від високочастотного нав'язування на частоті до 100 МГц;
- згасання у смузі частот від 300 до 3400 Гц за рівня вхідного сигналу 0,1 В – не менше – 65 дБ;
- згасання у смузі частот від 150 Гц до 10 кГц за рівня вхідного сигналу 10,0 В – не більше – 3 дБ;
- згасання на частоті 50 кГц за рівня вхідного сигналу 10 В – не менше 10 дБ.

### 4. Генератор шуму "СКЕЛЯ-1Г"

Генератор шуму призначений для технічного захисту мовної інформації від несанкціонованого знімання із абонентських ліній аналогової телефонної мережі. Підключається в абонентську лінію автоматичних телефонних станцій паралельно до кінцевого пристрою абонента. Електроживлення забезпечується від мережі змінного струму з номінальною напругою 220 В і частотою 50 Гц.

Генератор забезпечує:

- можливість включення і відключення подачі сигналу шуму у телефонну лінію;
- подачу сигналу шуму у телефонну лінію у режимі "Чекання", амплітудне значення якого повинно бути не меншим за 1,5 В;
- можливість створення вихідного сигналу "псевдобілого" шуму (псевдовипадкової перешкоди) в діапазоні частот 180–15000 Гц;
- ентропійний коефіцієнт якості сигналу шуму не менший за 0,8;
- глибину регулювання рівня шумового сигналу у робочому діапазоні частот не менше 40 дБ.

*Додаток 5*

## Система комплексного захисту телефонної лінії SEC-2004 ANTI FLY

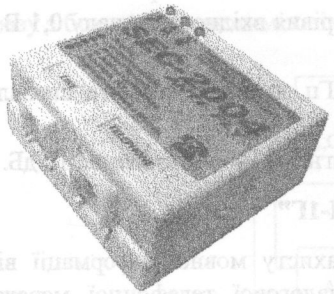


*Рис. Д.7. Зовнішній вигляд мікрокомп'ютерної системи SEC-2004 ANTI FLY*

Мікрокомп'ютерна система комплексного захисту телефонної лінії SEC-2004 ANTI FLY (рис. Д.7) призначена для контролю стану АТЛ, індикації прослуховування телефонних розмов та протидії засобам технічної розвідки.

Основні функції:

- "АКТИВІЗАТОР ДИКТОФОНІВ" – постійна дія, "змотування" носія і витрачання ресурсу елементів живлення диктофонів за будь-якого способу підключення до АТЛ, зокрема навіть індуктивним (безконтактним) способом.
- "АНТИ-ЖУЧОК" – захист від радіопередавачів і спецапаратури на АТЛ.
- "АНТИ-ПАРАЛЕЛЬ" – світлодіодна та аудіосигналізація у разі підключення до АТЛ паралельних телефонів або закладних пристроїв.
- "ANTI-FLY" – індикація підключення телефонних закладок для дистанційного прослуховування телефонних ліній.
- "АНТИ-ВУХО" – індикація підключення пристроїв типу "телефонне вухо" з метою прослуховування приміщення телефонною лінією.
- "УЛЬТРА ТОН" – низькочастотний генератор для придушення радіозакладок.
- "OVERVOLTEGE PROTECTION" – захист телефонів від перенапруг на лінії.
- Світлодіодна індикація стану лінії.
- Аудіоіндикація прослуховування тільки у трубці телефону.
- Індикація тимчасового відключення телефонної лінії.
- Захист від прослуховування приміщень апаратурою, що використовує метод "високочастотного нав'язування".
- Дистанційний кодовий доступ (тризначний код виробу і тризначний пароль користувача) із будь-якого виділеного телефону і/або локальне встановлення чутливості сенсорів.
- Повна "прозорість" для штатного телефонного апарата.
- Робота без джерел живлення.

*Додаток 6*

**Пристрій одностороннього маскування телефонних переговорів "Щит"**

Пристрій маскування "Щит" (рис. Д.8) забезпечує захист за допомогою акустичного маскування мови у телефонних каналах зв'язку без використання криптографічних алгоритмів.

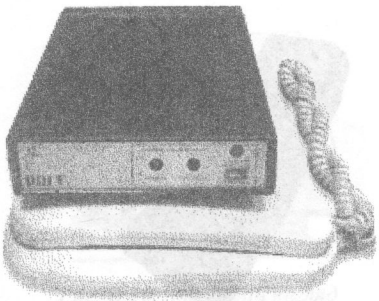


*Рис. Д.8. Зовнішний вигляд пристрою маскування "Щит" (Білорусь)*

Основні характеристики:

- Оперативність – можливість приймання конфіденційних повідомлень абонента, що використовує таксофон або мобільний зв'язок (включаючи GSM, AMPS/DAMPS, CDMA і транковий).
- Мобільність – можливість швидкого підключення до будь-якого телефонного апарата.
- Необхідність установки пристрою "Щит" тільки у приймаючого абонента.
- Маскування акустичної інформації й неможливість її прослуховування впродовж усього телефонного тракту, від абонента до абонента, включаючи АТС, незалежно від способу прослуховування й застосовуваних для цього технічних засобів.
- Мова, замаскована одним "Щитом", не може бути демаскована іншим, аналогічним пристроєм (характеристики маскувального шуму відомі лише пристрою, який його згенерував).
- Низький рівень шуму й повна розбірливість мови у телефонному апараті приймаючого абонента.
- Відсутність затримки, одержання інформації у реальному масштабі часу (на відміну від скремблерів і захищених вокодерів).
- Неможливість компенсації перешкоди й виділення мовного сигналу сучасними засобами шумоочистки.
- Неможливість ідентифікації мовця за голосом.
- Ефект "раптовості", що досягається несподіваним для зловмисника включенням маскування командою абонента.

*Додаток 7*

## Телефонний скремблер із акустоелектричним перетворенням ACS-2


*Рис. Д.9. Зовнішній вигляд скремблера ACS-2 фірми Research Electronics (США)*

Телефонний скремблер конструктивно виконаний у вигляді накладки на телефонну трубку (рис. Д.9). Забезпечує захист від прослуховування телефонних розмов за допомогою часо-частотних перетворень мовного сигналу. Сумісний із різними телефонними апаратами, зокрема радіотелефонами. Для входу у захищений режим потрібно ввести Секретний код (пароль), який відомий обом абонентам. Кількість ключів – 13122. Час встановлення захищеного режиму – 2,5 с. Вага пристрою – 285 г.

*Додаток 8*

## Телефонний скремблер "Орех-II"

Телефонний скремблер "Орех-II" (рис. Д.10) – вітчизняний виріб, призначений для забезпечення конфіденційності переговорів на телефонних каналах внутрішніх, міських та міжміських мереж за допомогою часо-частотних перетворень телефонних сигналів.

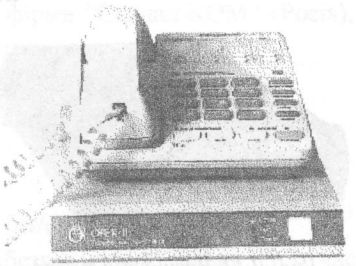


*Рис. Д.10. Зовнішній вигляд телефонного скремблера "Орех-II" (Україна)*

Телефонний скремблер "Орех-II" має такі основні технічні характеристики:

- Якість розмови у повнодуплексному режимі – не гірше 90 %.
- Затримка мовного сигналу у тракті "передача-прийом" – не більше 0,32 с.
- Пригнічення скрембльованого сигналу на передавальному боці (місцеве ехо) – не менше 40 дБ.
- Час встановлення закритого зв'язку – не більше 10 с.
- Обмін сеансовими криптографічними ключами реалізований за алгоритмом Діффі–Хеллмана завдовжки 128 біт.
- Ключ формується від фізичного датчика випадкових чисел і є унікальним для кожного сеансу зв'язку.
- Передбачена можливість аутентифікації за допомогою пароля, який може вводитися користувачем з клавіатури телефонного апарата.
- Забезпечується гальванічне розділення від абонентської лінії та від підключеного телефонного апарата.
- Електроживлення від мережі змінного струму – 220 В.
- Споживана потужність – не більше 1 Вт.
- Габарити – 200×280×40 мм.
- Маса – не більше 1,5 кг.

*Додаток 9*

## Апаратно-програмний комплекс криптографічного захисту телефонних повідомлень "Талисман-К"

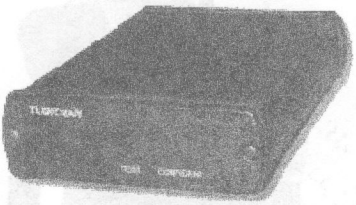


*Рис. Д.11. Зовнішній вигляд пристрою криптографічного захисту інформації "ТАЛИСМАН-К" (Росія)*

Апаратно-програмний комплекс "ТАЛИСМАН-К" (рис. Д.11) призначений для організації криптографічного захисту інформації, яка передається відкритими комутованими або виділеними каналами зв'язку із двопроводовим абонентським закінченням.

Залежно від конфігурації АПК "Талисман-К" може реалізовувати захист:

- телефонних переговорів (режим "мова");
- факсимільних повідомлень (режим "факс");
- даних (режим "передача даних").

Режим "мова"

| | |
|---|---|
| Алгоритм стиснення | модифікований CELP (4800 біт/с) |
| Розбірливість складів | не менше 96 % |
| Тип з'єднання | повний дуплекс |
| Затримка сигналу | не більше 100 мс |
| Рівень захисту телефонного повідомлення | гарантований (ГОСТ 28147-89) |

Режим "факс"

| | |
|---|---|
| Підтримувані протоколи | V.21, T.30, V.27 ter, v.29 |
| Швидкість передачі | 9600, 7200, 4800, 2400 біт/с |
| Сумісність | факс 3 і 4 групи (G3, G4 Fax) |
| Рівень захисту факсимільного повідомлення | гарантований (ГОСТ 28147-89) |

Режим "передача даних"

| | |
|---|---|
| Протокол передачі | Z-modem |
| Лінійна швидкість | 4800 біт/с |
| Швидкість порта | 19200 біт/с |
| Рівень захисту даних | гарантований (ГОСТ 28147-89) |

*Додаток 10*

**Захищений телефонний апарат Voice Coder-2400**

Захищений телефонний апарат Voice Coder-2400 фірми "Сигнал-КОМ" (Росія), забезпечує криптографічний захист телефонних повідомлень.

Основні технічні характеристики телефонного апарата Voice Coder-2400:

- швидкість передачі – 2400 біт/с (повний дуплекс);
- алгоритм шифрування – ГОСТ 28147-89;
- алгоритм компресії – LPC-10;
- розбірливість складів мови на швидкості 2400 біт/с – не нижче 87 %;
- доступ до захищеного режиму зв'язку забезпечується тільки під час зчитування пароля з енергонезалежної пам'яті Touch Memory;
- апарат може працювати як за безпосереднього виходу в телефонну мережу, так і у складі офісних АТС.

# ПЕРЕЛІК СКОРОЧЕНЬ

**АТЛ** – абонентська телефонна лінія.
**АМТС** – автоматична міжміська телефонна станція.
**АТС** – автоматична телефонна станція.
**АВН** – автоматичний визначник номера.
**АЦП** – аналого-цифровий перетворювач.
**ВАК** – вузли автоматичної комутації.
**ВОЛЗ** – волоконно-оптичні лінії зв'язку.
**ДС** – диференціальна система.
**ДСУЗ** – Державна служба урядового зв'язку.
**ІКМ** – імпульсно-кодова модуляція.
**ЗЛ** – з'єднувальна лінія.
**ЗТР** – засіб технічної розвідки.
**КТЧ** – канал тональної частоти.
**МККТТ** – Міжнародний консультаційний комітет із телеграфії та телефонії.
**НСКЗ** – Національна система канфіденційного зв'язку.
**ОЦК** – основний цифровий канал.
**ПМЗ** – первинна мережа зв'язку.
**СКС** – спільний канал сигналізації.
**СП** – система передачі.
**ТА** – телефонний апарат.
**ТфМЗК** – телефонна мережа загального користування.
**ЦАП** – цифроаналоговий перетворювач.
**ЦСК** – цифрова система комутації.
**ШПФ** – швидке перетворення Фур'є.
**ATM** – Asynchronous Transfer Mode.
**DTMF** – Dual Tone Multi-Frequency.
**GSM** – Global System for Mobile communications.
**FDM** – Frequency Division Multiplexing.
**FEXT** – Far-End Crosstalk.
**FR** – Frame Relay.
**ISDN** – Integrated Services Digital Network.
**NEXT** – Near-End Crosstalk.
**LAN** – Local Area Network.
**LPC** – Linear Predictive Coding.
**PDH** – Plesiochronous Digital Hierarchy.
**PSTN** – Public Switched Telephone Network.
**TDM** – Time-Division Multiplexer.
**SDH** – Synchronous Digital Hierarchy.
**QoS** – Quality of Service.
**WAN** – Wide Area Network.
**WDM** – Wavelength Division Multiplexing.

# ІМЕННИЙ ПОКАЖЧИК

Белл Александр Грехам 5
Голубицький Павло Михайлович 9
Грей Еліша 6
Дадлі Гомер 39
Михальський Михайло 6
Строугер Алмон Браун 9
Фур'є Жан Батіст Жозеф 164
Холмс Едвін 8
Шеннон Клод Елвуд 30

# ПРЕДМЕТНИЙ ПОКАЖЧИК

абонентський шлейф 14
абонентська телефонна лінія 14
автоматична телефонна станція 19, 46
блокатор нелегальних підключень 180
блокування доступу 95
високочастотне нав'язування 116
вокодер 38
- з лінійним передбачуванням 41
- канальний 39
- формантний 40
Державна система урядового зв'язку 98
динамічний діапазон 30
диференціальна система 24
еквалайзер 23
експандер 36
енергетичний спектр 30
ехо 23
ехозагороджувач 24
ехокомпенсатор 24
імпульсна характеристика каналу 22
імпульсний рефлектомір 139
імпульсно-кодова модуляція 31
- диференціальна 36
- адаптивна диференціальна 38
інвертор спектра 161
індикатор стану АТЛ 179
завада 21
загороджувальний фільтр 148
загрози 94
засіб технічної розвідки 108
згасання сигналу 22
квантизатор 32
- рівномірний 33
- нерівномірний 35
кількість інформації 30
коефіцієнт активності 29
компандування 35
компандер 36
комутатор 46
- ручний 46
- часовий 47
- часово-просторовий 48
комутаційне поле 46
контроль АТЛ 127
- у робочому стані 127
- знеструмлених 133
лінія зв'язку 15
лінійний абонентський модуль 50
маскувальна перешкода 152
- високочастотна 153

- низькочастотна 152
мережа зв'язку 56
- вторинна 56
- зонова 57
- магістральна 57
- первинна 54
мікрофон 11
- виносний 119
мікрофонний ефект 114
набір номера абонента 12
- імпульсний 12
- частотний 13
Національна система конфіденційного зв'язку 100
нелінійний розв'язувальний пристрій 148
одностороннє маскування 157
основний тон 27
пік-фактор 30
потужність 29
- максимальна 29
- мінімальна 29
- середня 29
рефлектограма 140
самозбудження 23
світловод 18
сигналізація 12
- абонентська 12
- міжстанційна 79
- - децентралізована 79
- - централізована 80
система комутації 46
- нумерації 71
- сигналізації 79
скремблювання 156
- часове 164
- часо-частотне 166
- частотне 162
спотворення 22
- випадкові 23
- детерміновані 23
- - лінійні 23
- - нелінійні 23
стільниковий зв'язок 82
телефонна закладка 108
- капсула 11
- мережа 54
- - загального користування 58
- - - зонова 69
- - - міжзонова 69
- - - міська 61
- - - сільська 61
телефонне повідомлення 155
- вухо 121
телефонний апарат 10
- зв'язок 5
- канал 22
- тракт 96
- шлюз 88
ущільнення телефонних ліній 14
характеристика вольт-амперна 136
- компандування 35
- Лісажа 137
- навантажувальна 131
- перехідна 137
форманта 29
цифрова ієрархія 44
- плезіохронна 45
- синхронна 45
цифрова система передачі 42
часове групоутворення 43
шум 33
- квантування 33
- обмеження 34

# ЗМІСТ

**ВСТУП** ..... 3
**Розділ 1. ОСНОВИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ** ..... 5
1.1. Ретроспективний погляд на телефонний зв'язок ..... 5
1.1.1. Принцип телефонної передачі А. Белла ..... 5
1.1.2. Еволюція телефонного зв'язку ..... 6
1.2. Телефонний апарат як термінальний пристрій телефонної мережі ..... 10
1.2.1. Будова і функції телефонного апарата ..... 10
1.2.2. Імпульсний і частотний способи набору номера абонента ..... 12
1.3. Абонентський шлейф, системи передачі та комутації у телефонії ..... 14
1.3.1. Способи ефективного використання абонентського шлейфа ..... 14
1.3.2. Характеристика ліній зв'язку у системах передачі ..... 15
1.3.3. Етапи розвитку телефонних мереж ..... 19
1.4. Чинники, що впливають на якість передачі сигналів у телефонії ..... 21
1.4.1. Завади і шум ..... 21
1.4.2. Спотворення і згасання сигналу ..... 22
1.4.3. Ехо і самозбудження ..... 23
**Питання для самоконтролю** ..... 24
**Розділ 2. ЗАСАДИ І СТРУКТУРНІ ЕЛЕМЕНТИ ЦИФРОВОЇ ТЕЛЕФОНІЇ** ..... 26
2.1. Перетворення сигналу мовлення до цифрового вигляду ..... 26
2.1.1. Параметри сигналів мовлення ..... 26
2.1.2. Імпульсно-кодова модуляція ..... 31
2.1.3. Компандування ..... 35
2.1.4. Диференціальна імпульсно-кодова модуляція ..... 36
2.2. Вокодери як спеціалізовані пристрої компресії сигналу мовлення ..... 38
2.2.1. Канальні вокодери ..... 39
2.2.2. Формантні вокодери ..... 40
2.2.3. Вокодери з лінійним передбачуванням ..... 41
2.3. Цифрові системи передачі ..... 42
2.3.1. Принципи часового групоутворення ..... 43
2.3.2. Ієрархія цифрових систем передачі ..... 44
2.4. Структура і функції цифрових систем комутації ..... 46
2.4.1. Часово-просторові комутаційні поля цифрових систем комутації ..... 46
2.4.2. Лінійні абонентські модулі цифрових систем комутації ..... 50
2.5. Переваги і недоліки цифрової телефонії ..... 51
**Питання для самоконтролю** ..... 52
**Розділ 3. СТРУКТУРА ТА ФУНКЦІОНУВАННЯ ТЕЛЕФОННИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ** ..... 54
3.1. Телефонна мережа та її місце у сучасній телекомунікації ..... 54
3.1.1. Первинні та вторинні мережі зв'язку ..... 54
3.1.2. Первинна мережа ВАТ "Укртелеком": стан і перспективи розвитку ..... 56
3.1.3. Телефонна мережа загального користування України ..... 58
3.2. Місцеві телефонні мережі загального користування ..... 60
3.2.1. Структура міських та сільських телефонних мереж ..... 61

3.2.2. Перехід від аналогових телефонних мереж до цифрових ..... 64
3.2.3. Особливості цифрових мереж з інтеграцією послуг ..... 68
3.3. Міжміський та міжнародний телефонний зв'язок ..... 69
3.3.1. Зонові та міжзонові телефонні мережі ..... 69
3.3.2. Системи нумерації у телефонних мережах ..... 71
3.4. Телефонна сигналізація ..... 76
3.4.1. Види сигналів телефонної сигналізації ..... 76
3.4.2. Алгоритм встановлення з'єднань у телефонній мережі ..... 77
3.4.3. Системи міжстанційної сигналізації ..... 79
**Питання для самоконтролю** ..... 81
**Розділ 4. ТЕЛЕФОННИЙ ЗВ'ЯЗОК ПОЗА ТЕЛЕФОННОЮ МЕРЕЖЕЮ ЗАГАЛЬНОГО КОРИСТУВАННЯ** ..... 82
4.1. Стільниковий зв'язок ..... 82
4.1.1. Архітектура і технологія системи GSM ..... 82
4.1.2. Засоби безпеки системи GSM ..... 86
4.2. Телефонія у мережах з пакетною комутацією ..... 87
4.2.1. Телефонний зв'язок у локальній мережі ..... 88
4.2.2. Телефонний зв'язок через Інтернет ..... 90
4.2.3. Проблеми забезпечення якості телефонних розмов у IP-телефонії ..... 91
4.2.4. Особливості кодеків голосу для IP-телефонії ..... 92
**Питання для самоконтролю** ..... 93
**Розділ 5. КОНЦЕПТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ ІЗ ТЕЛЕФОННИМ ЗВ'ЯЗКОМ** ..... 94
5.1. Аналіз загроз для інформації у телефонних мережах загального користування ..... 94
5.2. Шляхи забезпечення захищеності обміну інформації у каналах зв'язку ..... 98
5.2.1. Використання Державної системи урядового зв'язку ..... 98
5.2.2. Використання Національної системи конфіденційного зв'язку ..... 100
5.2.3. Використання мереж зв'язку загального користування ..... 102
5.3. Організація захищеної корпоративної мережі телефонного зв'язку ..... 104
5.3.1. Основні вимоги до систем закриття мовної інформації у телефонних каналах ..... 104
5.3.2. Вимоги до систем захисту мовних повідомлень для стаціонарних абонентів ..... 105
5.3.3. Вимоги до систем закриття мовних повідомлень для рухомих абонентів ..... 106
**Питання для самоконтролю** ..... 107
**Розділ 6. МЕТОДИ І ЗАСОБИ НЕСАНКЦІОНОВАНОГО ОДЕРЖАННЯ ІНФОРМАЦІЇ ІЗ ТЕЛЕФОННИХ ЛІНІЙ** ..... 108
6.1. Принципи побудови та класифікація засобів технічної розвідки, які використовуються у телефонних лініях ..... 108
6.2. Найімовірніші місця встановлення телефонних закладок ..... 112
6.3. Застосування закладок для перехоплення телефонних повідомлень ..... 113
6.4. Способи використання засобів телефонного зв'язку для прослуховування приміщень ..... 114
6.4.1. Перехоплення сигналів "мікрофонного ефекту" ..... 114
6.4.2. Використання високочастотного нав'язування ..... 116
6.4.3. Прослуховування приміщень за допомогою виносних мікрофонів ..... 119
6.5. Перехоплення побічних електромагнітних сигналів випромінювання і наведень ..... 122
**Питання для самоконтролю** ..... 123

**Розділ 7. ЗАСОБИ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ МІСЦЬ КОНТАКТНИХ ПІДКЛЮЧЕНЬ ЗАСОБІВ ТЕХНІЧНОЇ РОЗВІДКИ У ТЕЛЕФОННИХ ЛІНІЯХ** ..... 125
7.1. Класифікація методів виявлення несанкціонованих підключень до абонентських телефонних ліній ..... 125
7.2. Контроль абонентських телефонних ліній у робочому стані ..... 127
7.2.1. Контроль напруги живлення АТЛ ..... 128
7.2.2. Контроль струму короткого замикання АТЛ ..... 130
7.2.3. Контроль навантажувальної характеристики ..... 131
7.2.4. Виявлення сторонніх сигналів у АТЛ та радіоефірі ..... 132
7.3. Контроль параметрів знеструмлених абонентських телефонних ліній ..... 133
7.3.1. Вимірювання опору шлейфа, омічної асиметрії та параметрів імпедансу абонентських телефонних ліній ..... 134
7.3.2. Контроль вольт-амперної характеристики ..... 136
7.3.3. Контроль Лісажа-характеристики ..... 137
7.3.4. Контроль перехідної характеристики ..... 137
7.3.5. Визначення віддаленості місця несанкціонованого підключення до АТЛ за неоднорідністю ..... 139
7.4. Комплексні системи моніторингу телефонних ліній ..... 141
**Питання для самоконтролю** ..... 142
**Розділ 8. ЗАХИСТ АБОНЕНТСЬКИХ ТЕЛЕФОННИХ ЛІНІЙ ВІД ПРОСЛУХОВУВАННЯ** ..... 144
8.1. Характеристика завдань забезпечення конфіденційності на ділянці АТЛ ..... 144
8.2. Методи обмеження фізичного доступу до АТЛ та знищення гальванічно підключених телефонних закладок ..... 146
8.3. Запобігання прослуховуванню приміщень через АТЛ ..... 147
8.3.1. Пасивні засоби захисту: нелінійні розв'язувальні пристрої, загороджувальні фільтри та електронні комутатори ..... 147
8.3.2. Активні засоби захисту. Генератори маскувальних сигналів ..... 151
8.4. Методи захисту від підслуховування телефонних повідомлень на ділянці абонентських телефонних ліній ..... 152
8.4.1. Накладання маскувальних перешкод ..... 152
8.4.2. Придушення електронних засобів технічної розвідки ..... 153
**Питання для самоконтролю** ..... 154
**Розділ 9. ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПІД ЧАС ПЕРЕДАЧІ МОВНИХ ПОВІДОМЛЕНЬ КАНАЛАМИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ** ..... 155
9.1. Класифікація і характеристика методів забезпечення конфіденційності телефонних повідомлень ..... 155
9.2. Захист від перехоплення телефонних повідомлень на енергетичному рівні. Метод одностороннього маскування ..... 157
9.3. Приховування семантичного змісту телефонних повідомлень часо-частотними перетвореннями ..... 161
9.3.1. Інверсія та перетворення спектра телефонних сигналів ..... 161
9.3.2. Часові перестановки фрагментів телефонних сигналів ..... 164
9.3.3. Часо-частотне скремблювання телефонних повідомлень ..... 166
9.4. Оцифровування і стиснення мови з подальшим шифруванням ..... 169

9.4.1. Шифрування стиснених телефонних повідомлень ..... 170
9.4.2. Кодування параметрів мовного сигналу із подальшим шифруванням цифрового потоку ..... 171
9.4.3. Алгоритм встановлення шифрованого телефонного зв'язку у телефонній мережі загального користування ..... 173
**Питання для самоконтролю** ..... 176
**Розділ 10. ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ВИКОРИСТАННЮ РЕСУРСІВ ТЕЛЕФОННОГО ЗВ'ЯЗКУ** ..... 177
10.1. Технічні аспекти, що застосовуються для боротьби із телефонним шахрайством ..... 178
10.2. Сигналізація про нелегальні підключення ..... 179
10.3. Блокування нелегальних підключень ..... 180
10.3.1. Блокатор типу "заглушка" ..... 182
10.3.2. Блокатор паралельних телефонних апаратів ..... 183
10.4. Запобігання доступу до міжміської автоматичної телефонної станції ..... 184
10.4.1. Блокування цифри "0" ..... 184
10.4.2. Обмеження формату набору ..... 185
10.5. Рекомендовані ВАТ "Укртелеком" організаційно-технічні засоби захисту від стороннього підключення ..... 186
**Питання для самоконтролю** ..... 188
**ЛІТЕРАТУРА** ..... 190
**ДОДАТКИ** ..... 192
Додаток 1. Приклади конструктивного виконання телефонних закладок ..... 192
Додаток 2. Призначення та основні технічні характеристики універсального аналізатора проводових комунікацій "ULAN-2" ..... 193
Додаток 3. Основні характеристики засобів фізичного знищення телефонних закладних пристроїв ..... 194
Додаток 4. Призначення та характеристика приладу технічного захисту інформації абонентів телефонної мережі "СКЕЛЯ-1" ..... 195
Додаток 5. Система комплексного захисту телефонної лінії SEC-2004 ANTI FLY ..... 198
Додаток 6. Пристрій одностороннього маскування телефонних переговорів "Щит" ..... 199
Додаток 7. Телефонний скремблер із акустоелектричним перетворенням ACS-2 ..... 200
Додаток 8. Телефонний скремблер "Орех-ІІ" ..... 201
Додаток 9. Апаратно-програмний комплекс криптографічного захисту телефонних повідомлень "Талисман-К" ..... 202
Додаток 10. Захищений телефонний апарат Voice Coder-2400 ..... 203
**ПЕРЕЛІК СКОРОЧЕНЬ** ..... 204
**ІМЕННИЙ ПОКАЖЧИК** ..... 205
**ПРЕДМЕТНИЙ ПОКАЖЧИК** ..... 205

**наші книжки**
**В ІНТЕРНЕТІ**
**http:// vlp.com.ua**

- **повний каталог** навчальної та наукової літератури, наукових журналів;
- можливість детально ознайомитися із змістом, анотацією та передмовою книжкових видань;
- **докладна інформація** про можливість та умови придбання книг через нашу Інтернет-сторінку;
- продаж книг за системою **"друк на вимогу"**.

## МЕРЕЖА КНИГАРЕНЬ
### у Львівській політехніці:

**Головний корпус** – вул. С. Бандери, 12.....тел.: 258-24-92

**1 корпус** – вул. Карпінського, 2/4

**2 корпус** – вул. Карпінського, 6

**4 корпус** – вул. Митрополита Андрея, 5.....тел.: 258-23-56

**5 корпус** - вул. С. Бандери, 28а

**8 корпус** - пл. Св. Юра, 2

**11 корпус** - вул. Професорська, 2

**Студентська бібліотека** - вул. Митрополита Андрея, 3.....тел: 258-03-93

*Видавництво Львівської політехніки*
вул. Ф. Колесси, 2, корп. 23 А, м. Львів, 79000
тел. +380 32 2582146, факс +380 32 2582136, http://vlp.com.ua, vmr@vlp.com.ua

НАВЧАЛЬНЕ ВИДАННЯ

**Дудикевич Валерій Богданович**
**Хома Володимир Васильович**
**Пархуць Любомир Теодорович**

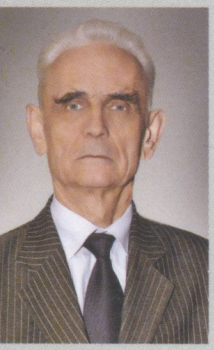
# ЗАХИСТ ЗАСОБІВ І КАНАЛІВ ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Редактор *Ольга Грабовська*
Коректор *Наталія Колтун*
Технічний редактор *Лілія Саламін*
Комп'ютерне верстання *Наталії Максимюк*
Художник-дизайнер *Уляна Келеман*

Здано у видавництво 20.04.2012. Підписано до друку 19.06.2012.
Формат $70\times90^{1}/_{16}$. Папір офсетний. Друк офсетний.
Умовн. друк. арк. 15,5. Обл.-вид. арк. 12,7.
Наклад 150 прим. Зам. 120448.

Видавець і виготівник: Видавництво Львівської політехніки
*Свідоцтво суб'єкта видавничої справи ДК № 751 від 27.12.2001 р.*
*вул. Ф. Колесси, 2, Львів, 79000*

тел. +380 32 2582146, факс +380 32 2582136
vlp.com.ua, ел. пошта: vmr@vlp.com.ua



**ДУДИКЕВИЧ Валерій Богданович** – доктор технічних наук, професор, завідувач кафедри захисту інформації Національного університету "Львівська політехніка", керівник Західного регіонального навчально-наукового центру захисту інформації, Заслужений винахідник України. У 1963 році закінчив факультет автоматики та напівпровідникової електроніки. Голова спеціалізованої Вченої ради Д 35.052.18.

***Наукові інтереси:*** вимірювальні перетворювачі частотних сигналів, число-імпульсні перетворювачі кодів для засобів вимірювання та керування, медичне приладобудування, вимірювальні випробувальні комплекси, методи і засоби технічного захисту інформації. Автор понад 200 авторських свідоцтв і патентів.

**ХОМА Володимир Васильович** – доктор технічних наук, професор кафедри захисту інформації Національного університету "Львівська політехніка". У 1981 році закінчив Львівський політехнічний інститут за спеціальністю автоматика і телемеханіка. До 1993 року працював науковим співробітником НДКІ "ЕЛВІТ" ЛПІ, займався розробленням та впровадженням засобів вимірювання імпедансу, має відзнаку "Винахідник СРСР".

***Наукові інтереси:*** прикладне вимірювання імітансу; цифрове оброблення вимірювальних сигналів; ідентифікація технічних каналів витоку інформації. Автор понад 150 наукових робіт, з них: 17 патентів; 25 публікацій, опублікованих за кордоном.

**ПАРХУЦЬ Любомир Теодорович** – доктор технічних наук, професор кафедри захисту інформації Національного університету "Львівська політехніка". У 1981 році закінчив Львівський університет імені Івана Франка за спеціальністю "Радіофізика і електроніка". У 2011 році захистив докторську дисертацію за спеціальністю 05.13.21 – системи захисту інформації. Заступник завідувача кафедри захисту інформації, вчений секретар спеціалізованої Вченої ради Д 35.052.18.

***Наукові інтереси:*** методи та засоби захисту інформації, проектування комплексних систем захисту інформації, захищені комп'ютерні мережі спеціального призначення.

Автор понад 100 наукових публікацій, 10 авторських свідоцтв на винаходи, підручника та навчального посібника.

ISBN 978-617-607-283-6