**Міністерство транспорту та зв'язку України**
**Державна адміністрація зв'язку**
_____
**Одеська національна академія зв'язку ім. О.С. Попова**
_____
Кафедра інформаційної безпеки та передавання даних

**Д. В. Голев, О.Ю.Русляченко, Ю.В.Бєлова, Д.С.Гончарук**

# ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ
## Лабораторний практикум
## Частина 2 – Комплекси технічного захисту інформації

**Навчальний посібник**

Для студентів вищих навчальних закладів, які навчаються за напрямом «Системи технічного захисту інформації»

За редакцією члена-кореспондента МАЗ, к. т. н., доцента В.Г. Кононовича

Одеса 2010

УДК 004.056; 681.336; 621.39

**Д. В. Голев, О.Ю.Русляченко, Ю.В.Бєлова, Д.С.Гончарук** Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 2 – Комплекси техничного захисту інформації Навч. посібник / За ред. чл.-кор. МАЗ **В.Г. Кононовича**.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 184.

Рецензенти:

……..

ISBN _____

Представлені тематичні цикли лабораторного практикуму в галузі знань «Інформаційна безпека». Цикли лабораторного практикуму складені з навчально методичних рекомендацій та посібників для виконання лабораторних робіт з напряму підготовки «Системи технічного захисту інформації» і об'єднані задачею створення комплексних систем технічного захисту інформації на об'єктах інформаційної діяльності органів місцевої державної влади.

Навчальний посібник буде корисний студентам бакалаврату, магістрату та слухачам курсів підвищення кваліфікації у галузі знань інформаційної безпеки.

Для студентів старших курсів вищих навчальних закладів.

СХВАЛЕНО
на засіданні кафедри інформаційної
безпеки та передавання даних
і рекомендовано до друку
Протокол № 1 від 28.08.2010 р.



**ISBN**

# ВСТУП

Інформаційна сфера відіграє дедалі зростаючу роль у забезпеченні безпеки держави і суспільства. Саме через цю сферу реалізується значна частина загроз національній безпеці держави.

Основними джерелами загроз інформаційної безпеки є діяльність іноземних спеціальних служб, кримінальних угруповань та організацій, а також протизаконна діяльність окремих осіб, спрямована на збір, розкрадання та розповсюдження (продаж) цінної інформації, закритої для доступу сторонніх осіб.

Тому проблема надійного захисту інформації в різних організаціях та установах в сучасних умовах є досить актуальною.

Не секрет, що основний обсяг інформації, яка охороняється, сьогодні може бути негласно здобутий за допомогою сучасних технічних засобів радіоелектронної розвідки. Цьому сприяють високі рівні розвитку технологій в різних областях техніки, що дозволяють створювати високоефективні автономні автоматичні засоби здобування інформації в портативному, мініатюрному і надмініатюрному виконанні.

Широкий клас створюваних портативних пристроїв дає можливість використання різноманітних методів їх застосування з урахуванням різних обмежень по територіальній доступності.

Одними з найбільш поширених технічних засобів, що використовуються для несанкціонованого здобування інформації, можуть бути різноманітні електронні пристрої перехоплення інформації або так звані закладні пристрої. Основне місце їх установки – різного роду внутрішні приміщення. Виявлення і нейтралізація таких пристроїв є найважливішою і досить складною задачею в системі заходів із захисту інформації в різних організаціях і установах.

У даному посібнику пропонуються рекомендації щодо виявлення закладних пристроїв із застосуванням організаційно-технічних заходів, які певною мірою дозволяють вирішити цю проблему. У посібнику представлені різні технічні засоби пошуку електронних пристроїв перехоплення інформації.

Бакалаври за напрямом підготовки «Системи технічного захисту інформації» мають набути такі загально професійні компетенції:

- здатність оперативно управляти діяльністю підрозділу з захисту інформації;
- здатність і готовність до використання методів аналізу й діагностики стану програмно-апаратних засобів і систем технічного захисту інформації та до забезпечення процесу захисту інформації з використанням необхідних видів, методів, засобів і технологій захисту;
- здатність і готовність до використання вміння:
- по обліку, обробці, зберіганню, передачі, організації використання різних носіїв конфіденційної інформації;
- по виявленню й блокуванню каналів і методів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію;

- по установці та адаптації систем і засобів забезпечення захисту інформації;

- по здійсненню контролю якості функціонування устаткування захищених інформаційних систем, аналізу якісних і кількісних показників функціонування устаткування, діагностиці й усунення відмов, настроюванню й ремонту устаткування.

Проведення лабораторного практикуму та самостійне вивчення розділів змістовних модулів забезпечується лабораторними класами, оснащеними сучасною комп'ютерною технікою, вимірювальними та індикаторними приладами й комплексами, зразками технічних та програмно – технічних засобів захисту інформації, автоматизованими системами навчання.

Кожному студенту доступні загальні та режимні бібліотечні фонди, бази даних, навчальні пакети на носіях, за змістом відповідним дисциплінам основної освітньої програми:

- «Методи та засоби технічного захисту інформації»;
- «Безпека інформаційно – комунікаційних систем»;
- «Технічні засоби охорони об'єктів»;
- «Комплексні системи захисту інформації»
- «Управління інформаційною безпекою»;
- «Системи технічного захисту інформації»
- «Аудит інформаційної безпеки».

Навчальний посібник підготували: Д.В.Голев (вступ, розд. 1), О.Ю.Русляченко (розд. 2), Ю.В.Бєлова (розд. 2), Д.С. Гончарук (розд. 1,).

# ГЛАВА 1 ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

У цьому циклі забезпечується здобуття знань і умінь виявлення та блокування витоку інформації технічними каналами. Професійні компетенції цього циклу передбачають уміння:

- кваліфіковано аналізувати інформацію, надану технічними системами, з метою виявлення типових ознак можливого несанкціонованого доступу;
- уміти зафіксувати інформацію з додержання чи порушення заходів об'єктового контролю у відповідних реєстраційних документах;

розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу;

- проводити атестацію режимних територій в умовах додержання режиму секретності із за фіксуванням результатів у відповідних документах;
- розробляти узагальнений перелік потрібних технічних засобів;
- використовувати технічні засоби захисту інформації в умовах забезпечення режиму секретності на підприємствах, в організаціях та установах різних форм власності, уміти провести дії щодо організації технічного захисту інформації, зокрема приймати рішення про додержання чи наявність факту порушення конфіденційності інформації обмеженого доступу;
- розробляти номенклатурний перелік технічних засобів захисту інформації від витоку технічними каналами та реалізовувати технічні заходи закриття можливих каналів витоку інформації (за переліком каналів витоку);
- оцінювати ефективність систем захисту.

## Лабораторна робота № 1.
## Виявлення витоку інформації з обмеженим доступом технічними каналами за допомогою багатофункціонального пошукового приладу ST– 031 Піранья

### 1 Мета роботи

вивчення багатофункціонального пошукового приладу ST– 031 Піранья;

вивчення методів проведення заходів щодо виявлення й локалізування спеціальних технічних засобів таємного добування інформації, для виявлення природних та штучно створених каналів витоку інформації;

вивчення методів контролю якості захисту інформації.

### 2 Домашнє завдання

а) вивчити канали несанкціонованого витоку інформації;

б) вивчити типи закладних пристроїв;

в) вивчити методи пошуку закладних пристроїв несанкціонованого знімання інформації.

### 3 Зміст роботи

а) вивчення пошукового приладу ST–031 Піранья та особливостей роботи в різних режимах пошуку;

б) практичне використання методів виявлення можливих каналів несанкціонованого витоку інформації за допомогою пошукового приладу ST–031 Піранья;

в) складання протоколу вимірювань.

### 4 Склад протоколу вимірювань

а) структурна схема закладного пристрою;

б) структурна схема пошукового процесу;

в) опис проведення пошуку закладних пристроїв;

г) оцінка результатів пошуку (висновки).

### 5 Ключеві положення

Сьогодні широкого розповсюдження набуло застосовування підслуховуючої апаратури та закладних пристроїв (ЗП). Поєднання відносно невеликої ціни та високої якості таких пристроїв, а також відсутність створених правових норм, перетворюють цей канал витоку інформації на один з найнебезпечніших та найдоступніших.

Для виявлення в будівельних конструкціях приміщень та предметах інтер’єру таємно встановлених радіопередавальних пристроїв та інших

технічних засобів для знімання інформації, котрі мають у своєму складі напівпровідникові компоненти, й перебувають як у ввімкненому, так і у вимкненому стані, використовуються переважно два способи:

– пасивне виявлення (до даного способу належить контроль радіоефіру за допомогою прийомних засобів;

– активне виявлення за допомогою локації. Локація, в свою чергу, може здійснюватися радіолокаційним зондуванням конструкцій на предмет виявлення закладних пристроїв.

Канали витоку інформації в радіочастотному діапазоні можуть бути створені штучно (зумисно), за рахунок використання зацікавленими органами й організаціями спеціальних технічних засобів (радіомікрофони, телефонні радіоретранслятори, несанкціоновано ввімкнені радіостанції, радіомаяки і тощо). Вони можуть виникнути і природно, за рахунок побічних електромагнітних випромінювань (ПЕМВ) технічних засобів опрацьовування інформації (ПЕОМ, телекси, факси і тощо).

У будь-якому випадку виникає необхідність класифікування сигналів у радіочастотному діапазоні за сукупністю критеріїв.

З погляду на розв’язок завдань контролю захисту інформації й використання при цьому приладу ST – 031 Піранья, усі радіосигнали, що вони потрапляють у його робочого діапазону, можна вельми об'єктивно поділити на небезпечні й безпечні.

Корисним, для практики є також класифікування радіосигналів за найбільш імовірним місцем їхнього виникнення: внутрішнім та зовнішнім, щодо перевірюваного об'єкта стосовно перевірюваного (приміщення). Небезпечні радіосигнали може бути створено як внутрішніми, так і зовнішніми джерелами. Більш того, на практиці зустрічається досить велика кількість їхніх найрізноманітніших сполучень.

Зазвичай, до цілковито внутрішніх небезпечних радіосигналів відносять:

– сигнали радіозакладок (радіомікрофони, телефонні радіотранслятори і тощо);

– сигнали радіомаяків;

– сигнали несанкціоновано ввімкнених у приміщенні радіостанцій та радіотелефонів;

– побічні електромагнітні випромінювання ПЕОМ та інші технічні засоби опрацьовування інформації.

До категорії небезпечних, у сполученні внутрішні — зовнішні, прийнято відносити радіосигнали, джерелами яких можуть бути:

– радіомікрофони з виносним акустичним мікрофоном;

– телефонні радіоретранслятори, установлені на лінії зв'язку за межами приміщення (але поблизу нього);

– радіостетоскопи, встановлені із зовнішнього боку поверхонь, котрі огороджують приміщення;

– винесені передавачі прихованих відеокамер;

– пристрої зовнішнього високочастотного опромінювання.

Чисто зовнішні джерела радіовипромінювання, як правило, прямої небезпеки, з погляду витоку інформації, не становлять. До їхнього числа можна віднести широкомовленєві радіостанції, станції телевізійного мовлення, засоби радіозв'язку і тощо.

Як джерела внутрішніх безпечних радіосигналів можуть розглядатися, насамперед, електроприлади, оргтехніка, побутові засоби, а також їхні блоки живлення.

## 1.1 Особливості потенційно небезпечних радіосигналів та їхніх джерел

– Як зазначалося, джерелами потенційно небезпечних радіосигналів є радіомікрофони, телефонні радіоретранслятори, радіостетоскопи, присховані відеокамери з радіоканалом передавання інформації, радіозакладки в ПЕОМ, засоби просторового високочастотного опромінювання, несанкціоновано ввімкнення засоби зв'язку (радіостанції, радіотелефони, телефони з радіоподовжувачами).

– Через величезну розмаїтість варіантів конструктивного та схемного виконання радіомікрофонів саме для них є притаманний широкий спектр особливостей радіовипромінювань.

### 1.1.1 Радіомікрофони

Широкого розповсюдження набули радіомікрофони з параметричною стабілізацією частоти передавача. Основна особливість – великі межі змінювання несучої частоти (до кількох мегагерц) тому для локалізування радіомікрофонів такого типу найбільш доцільне є використання методу акустозав'язки.

Досить широко застосовуються радіомікрофони з кварцовою стабілізацією частоти й вузькосмуговою частотною модуляцією. Основні їхні особливості полягають у невеликих межах змінювання несучої частоти (до десятка кілогерців) і слабкому звуковому сигналі на виході амплітудного детектора приймача приладу. Останнє визначає значно менші розміри зони виникнення акустозав'язки. Тому для пошуку й локалізування такого типу джерел найбільш доцільне є використання амплітудного методу.

Як високопрофесійні засоби таємного добування інформації застосовуються радіомікрофони з винесеним передавачем. Їхня головна особливість – рознесення місць установлювання мікрофона і власне радіопередавача (аж до винесення до іншого приміщення). У цьому разі слід поєднати метод акустозав'язки та амплітудного методу. Причому для локалізування мікрофона слід використовувати метод акустозав'язки, а радіопередавача – (у перевірюваному приміщенні чи за його межами) – амплітудний метод.

Високопрофесійними засобами є й радіомікрофони із закритим чи замаскованим радіоканалом. Їхня головна особливість полягає в тім, що

прийнятий і демодульований сигнал не несе в собі інформації про акустичний фон приміщення. Це визначається використанням для закриття (маскування) радіоканалу методів інверсії спектра, цифрових методів передавання та складних видів модуляції. Отже, в основу їхнього виявлення й локалізування має бути покладено амплітудний метод з доповненням його аналізом осцилограм та спектрограм.

У радіомікрофонів, призначених для установлювання в автомобілях та інших транспортних засобах, виокремлюють дві головних особливості – підвищену потужність радіопередавача й більш чистий, без ознак зовнішнього фону, демодульований сигнал (внаслідок звукоізолювальних властивостей корпуса автомобіля). Інші особливості можуть виявлятися в залежності від використовуваних способів стабілізації несучої частоти й застосовуваних видів модуляції. Тому методи пошуку та локалізування таких радіомікрофонів є цілковито аналогічні до розглянутих вище.

### 1.1.2 Телефонні радіо ретранслятори

Незважаючи на різноманіття варіантів виконання телефонних радіоретрансляторів, чітко виокремлюються дві їхні групи за способом підмикання до елементів телефонної лінії – з гальванічним контактом та без нього. При цьому гальванічне підмикання може здійснюватися як послідовно (у розрив одного з проводів телефонної лінії), так і паралельно (водночас до двох проводів телефонної лінії).

Телефонні радіоретранслятори послідовного вмикання відрізняються головною особливістю – з’явленням в ефірі модульованого сигналу лише за піднятої слухавки телефонного апарата. При цьому явно прослуховуються сигнали АТС («виклик», «зайнято»), клацання при набиранні номера, розмова абонентів після встановлення з’єднання. Такий радіоретранслятор принципово може бути встановлено практично на будь-якій ділянці телефонної лінії (корпус апарата, його трубка, розподільні коробки й щити, власне провід абонентської лінії). Локалізування телефонних ретрансляторів даного типу найбільш доцільно здійснювати амплітудним методом. Це зумовлено тим, що телефонні апарати, використовувані даного часу, мають доволі чутливі мікрофони й, вельми часто, режим гучномовного зв'язку. Застосовування методу акустозав’язки може призвести до помилкових висновків щодо наявністі встановленого телефонного радіоретранслятора.

Телефонні радіоретранслятори паралельного ввімкнення можуть мати два різновиди.

Перший різновид передбачає реалізацію лише функції ретранслятора. При цьому в режимі піднятої слухавки на радіочастоті прослуховуються сигнали АТС (виклик, зайнято), клацання при набиранні номера й розмова абонентів. При покладеній слухавки модуляція радіосигналу відсутня, може бути відсутня й сама несуча частота. Такий радіоретранслятор може бути принципово встановлено на будь-якій ділянці телефонної лінії. Для

локалізування закладок такого типу більш оптимальним є амплітудний метод з їхньою активізацією шляхом підняття слухавки телефонного апарата.

В другому різновиді часто сполучують функції телефонного радіоретранслятора та радіомікрофона, він живиться від телефонної лінії й забезпечує контроль акустики приміщення в режимі покладеної слухавки. Такі закладки встановлюються на елементах телефонної лінії в межах контрольованого приміщення. Для їхнього локалізування, за прокладеної слухавки, використовується метод акустозав'язки із застосуванням тестового звукового сигналу. У режимі піднятої слухавки, для локалізування таких закладок, краще застосовувати амплітудний метод.

Слід мати на увазі, що радіоретранслятори гальванічного підмикаанння, як правило, не мають власних антен, а використовують замість них провід телефонної лінії. У цьому разі їхнє локалізування може бути здійснено лише амплітудним методом за рахунок виявлення розподілу максимумів рівня високочастотного електромагнітного поля уздовж телефонної лінії. Максимуми чергуються через половину довжини хвилі, а найближчий, стосовно передавача, віддалено від нього на відстань чверті довжини хвилі.

Довжина хвилі визначається у відповідності зі значенням частоти, «захопленої» частотоміром приладу. Наприклад, за частоти випромінювання 300 МГц довжина хвилі становить 1 м. Отже, максимуми випромінювання для даного випадку чергуватимуться через 0,5 м, а місця найбільш імовірного встановлення такого роду радіоретрансляторів знаходитимуться на відстані 25 см від місць максимуму.

Телефонні радіоретранслятори негальванічного вмикання (індуктивного знімання інформації) може бути встановлено на будь-якій ділянці телефонної лінії, як правило, поза контрольованим приміщенням на абонентській проводці без порушення ізоляції. Вони формують модульований радіосигнал лише за підняття слухавки телефонного апарата при цьому прослуховуються сигнали АТС (виклик, зайнято), клацання при набиранні номера, розмова абонентів після встановлення з'єднання. Їхнє локалізування здійснюється амплітудним методом в міру обстеження телефонної лінії на всьому її доступному протязі.

### 1.1.3 Інші джерела потенційно небезпечних радіовипромінювань

Тут варто розглянути, насамперед, радіостетоскопи, приховані відеокамери з радіоканалом передавання інформації, радіозакладки в ПЕОМ, радіомаяки, засоби просторового високочастотного опромінювання, несанкціоновано ввімкнені засоби зв'язку (радіостанції, радіотелефони, телефони з радіоподовжувачами).

Основна особливість радіостетоскопів полягає в тому, що вони встановлюються лише із зовнішнього боку поверхонь, які огороджують контрольоване приміщення, або на трубах систем опалення, водогону й інших комунікацій, що виходять за його межі.

Приховані відеокамери з радіоканалом передавання інформації відрізнюються тим, що сигнал, випромінюваний у радіодіапазоні, за структурою є схожий із сигналом каналу яскравості передавачів телевізійного мовлення. Цей сигнал, за обговореною вище класифікацією, є внутрішнім (щодо перевірюваного приміщення). Виявлення такого сигналу й локалізування його джерела найбільш доцільно здійснювати амплітудним методом, доповнюючи цей метод прослуховуванням змінювання тону продетектованого сигналу.

Радіозакладки в ПЕОМ призначено для передавання зображення монітора та цифрових сигналів системного блока й інших елементів фізичної архітектури комп'ютера. Основна їхня особливість полягає в тім, що сигнал, котрий передає зображення монітора, за структурою схожий на сигнал передавача прихованої відеокамери, а в інших випадках містить всі ознаки цифрового передавання. За основу для їхнього виявлення й локалізування слугує амплітудний метод, що він доповнюється аналізом зображень сигналів.

Радіомаяки відрізнюються тим, що їхнє радіовипромінювання не має модуляції акустичним фоном приміщення (об'єкта), є неперервним або чітко вираженим періодичним. Можлива є модуляція тоном. Їхнє виявлення може здійснюватися амплітудним методом у сполученні з прослуховуванням сигналу, а локалізовуваня – лише амплітудним методом.

Засоби просторового високочастотного опромінювання є зовнішніми й використовуються для здобуття інформації з приміщень шляхом орієнтації на нього (переважно через віконні прорізи) потужного гостро спрямованого променя електромагнітного випромінювання високої частоти і приймання перевипроміненого, вже промодульованого сигналу, на частотах вищих гармонік. Основні особливості, що вони забезпечують можливість їх (засобів) виявлення й локалізування полягають у тім, що зондувальний сигнал є стабільним за частотою, його модуляція відсутня, рівень нерівномірний (більш високий у районі вікон, істотно більш низький в коридорі та інших приміщеннях). Окрім того, перевипромінений сигнал за частотою відповідає вищим гармонікам зондувального сигналу і має модуляцію акустичним фоном приміщення. Тому виявлення таких засобів здійснюється амплітудним методом у сполученні з прослуховуванням сигналу, а локалізування напрямку опромінення – лише амплітудним методом.

Головною особливістю несанкціоновано ввімкнених на передавання радіостанцій, радіотелефонів та телефонів з радіоподовжувачами є значно менша чутливість вмонтованого мікрофона, ніж у радіомікрофонів. Окрім того, у багатьох з них (надто в радіотелефонах) використовуються складні види модуляції. Це призводить до того, що в прийнятому та продетектованому радіосигналі акустичний фон приміщення або не прослуховується, або акустозав’язка виникає в безпосередній близькості до таких засобів. Для їхнього пошуку й локалізування слід орієнтуватися на амплітудний метод.

## 2 Опис роботи багатофункціонального пошукового приладу ST– 031 Піранья

### 2.1 Призначення та основні можливості

Багатофункціональний пошуковий прилад ST – 031 Піранья призначено для проведення заходів щодо виявлення та локалізування спеціальних технічних засобів таємного здобування інформації, для виявлення природних та штучно створених каналів витоку інформації, а також для контролю якості захисту інформації. Він забезпечує розв'язок контрольно-пошукових завдань лише в так названій ближній зоні, тобто в межах приміщення (об'єкта) чи то в безпосередній близькості до нього.

З використанням приладу ST – 031 Піранья можливе розв'язування таких контрольно-пошукових завдань:

1 Виявлення факту роботи та локалізування місця розташування радіо-випромінювальних спеціальних технічних засобів, які створюють потенційно небезпечні, з огляду витоку інформації, радіовипромінювання. До таких засобів, насамперед, відносять:

– радіомікрофони;

– телефонні радіоретранслятори;

– радіостетоскопи;

– приховані відеокамери з радіоканалом передавання інформації;

– технічні засоби систем просторового високочастотного опромінювання в радіодіапазоні;

– технічні засоби передавання зображення з монітора ПЕОМ радіоканалом;

– радіомаяки систем спостереження за переміщування об'єктів (людей, транспортних засобів, вантажів тощо);

– несанкціонованно ввімкнення радіостанції, радіотелефони й телефони з радіо-подовжувачем;

– технічні засоби опрацювання інформації, робота яких супроводжується виникненням побічних електромагнітних випромінювань (елементи фізичної архітектури ПЕОМ, факси, ксерокси, деякі типи телефонних апаратів тощо).

2 Виявлення й локалізування місця розташування спеціальних технічних засобів, які працюють з випромінюванням в інфрачервоному діапазоні. До таких засобів, у першу чергу, відносять:

закладні пристрої здобування акустичної інформації з приміщень, з її наступним передаванням каналом в інфрачервоному діапазоні;

технічні засоби систем просторового опромінювання в інфрачервоному діапазоні.

3 Виявлення та локалізування місця розташування спеціальних технічних засобів, що їх використовують для здобування та передавання інформації провідні лінії різноманітного призначення, а також технічних засобів опрацьовування інформації, котрі здійснюють наведення інформативних сигналів на поряд розташованих провідних лініях або

переміщування цих сигналів у лінії мережі електроживлення. Такими засобами можуть бути:

– закладні пристрої, що їх використовують для передавання перехоплюваної інформації лінії мережі змінного струму 220 В й які здатні працювати на частотах до 15 МГц;

– ПЕОМ та інші технічні засоби виготовлення, розмноження й передавання інформації;

– технічні засоби систем лінійного високочастотного нав'язування, що вони працюють на частотах понад 150 кГц;

– закладні пристрої, що вони використовують для передавання перехоплюваної інформації абонентські телефонні лінії, лінії систем пожежної й охоронної сигналізації з несучою частотою понад 20 кГц.

4 Виявлення та локалізування місця розташування джерел електромагнітних полів з перевагою (наявністю) магнітної складової поля, трас прокладання прихованої (непозначеної) електропроводки, потенційно придатної для встановлення закладних пристроїв, а також дослідження технічних засобів, що вони опрацьовують мовну інформацію.

До таких джерел та технічних засобів узвичаєно відносити:

– вихідні трансформатори посилювачів звукової частоти;

– динамічні гучномовці акустичних систем;

– електродвигуни магнітофонів та диктофонів.

5 Виявлення найбільш уразливих місць, з огляду на виникнення віброакустичних каналів витоку інформації, а також оцінення ефективності систем віброакустичного захисту приміщень.

6 Виявлення найбільш уразливих місць, з огляду на виникнення каналів витоку акустичної інформації, а також оцінювання ефективності звукоізолювання приміщення.

## 2.2 Режими роботи приладу

Розв’язок контрольно-пошукових завдань забезпечується певною сукупністю режимів роботи приладу.

Схемотехнічна та програмна база дозволяє використання приладу в таких режимах роботи:

- режимі високочастотного детектора-частотоміра;
- режимі сканувального аналізатора провідних ліній;
- режимі детектора інфрачервоних випромінювань;
- режимі детектора низькочастотних магнітних полів;
- режимі акустичного приймача.
- режимі віброакустичного приймача;

### 2.2.1 Органи керування приладом

Керування приладом здійснюється за допомогою 16 – кнопкової клавіатури, яка забезпечує керування приладом в усіх його режимах.

Призначення кнопок:

– MUTE – здійснює ввімкнення (вимикання) вмонтованого гучномовця;

– HELP – дозволяє дістати контекстну допомогу, яку можна змінювати за допомогою кнопок”∇” та ”Δ”;

– OSC – здійснює осцилографічний контроль параметрів сигналу;

– SA – здійснює ввімкнення спектрального контролю параметрів сигналу;

– SAVE – забезпечує запис осцилограми в пам’ять;

– LOAD – здійснює виклик на екран з пам’яті осцилограми чи спектрограми;

– RUN/STOP – здійснює пуск/ зупин. динамічних вимірювань параметрів сигналу;

– SET – дозволяє здійснювати вибір різноманітних варіантів аналізування спектра сигналу;

– ENTER – забезпечує виведення для слухового контролю тонального або де модульованого сигналу;

– RESET – здійснює перезапускання приладу.

### 2.2.2 Порядок управління приладом у режимі високочастотного детектора-частотоміра

Підімкнути телескопічну антену, використовуючи перехідник, або високочастотну антену до розніму RF ANT. Увімкнути живлення приладу.

Встановлення «нульового» порога детектора здійснюється автоматично, при вмиканні. У разі потреби, натисканням кнопок « ◀ » чи « ▶ » встановити вручну поріг детектора, керуючись показаннями додаткової шкали «min - - -|- - -max». В разі потреби, натисканням кнопки «▲» повернутися до режиму автоматичного встановляння порога.

Візуально, за кількістю цілковито пофарбованих елементів індикаторів рівня сигналу та «на слух», за частістю клацань у вмонтованому гучномовці або головних телефонах, оцінити рівень прийнятого сигналу.

За потреби натисканням кнопки SET встановити потрібні межі динамічного діапазону: (– 8...16) дБ; (– 8...32) дБ; (– 8...48) дБ.

Натиснути кнопку RUN/STOP і зупинити, за потреби, динамічні вимірювання рівня та частоти радіосигналу. Повторним натисканням цієї кнопки відновити динамічні вимірювання.

Натиснути кнопку ENTER (для переведення звукової індикації до режим AUD), прослухати наявність та зміст потенційно небезпечних модульованих радіовипромінювань.

Натисканнями кнопок «+» та «–» встановити необхідну гучність звукового сигналу (тонального чи демодульованого), виведеного на вмонтований гучномовець або на головні телефони.

Натиснути кнопку OSC і перейти, за потреби, до осцилографічного контролю параметрів сигналу.

Натиснути кнопку SA і перейти, за потреби, до аналізу спектра демодульованого сигналу.

У разі збивання у роботі натиснути кнопку RESET, та здійснити перезапускання приладу.

### 2.2.3 Порядок керування приладом у режимі скандувального аналізатора провідних ліній

Підімкнути мережний адаптер до розніму PROBES, а його щупи – до провідної лінії (або до лінії електромережі з напругою до 600 В).

Увімкнути живлення приладу.

Дочекатися дво–, трикратного «пробігу» підрядковим маркером діапазону сканування в автоматично встановлених межах 0,0....10,45 МГц.

Встановити необхідні, найбільш раціональні, межі сканування частотного діапазону.

Натиснути кнопку SET, потім кнопку «4». Натисканням кнопок з цифровим маркуванням набрати число, відповідне нижній межі діапазону.

Натисканням кнопки ENTER підтвердити завершення встановлення значення нижньої межі.

Натисканням кнопок з цифровим маркуванням набрати число, відповідне верхній межі діапазону.

Натисканням кнопки ENTER підтвердити встановлення верхньої межі діапазону.

За помилки, в перебігу набирання значень частот нижньої чи верхньої межі діапазону сканування натиснути кнопку « ◀ » й вилучити набране число.

Натиснути кнопку « ◀ » чи « ▶ » й обрати потрібні напрямки та швидкість сканування.

Натиснути кнопку SET, потім кнопку «3», до з’явлення на екрані в четвертому рядку напису: 3 - > ↑↓ THRESHOLD level.

Натисканням кнопки ENTER повернути на екран зображення панорами.

Натисканням кнопок « ▲ » та « ▼ » встановити найбільш зручну межу індикації вимірювача рівня сигналу (напис під горизонтальною віссю THRESHOLD level = XX%).

Натиснути кнопку RUN/STOP й зупинити в необхідному місці частотної осі автосканування. Натисканням кнопок « ◀ » чи « ▶ » провести точне ручне налаштовування на потрібну частоту. Прослухати демодульований сигнал.

Натисканням кнопки ENTER (AM/FM) обрати вид демодуляції (на слух, за якістю його відтворення).

Натиснути кнопку RUN/STOP і повернутися до автосканування.

Увімкнути систему автоматичної зупинки сканування на найбільш окреслених (за амплітудою) частотних складових панорами.

Натиснути кнопку SET, потім кнопкою «3» встановити в четвертому рядку меню напис 3 - > ↑↓ SQUELCH level.

Натиснути кнопку ENTER.

За допомогою кнопок «▲» та «▼» обрати бажаний рівень автоматичної зупинки автосканування (за положенням короткої горизонтальної риски в правій частині екрана). Після зупинки сканування кнопками «◀» та «▶» зробити уточнення налаштування, за ознакою якості демодульованого сигналу. Для продовження сканування натиснути кнопку RUN/STOP.

Увімкнути (за потреби) режим обчислення спектрів.

Натиснути кнопку SET, потім кнопку «2» та встановити напис «2 - > Difference ON D2-1».

Для початку процедури обчислення спектрів натиснути кнопку ENTER.

Вийти з режиму обчислення спектрів.

Натиснути кнопку SET, потім кнопкою «2» установити напис «Difference OFF».

Натиснути кнопку ENTER.

Записати, за потреби, зображення панорами в енергонезалежну пам'ять.

Натиснути кнопку SAVE, потім кнопку ENTER.

Викликати з пам'яті необхідне зображення панорами.

Натиснути кнопку LOAD.

Натисканням кнопки RUN/STOP повернути на екран панораму, яка динамічно відбивається.

Стерти (вилучити) з пам'яті зображення певної панорами.

Натиснути кнопку LOAD, потім SAVE та ENTER.

Натисканням кнопки OSC перейти, за потреби, до осцилографічного контролю параметрів сигналу.

Натисканням кнопки SA перейти, за потреби, до аналізу спектра сигналу.

У разі збивання у роботі натиснути кнопку RESET і здійснити перезапускання приладу.

### 2.2.4 Порядок керування приладом в режимі детектора інфрачервоних випромінювань

Підімкнути інфрачервоний давач до з'єднувального кабелю, а сам кабель – до розніму PROBES.

Увімкнути живлення приладу.

Встановлення «нульового» порога детектора здійснюється автоматично, при вмиканні. У разі потреби, натисканням кнопок «◀» чи «▶» встановити вручну поріг детектора, керуючись показами додаткової шкали «min - - -|- - - max». Якщо буде потрібно, натисканням кнопки «▲» повернутися до автоматичного встановлення порога.

Візуально, за кількістю цілковито пофарбованих елементів 21-сегментної шкали та «на слух», за частістю клацань у вмонтованому гучномовці чи то головних телефонах, оцінити рівень прийнятого інфрачервоного випромінювання.

Натисканням кнопки RUN/STOP зупинити, за потреби, динамічні вимірювання рівня інфрачервоного випромінювання. Повторним натисканням цієї кнопки відновити динамічні вимірювання.

Натисканням кнопки ENTER (для переведення звукової індикації до режиму AUD) прослухати наявність та зміст потенційно небезпечних модульованих інфрачервоних радіовипромінювань.

Натиснути кнопку MUTE й наступними натисканнями кнопок «+» та «–» встановити необхідну гучність звукового сигналу (тонального чи демодульованого), виведеного на вмонтований гучномовець, чи на головні телефони.

Натисканням кнопки OSC перейти, за потреби, до осцилографічного контролю параметрів демодульованого сигналу.

Натисканням кнопки SA перейти, за потреби, до аналізування спектра демодульованого сигналу.

У разі збивання у роботі натиснути кнопку RESET – і здійснити перезапускання приладу.

### 2.2.5 Порядок керування приладом в режимі детектора низькочастотних магнітних полів

Підімкнути зовнішню магнітну антену до з’єднувального кабелю, а сам кабель – до розніму PROBES.

Увімкнути живлення приладу. Осцилографічний контроль параметрів прийнятого по магнітному полю сигналу вмикається автоматично.

Візуально, за амплітудою та характером сигналу, на осцилограмі та на слух, за його тональністю, у вмонтованому гучномовці чи головних телефонах, оцінити рівень магнітного поля та присутність фону електромережі 220 В × 50 Гц чи її гармонік. За потреби, в разі високого рівня фону електромережі, перемикачем на її корпусі (положення до білої точки) увімкнути диференційний режим антени.

Натисканням кнопки RUN/STOP зупинити, за потреби, динамічні вимірювання. Повторним натисканням цієї кнопки відновити виведення на екран осцилограми, яка буде динамічно змінюватиметься.

Натиснути кнопку MUTE і наступними натисканнями кнопок «+» та «–» встановити потрібну гучність сигналу, виведеного на вмонтований гучномовець або на головні телефони.

Натиснути кнопку SA і перейти, за потреби, до аналізу спектра прийнятого сигналу.

У разі збивань у роботі натиснути кнопку RESET і здійснити перезапускання приладу.

### 2.2.6 Порядок керування приладом в режимі віброакустичного приймача

Підімкнути зовнішній віброакустичний давач до розніму PROBES.

Увімкнути живлення приладу.

Осцилографічний контроль параметрів прийнятого віброакустичним каналом сигналу вмикається автоматично.

Візуально, за амплітудою та характером сигналу на осцилограмі й «на слух», за його розбірливістю та якістю у вмонтованому гучномовці чи головних телефонах, оцінити рівень та темброві характеристики перетвореного звукового сигналу.

Натисканням кнопки RUN/STOP зупинити, за потреби, динамічні вимірювання. Повторним натисканням цієї кнопки відновити зображення осцилограми на екрані, яка динамічно змінюватиметься.

Натиснути кнопку MUTE і наступними натисканнями кнопок «+» та «–» встановити необхідну гучність сигналу, виведеного на вмонтований гучномовець чи на головні телефони.

Натисканням кнопки SA перейти, за потреби, до аналізування спектра сигналу, прийнятого у віброакустичному каналі.

У разі збивання у роботі натиснути кнопку RESET і здійснити перезапускання приладу.

### 2.2.7 Порядок керування приладом в режимі акустичного приймача

Підімкнути виносний мікрофон до розніму PROBES.

Увімкнути живлення приладу.

Осцилографічний контроль параметрів прийнятого акустичного сигналу вмикається автоматично.

Візуально, за амплітудою та характером сигналу на осцилограмі й «на слух», за його розбірливістю та якістю у вмонтованому гучномовці чи головних телефонах, оцінити рівень та темброві характеристики перетвореного звукового сигналу.

Натиснути кнопку RUN/STOP і зупинити, за потреби, динамічні вимірювання. Повторним натисканням цієї кнопки відновити виведення на екран осцилограми, яка динамічно змінюватиметься.

Натиснути кнопку MUTE і наступними натисканнями кнопок «+» та «–» встановити необхідну гучність сигналу, виведеного на вмонтований гучномовець, чи на головні телефони.

Натиснути кнопку SA і перейти, за потреби, до аналізування спектра сигналу, прийнятого акустичним каналом.

У разі збивання у роботі натиснути кнопку RESET та здійснити перезапускання приладу.

### 2.2.8 Порядок керування вмонтованим осцилографом, аналізатором спектра та енергонезалежною пам'яттю

Після ввімкнення осцилографічного контролю сигналу автоматично чи вручну через кнопку OSC (у режимах високочастотного детектора-частотоміра, сканувального аналізатора провідних ліній, детектора інфрачервоних випромінювань) встановлюється такий порядок використання органів керування приладом:

Натиснути кнопку «▲» чи «▼» та виставити, вручну, необхідне значення межі вертикальної розгортки.

Натиснути кнопку «◀» чи «▶» й обрати найбільш зручне, для переглядання осцилограми, значення межі горизонтальної розгортки.

Натиснути кнопку SET, далі кнопку «3» й обрати необхідний варіант оцифрування сигналу. Натисканням кнопки ENTER підтвердити вибір.

Натиснути кнопку SET, далі кнопку «4» й обрати необхідний режим синхронізації. Натисканням кнопки ENTER підтвердити вибір.

Натиснути кнопку SET, далі кнопку «5» і встановити необхідний варіант умови синхронізації. Натисканням кнопки ENTER підтвердити вибір.

Якщо відсутня потреба використання чисельних значень параметрів сигналів, котрі відбиваються на осцилограмі, натиснути кнопку MUTE. Її повторне натискання повертає на екран зображення індикації чисельних значень параметрів аналізованого сигналу.

Натиснути кнопку RUN/STOP і ввімкнути, за потреби, режим курсорних вимірювань. Натисканням кнопок «◀» та «▶» встановити вертикальний маркер в необхідне місце осцилограми.

Натиснути кнопку RESET та провести, за потреби, відносні вимірювання тимчасових інтервалів.

Натисканням кнопки RUN/STOP вийти з режиму курсорних вимірювань.

Натисканням кнопки ENTER перевести осцилограф до двоканального режиму з подаванням сигналу другим каналом через додатковий рознім OSC2. Повторним натисканням кнопки ENTER передати функції вимірювання та індикації на другий канал по входу OSC2.

Натисканням кнопки RESET знову запустити прилад в активованому режимі, потім кнопкою OSC повернути режим одноканального осцилографа .

Двічі, з інтервалом у 2 с, натисканням кнопки OSC, перевести осцилограф до одноканального режиму, з подаванням сигналу лише по додатковому входу OSC2.

Натисканням кнопки RESET знову запустити прилад до активованого режиму, потім кнопкою OSC повернути попередній осцилографічний режим.

Натисканням кнопки SAVE, далі кнопки ENTER записати необхідну осцилограму в енергонезалежну пам'ять.

Натисканням кнопки LOAD вивести на екран зображення кожної із записаних до пам'яті осцилограм.

Натисканням кнопки RUN/STOP, повернути режим роботи осцилографа до попереднього стану.

Натисканням кнопки LOAD, потім кнопки SAVE та ENTER стерти, вилучити з пам'яті осцилограму, яка не становить інтересу.

Натисканням кнопки SA увімкнути аналізатор спектра.

Натиснути кнопку «▲» чи «▼» й виставити, за потреби, відповідне значення межі вертикального розгорнення.

Натиснути кнопку «◀» чи «▶» й обрати найбільш зручне значення межі горизонтальної розгортки.

Натиснути кнопку SET, далі однією з кнопок – «2», «3», «4», «5» та «6» – обрати необхідний варіант режиму аналізування спектра. Зроблений вибір бажано щоразу потверджувати натисканням кнопки ENTER.

Якщо відсутня потреба використання чисельних значень параметрів сигналів, котрі відбиваються на спектрограмі, натиснути кнопку MUTE. Повторне натискання цієї кнопки повертає на екран індикацію чисельних значень параметрів аналізованого сигналу.

Натисканням кнопки RUN/STOP увімкнути, за потреби, режим курсорних вимірювань. Натисканням кнопок «◀» та «▶» встановити вертикальний маркер на необхідну частотну складову спектрограми.

Натисканням кнопки RESET провести, за потреби, відносні вимірювання частотних інтервалів.

Натисканням кнопки RUN/STOP вийти з режиму курсорних вимірювань.

Натисканням кнопки ENTER перевести аналізатор спектра до двоканального режиму з подаванням сигналу другим каналом через додатковий рознім OSC2. Повторним натисканням кнопки ENTER передати функції вимірювання та індикації на другий канал по входу OSC2.

Натисканням кнопки RESET знову перевести прилад до активованого режиму, потім кнопкою SA повернути аналізатор спектра до попереднього одноканального режиму.

Двічі, з інтервалом у 2 с, натисканням кнопки SA перевести аналізатор до одноканального режиму з подаванням сигналу лише по додатковому входу OSC2.

Натисканням кнопки RESET знову перевести прилад до активованого режиму, потім кнопкою SA повернути попередній режим аналізатора спектра.

Натисканням кнопки SAVE, потім кнопки ENTER записати необхідну спектрограму до енергонезалежної пам'яті.

Натисканням кнопки LOAD вивести на екран зображення кожної із записаних до пам'яті спектрограм.

Натисканням кнопки RUN/STOP повернути аналізатор спектра до попереднього стану.

Натисканням кнопки LOAD, потім кнопок SAVE та ENTER стерти (вилучити) з пам'яті спектрограму, яка не становить інтересу.

# 3 Рекомендації з проведення контрольно-пошукових робіт з використанням приладу ST– 031 Піранья

## 3.1 Методи пошуку та локалізування джерел небезпечних радіосигналів

У практиці взагалі й за роботи з приладом ST – 031 Піранья зокрема, використовують роздільно або в сполученні два головних методи пошуку та локалізування джерел небезпечних радіосигналів. Ними є так звані амплітудний метод та метод акустичної зав'язки.

Амплітудний метод ґрунтується на різкому зростанні рівня прийнятого сигналу при наближенні приймальної антени приладу до місця розташування його джерела. Радіус зони виявлення джерела залежить від потужності випромінюваного сигналу, спрямованості його антени та рівня фону електричного поля в місці розташування приймальної антени приладу.

Після фіксації факту виявлення потенційно небезпечного радіосигналу слід рухатися в напрямку зростання його рівня. Контроль за рівнем прийнятого сигналу треба здійснювати за показниками індикаторів рівня на екрані дисплея приладу за частотою клацань звукової сигналізації в режимі TONE.

Метод акустичної зав'язки ґрунтується на виникненні позитивного акустичного зворотного зв'язку поміж мікрофоном радіо закладки та динаміком приладу ST – 031 Піранья. Обов'язкове є ввімкнення звукової сигналізації приладу до режиму AUD для виведення на динамік демодульованого сигналу. Ефект акустичної зав'язки виникає лише стосовно радіозакладки, в якій застосовано звичайні види модуляції – амплітудна й частотна (вузько смугова чи широкосмугова). Причому, у разі частотної модуляції ефект грунтується на наявності паразитної амплітудної модуляції в частотно-модульованому сигналі (в разі якісно виконаної радіозакладки ефект акустозав’язки буде досить слабким, аж до повної відсутності).

Ознакою виникнення акустозав’язки є характерний писк, тон і інтенсивність якого змінюються при наближенні динаміка приладу до мікрофона «радіозакладки».

Слід враховувати, що наявність характерного звуку при використанні даного методу демаскує проведення робіт. Тому, в разі застосування радіозакладок з дистанційним керуванням вони можуть бути вимкнені на час перевірки.

Раціональний вибір того чи іншого методу багато в чому залежить від особливостей, притаманним потенційно небезпечним радіосигналам та їхнім джерелам.

## 3.2 Основні правила та особливості проведення контрольно-пошукових робіт

Початковий етап підготовки проведення контрольно-пошукових робіт полягає в створенні таких умов, за яких забезпечується мінімально можливий

рівень фону електричного поля. Це досягається вимкненням потенційних джерел підвищення фону, якими є засоби оргтехніки, ПЕОМ, перетворювачі та блоки живлення, базові станції безпроводових телефонів, люмінесцентні освітлювальні лампи й інші електронні пристрої та електроприлади. Доцільно також зачинити вікна і двері, спустити (задвинути) штори чи жалюзі.

Надто слід звернути увагу на те, щоби було вимкнено радіотелефони й інші радіопередавальні засоби, а також засоби активного радіотехнічного захисту. Не припускається робота приладу ST – 031 Піранья з нелінійними локаторами.

Якщо об'єктом перевірки є автомобіль, то необхідно правильно обрати, з погляду на зменшення рівня електромагнітного фону, місце проведення робіт. Приміром, поблизу нього не повинні знаходитися високовольтні лінії електропередач, трансформаторні підстанції, випромінювальні засоби зв'язку, теле- й радіомовлення, а також великі, відбивальні (чи перевипромінювальні) поверхні – металеві огородження, стіни будинків, гаражі, інші автомобілі.

Пошук потенційно небезпечних радіосигналів та їхніх джерел зазвичай провадять послідовно, по черзі перевіряючи наявність:

- автономних радіомікрофонів та телефонних радіоретрансляторів;
- камуфльованих радіомікрофонів, що вони живляться від електромережі;
- радіостетоскопів;
- прихованих відеокамер з радіоканалом;
- просторового високочастотного опромінення;
- радіозакладок у ПЕОМ.

Для створення акустичного фону й активізування радіозакладок з акустопуском слід підготувати та розмістити в контрольованому приміщенні тестове джерело звуку. Таким джерелом може бути магнітофон з добре відомою музичною чи мовною фонограмою. Не рекомендується використовувати для таких цілей радіоприймач чи телевізор, тому що створюваний ними звуковий сигнал, перевипромінюваний радіозакладкою, може збігтися з радіосигналом власної мовної станції. Вибір гучності тестового звукового сигналу визначається як розмірами приміщення, так і чутливістю мікрофона радіозакладки. Зазвичай такі мікрофони впевнено сприймають звук середньої гучності з відстані порядка 10 м.

Підготовка самого приладу ST – 031 Піранья, після перевірки його працездатності в даному режимі, полягає у встановленні нульового порога детектора, що, фактично, визначає умови для успішного проведення робіт. Заниження порога обов'язково призведе до частих помилкових спрацьовувань індикації, а його завищення – до ймовірного пропускання сигналу радіозакладки. Й те й те значно ускладнює роботу оператора, збільшує час і знижує вірогідність результатів перевірки. Тому при встановленні нульового порога слід неодмінно дотримуватися кількох найпростіших правил.

**Не можна** провадити встановлення порога в перевіюваному приміщенні, тому що при функціонуванні в ньому вже розміщеної радіозакладки, рівень її радіовипромінювання буде визначено приладом як нульовий.

Під час налаштовування порога **неприпустиме** є використання радіостанцій, радіотелефонів та інших радіовипромінювальних засобів.

**Не слід наближати** антену приладу до ввімкнених ПЕОМ та інших засобів оргтехніки, як джерел ПЕОМ, в діапазоні роботи приладу.

**Не припускати** контакту антени приладу з металевими предметами та проводами, які є джерелами перевипромінюваних високочастотних сигналів.

Тому налаштовування приладу слід виконувати в одному з найближчих до перевірюваного приміщень, у якому, приблизно, рівень фону істотно не відрізняються, а встановляння радіозакладок є чи то неможливе, чи то недоцільне. Під такими приміщеннями зазвичай розуміють приміщення іншого призначення, але котрі розташовано на тім самім поверсі і з віконними прорізами, які виходять на той самий бік будинку.

Якщо об'єктом перевірки є автомобіль чи інший транспортний засіб, то, забезпечивши правильний вибір місця робіт, налаштовування нульового порога слід провадити не ближче за 10....20 м від нього.

Після встановлення нульового порога прилад переміщують у контрольоване приміщення (до контрольованого об'єкта) БЕЗ ВИМИКАННЯ ЖИВЛЕННЯ, тому кожне наступне його ввімкнення призводить до автоматичного встановлення порога вже стосовно нових умов електромагнітної обстановки.

Пошук автономних радіомікрофонів та телефонних радіоретрансляторів доцільно здійснювати, вимкнувши з розеток електромережі шнури живлення всіх санкціонованих споживачів та освітлювальні прилади з лампами розжарювання.

З урахуванням того, що радіочастотний тракт приладу ST– 031 Піранья виконано за сполученою схемою детектора-частотоміра, для його застосовування придатні ті ж самі прийоми й методи, як і для автономних детекторів, інтерсепторів та радіочастотомірів. У цілому вони полягають в такому.

Якщо не накладаються обмеження на приховання проведення робіт, то найоптимальний ефект дає поєднання амплітудного методу й методу акустозав'язки. При проведенні прихованого пошуку необхідно орієнтуватися на амплітудний метод із прослуховуванням детектованих сигналів через головні телефони. Особлива увага звертається на радіовипромінювання в діапазоні 60....640 МГц, найбільш типовому для використання радіомікрофонами й телефонними радіоретрансляторами.

Пошук здійснюється шляхом планомірного обходу приміщення (об'єкта) з рухом уздовж стін і обстеженням меблів та інших розташованих у ньому предметів. Через доволі велику чутливість високочастотної антени пошук доцільно починати із застосуванням телескопічної антени. При обході антену слід орієнтувати в різних площинах, роблячи плавні, повільні повороти основного блока й домагаючись максимального рівня сигналу. Антену приладу

доцільно тримати на відстані не більш 20....25 см від обстежуваних поверхонь та предметів. За відсутності обмежень на використання методу акустозав'язки динамік вмонтованого гучномовця приладу слід орієнтувати в бік обстежуваних поверхонь та предметів (рівень гучності повинен бути встановлено на значення не менш за максимальне).

При наближенні антени приладу ST – 031 Піранья до місця розміщення радіозакладки напруженість електромагнітного поля зростає, відповідно підвищується й рівень сигналу на його вході. З перевищенням рівня сигналу встановленого нульового порога, залежно від виду сигналу, збільшується кількість пофарбованих секторів одного з рядків індикатора рівня й, розпочинаючи з четвертого (відлік від нульової оцінки), зростає частість клацань звукової сигналізації в режимі TONE, а за ввімкнення режиму AUD та динаміка гучномовця виникає акустозав'язка.

У разі перебування джерела з частотно модульованим сигналом збільшуватиметься кількість пофарбованих секторів верхнього індикатора рівня сигналу. При достатньому наближенні до джерела радіочастотомір здійснює захоплення частоти й зазначає в останньому рядку екрана її значення за результатами декількох вимірювань. Шляхом зменшення гучності кнопкою «– », зміни межі динамічного діапазону кнопкою SET, збільшення вручну порога спрацьовування детектора, постійного спостереження за показами частотоміра звужується зона обстеження й тим самим злокалізовується місце встановлення радіозакладки з похибкою в межах 10....15 см. Додаткові можливості, насамперед щодо класифікування радіовипромінювань, надає періодичне ввімкнення режиму AUD та прослуховування демодульованого сигналу.

Однак слід пам'ятати, що ефект акустозав'язки й виразне прослуховування демодульованого сигналу спостерігаються не завжди, наприклад, якщо закладки мають маскований радіоканал, тому в підґрунті їхнього пошуку лежить використання амплітудного методу в чистому вигляді. Доповнювальним тут може бути простий прийом. Якщо вимкнути джерело тестової фонограми і створити в перевірюваному приміщенні короткий різкий звук (удар по кришці столу чи по металевому предметові), то можна зафіксувати характерні зміни демодульованого сигналу на слух у режимі AUD, зміни осцилограми в режимі OSC та спектрограми в режимі SA.

У разі застосування радіозакладки з цифровими методами модулювання індикація підвищення рівня буде відбиватися на нижньому індикаторі. Індикація частоти прийманого сигналу в даному разі буде випадковою.

У разі застосування в якості радіозакладки телефонів стандарту DECT чи GSM, окрім індикації підвищення рівня сигналу в нижньому рядку, на індикаторі з'явиться напис DECT чи GSM.

Аналогічно до пошуку радіомікрофонів здійснюється пошук телефонних радіоретрансляторів. При цьому, для їхньої активізації, необхідно зняти трубки всіх телефонних апаратів. Власне пошук провадиться в два етапи.

Спочатку на наявність закладних пристроїв перевіряються власне самі телефонні апарати. Встановлений в апараті радіоретранслятор виявляється у такий самий спосіб, як і радіомікрофон. При наближенні антени приладу до

такого телефонного апарата реагують засоби звукової (у режимі TONE) індикації, індикатор рівня сигналу та частотомір. При перемиканні до режиму AUD у динаміку чи в головних телефонах прослуховується або неперервний, або переривчастий тональний сигнал телефонної станції. У низці випадків при наближенні мікрофона телефонної слухавки до динаміка приладу ST – 031 Піранья може виникнути ефект акустозав'язки. Не рекомендується перевіряти телефонні апарати в режимі гучномовного зв'язку (якщо його передбачено), тому що в цьому разі може виникнути помилкова акустозав'язка поміж мікрофоном та динаміком самого апарата.

Далі пошук телефонних радіоретрансляторів здійснюється шляхом обходу приміщення уздовж абонентської телефонної лінії та виявлення на ній місць зі зростанням (максимумом) рівня радіосигналу. При обході антену приладу необхідно орієнтувати в різних площинах на мінімально можливій відстані від лінії. Практично завжди існує необхідність перевірки лінії аж до головного розподільного щита. Особливу увагу необхідно звертати на розподільні коробки й місця, де лінію прокладено прихованою проводкою. Встановлені на лінії телефонні радіоретранслятори локалізуються переважно амплітудним методом, що доповнюється перевіркою на виникнення акустозав'язки.

Пошук закамуфльованих радіомікрофонів, що вони живляться від електромережі, й локалізування місця їхнього встановлення здійснюються тими ж самими методами, що їх було схарактеризовано вище. Для їхньої активізації необхідно ввімкнути тестове джерело звуку. По черзі ввімкнути наявні освітлювальні прилади з лампами розжарювання й підімкнути до розеток електромережі шнури живлення санкціонованих споживачів. Послідовно провести обстеження кожного із знову підімкнути засобів.

Пошук радіостетоскопів має певні особливості, зумовлені способами їхнього застосовування (встановлення поза контрольованим приміщенням). Тому для виявлення сигналів радіо стетоскопів слід обстежувати всі реально приступні зовнішні поверхні конструкцій, які огороджують приміщення. Оскільки середовищем поширення віброакустичних коливань можуть бути труби опалення та водопостачання, то перевірці підлягають і ці комунікації.

У переважній більшості радіостетоскопи використовують відкритий радіоканал. Це дає можливість аналізування прийнятого сигналу на слух в режимі AUD. При перевірці конструкцій, які огороджують приміщення, антену приладу слід розташовувати на мінімально можливій відстані від обстежуваних поверхонь, тому що радіус зони виявлення сигналу від радіостетоскопа зазвичай є менше, аніж від радіомікрофонів. При перевірці трубопровідних комунікацій необхідно виконувати такі ж самі рекомендації, але не припускати контакту антени з металевими поверхнями.

Локалізування радіостетоскопів здійснюється амплітудним методом у суміжних приміщеннях, що доповнюється, потреби, використанням режимів OSC і SA.

Пошук прихованих відеокамер з радіоканалом передавання зображення (часто і звуку) пов'язано з певними труднощами, котрі визначаються

подібністю сигналу відеопередавача із сигналом яскравості передавачів телевізійного мовлення й роботою значної кількості цих пристроїв у діапазоні телестанцій (від 60 МГц до 500 МГц). Тому в перебігу проведення робіт при виявленні такого сигналу першим є завданням його розпізнавання за критерієм зовнішній–внутрішній. Для розпізнавання необхідно закрити вікна шторами чи жалюзями, залишивши ввімкненим внутрішнє освітлення. Зробити кілька разів вмикання й вимикання штучного освітлення. При ввімкненому режимі AUD мають прослуховуватися виразні зміни тону продетектованого сигналу. Для підвищення надійності розпізнавання ввімкнути режим OSC й переконатися в зміненні структури сигналу за осцилограмою при вмиканні й вимиканні освітлення. Вид осцилограми радіосигналу передавання відеоінформації за різних значень параметрів горизонтальної розгортки подано на рисунках 1.1 та 1.2.

Якщо результати зазначеної перевірки є позитивні, то сигнал упевнено можна віднести до категорії внутрішніх, створюваних передавачем відеокамери, тому що зміна освітленості приміщення на параметри сигналу телевізійного мовлення не впливає. Принципово передавачі відеокамер можуть працювати на частотах до 2300 МГц.

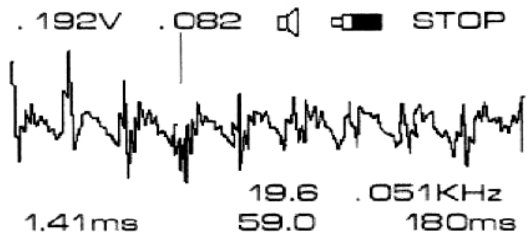



Рисунок 1.1 – Радіосигнал передавання відеоінформації, період розгортки 180 мс

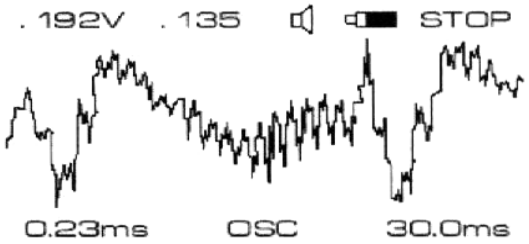



Рисунок 1.2 – Радісигнал передавання відеоінформації, період розгортки 30 мс

Виявлення сигналу (схожого на сигнал яскравості) на частотах поза діапазоном телевізійного мовлення практично однозначно свідчить про роботу передавача прихованої відеокамери. Локалізування таких засобів здійснюється амплітудним методом.

Стосовно просторового високочастотного опромінювання, головним є завдання виявлення факту створення цього штучного каналу знімання інформації. Зазвичай таке завдання розв’язується у два етапи. На першому етапі виявляється факт опромінення приміщення високочастотним сигналом. На другому етапі відстежується відгук на зондувальний високочастотний сигнал. При цьому слід орієнтуватися на такі моменти. Гостроспрямований промінь електромагнітної енергії може бути сформовано лише на надто високих частотах (800....900 МГц і вище). Особливості поширення радіохвиль цього діапазону (необхідність прямої видимості поміж джерелом випромінювання й опромінюваними предметами) визначають як основні шляхи їхнього проникнення в контрольоване приміщення, насамперед віконні прорізи.

Перевипромінюваними об'єктами можуть бути звичайні для даного приміщення технічні засоби, яким є притаманний так названий мікрофонний ефект (паразитні акустоелектричні перетворювачі). До них зазвичай відносять динаміки побутових гучномовців, акустичні системи навіть вимкненої аудіоапаратури, телефонні апарати з електричним дзвінком й т. п. Перевипромінений сигнал на частотах вищих (найчастіше другої чи третьої) гармонік локалізується в безпосередній близькості від опромінюваних предметів і має модулювання акустичним фоном приміщення.

Виходячи з викладеного, може бути використано такий порядок роботи.

Для виявлення факту високочастотного опромінювання слід обстежувати потенційно небезпечні віконні прорізи. Для цього піднести антену до внутрішнього скла на відстань 5....10 см, зафіксувати рівень та частоту найбільш потужного сигналу. Увімкнути режим AUD і на слух визначити наявність та особливості демодульованого сигналу. За графічним індикатором оцінити стабільність частоти випромінювання. Перейти в кожне з сусідніх приміщень (орієнтованих вікнами в той самий бік) і повторити перевірку в районі кожного з його віконних прорізів. Високочастотне випромінювання є цілком імовірне, якщо:

- частота прийнятого сигналу лежить (або надто близько) у межах зазначеного діапазону;
- стабільність частоти є висока;
- модуляція сигналу відсутня;
- у сусідніх, відносно перевірюваного, приміщеннях рівень прийнятого сигналу є значно менший.

Для виявлення джерел перевипромінювання необхідно ретельно обстежувати кожний, з потенційно небезпечних предметів, розміщуючи антену приладу в безпосередній близькості до нього. Підставою для ухвалення остаточного рішення щодо опромінювання та наявності у приміщенні перевипромінювальних предметів є покази індикатора рівня приладу ST – 031 Піранья та його частотоміра, а також результати прослуховування в режимі AUD. При цьому запереважні ознаки зазвичай розглядають фіксацію номіналу частоти, кратну максимуму третьої гармоніки опромінювального сигналу та ідентифікацію звукового сигналу в режимі AUD з акустичним фоном приміщення.

Перевірку ПЕОМ на наявність у них радіозакладок, доцільно провадити в останню чергу. Це зумовлено тим, що у ввімкненому стані вони створюють доволі інтенсивні побічні радіовипромінювання в діапазоні до 1000 МГц і вище, тобто є джерелами підвищення електромагнітного фону, що може маскувати випромінювання раніше розглянутих радіозакладних пристроїв. При цьому слід мати на увазі, що радіозакладки можуть передавати як сигнали, що відповідають зображенню на екрані монітора, так і сигнали, котрі несуть цифрову інформацію, опрацьовувану елементами системного блоку. І ті й ті сигнали мають вельми виразні зовнішні ознаки, що вони виявляються на їхніх осцилограмах у режимі OSC. Перші за структурою схожі із сигналом

передавачів відеокамер, а другі являють собою чітко позначену імпульсну послідовність.

Для виявлення сигналів радіозакладок слід переміщувати антену приладу ST – 031 Піранья навколо монітора й системного блока, фіксуючи рівень прийнятого сигналу й покази частотоміра. Наявності в ПЕОМ радіозакладки та її роботі на передавання, відповідають різке зростання рівня прийнятого сигналу й відносно висока стабільність частоти. У цьому разі слід зафіксувати положення антени, якому відповідає максимальний рівень, увімкнути режим OSC й візуально оцінити вид сигналу. Для запобігання помилковим висновкам, порівняти його з осцилограмою побічних електромагнітних випромінювань монітора ПЕОМ, вигляд якої подано на рисунку 1.3.

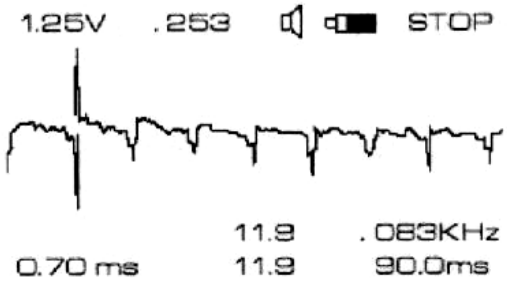



Рисунок 1.3 – ПЕМВ
монітора ПЕОМ

Визначення місця встановлення радіозакладки здійснюється, окрім того, й шляхом послідовного вмикання та вимикання монітора й системного блока.

Методика пошуку й локалізування несанкціоновано вмиканих на передавання радіостанцій, радіотелефонів, телефонів з радіоподовжувачами та радіомаяків є цілковито аналогічна до методики пошуку й локалізування радіомікрофонів. Причому в переважній більшості випадків слід орієнтуватися на амплітудний метод з періодичним прослуховуванням демодульованого сигналу в режимі AUD.

### 3.3 Використання приладу для виявлення каналів витоку інформації провідними лініями різного призначення

Тут розглядаються прийоми виявлення штучно створених каналів витоку інформації провідними лініями, в основу яких покладено використання спеціальних технічних засобів. Головними видами провідних ліній, для аналізу яких призначено прилад ST – 031 Піранья, є лінії електромережі (високопотенційні лінії), а також абонентські телефонні лінії та лінії систем пожежної й охоронної сигналізації (низькопотенційні лінії).

Взагалі прийоми й методи, застосовувані для перевірки провідних ліній зазначених видів, є однакові. Підімкнення до них здійснюється з використанням єдиного, універсального адаптера. Аналізування методом сканування підлягає загальний діапазон від 0 до 15 МГц. Висновок результатів сканування надається у вигляді зображення панорами з однотипним поданням

(відбиттям) вимірюваних параметрів. Функції органів керування приладом є одинакові (поза залежністю від виду перевірюваної лінії).

Загальні (для всіх ліній) положення методики роботи полягають у такому.

Проведення підготовки контрольованого приміщення полягає в перевірці відповідності кількості та призначення реально існуючих в ньому провідних ліній раніше виготовленим (поданим) схемам їхнього прокладання.

Підготовка самого приладу ST – 031 Піранья, після перевірки його працездатності в даному режимі, фактично полягає лише у виборі найбільш зручних наконечників до щупів стосовно типу й особливостей наявних провідних ліній.

Найбільшу увагу слід приділяти діапазонові 40....2500 кГц, як найбільш типовому для використання закладками, котрі живляться від напруги провідних ліній, й передавання перехопленої інформації з їхніх проводів. Значно рідше зустрічаються закладні пристрої з частотами близько 7 МГц та вище. Для забезпечення гарантованої надійності щодо не пропускання сигналів закладок за частотою верхню межу діапазону сканування в приладі ST – 031 Піранья визначено на рівні 15 МГц.

Рекомендується такий порядок дій оператора.

1 Увімкнути прилад.

2 Дочекатися початку сканування в діапазоні до 10....450 МГц і після завершення двох- трьох циклів встановити верхню межу діапазону на рівні 15МГц. Уважно вивчивши найбільш характерні особливості зображення панорами, визначити наявність частотних складових, які перевищують рівень загального фону.

3 За необхідності розбити діапазон на окремі інтервали й просканувати їх докладно, зупиняючись насамперед на частотах найбільш інтенсивних складових.

4 Межі інтервалів задаються послідовним натисканням кнопок SET, «4», кнопок з цифровим маркіруванням та кнопки ENTER (або альтернативний варіант із завданням центральної частоти та ширини смуги).

5 Встановити нижній поріг індикації рівня сигналу порядку 10…15 %. Для цього натиснути кнопку SET, кнопкою «3» вивести напис 3 - ( (( THRESHOLD level, натиснути кнопку ENTER і кнопками «(» та «(» домогтися встановлення цього порога індикації. В подальшому, подальшому залежно від характеру зображення панорами, обрати найбільш зручний для аналізу рівень порога.

6 Запускання й зупинка сканування здійснюються натисканням кнопки RUN/STOP.

7 Після проходу декількох циклів сканування можна обґрунтовано встановити поріг «автостопа» для чого натиснути кнопку SET, обрати кнопкою «3» режим SQUELCH LEVEL, підтвердити вибір кнопкою ENTER і, маніпулюючи кнопками «(» та «(», поставити курсор на необхідний рівень. Після зупинки на частоті того чи іншого сигналу слід зробити точне налаштовування кнопками «(» та «(», водночас аналізуючи сигнал «на слух» почерговим ввімкненням детекторів AM та FM кнопкою ENTER. Для аналізу

слабких сигналів можна обрати кнопками SET «5» та ENTER більш зручний амплітудний діапазон (0,1…1 мВ).

8 За потреби доповнити можливості аналізу сигналів у провідних лініях перемиканням приладу в режими OSC та SA, тому що зображення осцилограм та спектрограм сигналів, виведених на екран дисплея, дають більш докладну характеристику параметрів. У цьому можна переконатися порівнянням зображень панорами й осцилограми того самого цифрового сигналу передавання мовної інформації (див. рис.1.4 та рис.1.5).

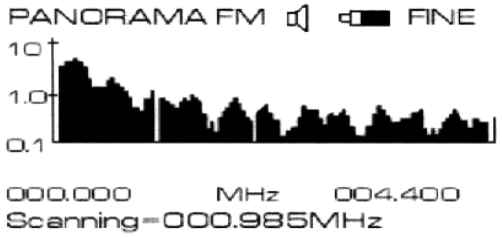



Рисунок 1.4 – Панорама цифрового сигналу передавання мовної інформації в провідній лінії

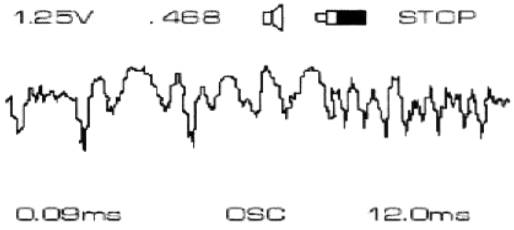



Рисунок 1.5 – Осцилограма цифрового сигналу передавання мовної інформації в провідній лінії (цей самий сигнал)

Якщо приміщення включено до плану регулярних періодичних перевірок, то доцільно зберегти в енергонезалежній пам'яті панораму (осцилограму, спектрограму) необхідних частотних інтервалів. Для збереження натиснути кнопки SAVE та ENTER. Для виклику з пам'яті потрібної панорами (осцилограми, спектрограми) натискати кнопку LOAD. Разом з тим необхідно враховувати й певні особливості, зумовлені специфікою ліній кожного виду.

Перевірку наявності в електромережі спеціальних технічних засобів, які приймають акустичні сигнали з приміщення, що вони живляться від мережі й передають інформацію на високій частоті її проводами, доцільно розпочинати з мережних розеток. Для зменшення рівня фону слід вимкнути (з механічним від'єднанням від розеток) всі електроприлади й апаратуру, розміщену в контрольованому приміщенні.

Підімкнути прилад до мережі, використовуючи для цього кожну з розеток (як правило, енергозабезпечення приміщення здійснюється від однієї фази або, принаймні, від одного розподільного щитка).

Провести аналіз зображення панорами.

Якщо виявлено сигнал, що він містить ознаки модуляції акустикою приміщення, то для локалізування його джерела може бути використано метод акустозав’язки за почергового підмикання до всіх розеток у перевірюваному приміщенні.

Аналогічну перевірку провести на елементах ліній, котрі живлять електроосвітлювальні прилади.

Після перевірки силових ліній та ліній, що вони живлять освітлювальні прилади, необхідно перевірити трійники, подовжувачі та інші

електроспоживальні засоби шляхом їхнього почергового підмикання до електромережі.

Перевірка провідних ліній систем пожежної й охоронної сигналізації, а також ліній невідомого призначення, є аналогічно до перевірки ліній електромережі, тому що аналогічні є власне самі технічні засоби, використовувані на цих комунікаціях.

При перевірці абонентських телефонних ліній, окрім пошуку описаних вище спеціальних технічних засобів, слід, розв'язувати завдання виявлення факту використання лінії для знімання акустичної інформації з приміщення за рахунок лінійного високочастотного нав'язування. Ознакою факту лінійного високочастотного нав'язування є наявність в лінії немодульованого стабільного зондувального сигналу на частотах не нижче за 150 кГц. При цьому порядок підмикання приладу та процедура аналізу стосовно перевірки ліній електромережі не відрізняються від викладеного.

### 3.4 Використання приладу для виявлення каналів витоку інформації в інфрачервоному діапазоні

Принципово слід розглядати два види таких каналів витоку інформації. Один з них утворюється за рахунок застосовування спеціальних технічних засобів з передавання перехоплюваної інформації в інфрачервоному діапазоні. Інший канал грунтується на опроміненні віконних скляних прорізів спрямованим променем джерела інфрачервоних випромінювань та прийманні відбитого сигналу, промодульованого акустикою приміщення.

Для виявлення обох каналів витоку слід провести однакові підготовчі заходи. Насамперед слід правильно обрати час проведення перевірки, а саме такий, коли у вікна контрольованого приміщення не потрапляють прямі сонячні промені. У самому приміщенні необхідно вимкнути лампи розжарювання та джерела інтенсивного теплового випромінювання. Доцільно також вимкнути, якщо він є, кольоровий телевізор, тому що давач приладу може реагувати на теплі тони зображення.

Специфіка інфрачервоних закладок визначає необхідність забезпечення прямої видимості поміж передавачем закладки та приймачем інфрачервоних випромінювань. Тому в приміщенні шлях слідування випромінювання передавача назовні може пролягати лише через віконні прорізи. З урахуванням цих особливостей пошук небезпечних сигналів слід розпочинати від вікон приміщення, пересуваючись у глиб його. Оскільки в передавача може бути досить вузька діаграма спрямованості, а кут зору давача приладу становить $30^{o}$C, необхідно плавно змінювати просторове орієнтування давача. Ознакою наявності інфрачервоного випромінювання є з'явлення пофарбованих сегментів шкали індикатора рівня та клацання звукової індикації в режимі TONE після фарбування 4-го елемента шкали. Аналіз виявлених сигналів може провадитися на слух в режимі AUD, а також візуально, з використанням вмонтованих осцилографа та аналізатора спектра. Локалізування джерел інфрачервоного випромінювання найбільш точно здійснюється поєднанням амплітудного

методу та методу акустозав'язки. При цьому порядок діє такий самий, як і при роботі в режимі високочастотного детектора-частотоміра.

Для виявлення зовнішніх потенційно небезпечних інфрачервоних випромінювань слід обстежувати кожен віконний проріз. При цьому давач орієнтується в бік вікна. Плавно змінюючи його просторове положення, провести обстеження всієї площі віконного прорізу. Оскільки зондувальний сигнал не має модуляції, то його наявність може бути оцінено лише за показниками індикатора рівня та тональної індикації в режимі TONE.

### 3.5 Використання приладу для виявлення каналів витоку інформації низькочастотними магнітними полями

Для таких каналів характерне є те, що вони виникають при використанні за цільовим призначенням санкціонованих засобів (ПЕОМ, переговорних пристроїв, систем звукопосилення, магнітофонів, телефонів тощо). Тому за одне з головних завдань слід вважати дослідження таких засобів на наявність, інтенсивність та дальність низькочастотного магнітного поля. Супутними можуть вважатися завдання пошуку прихованої (несанкціоновано прокладеної) проводки та виявляння працюючих диктофонів.

Перед проведенням робіт доцільно вимкнути в приміщенні люмінесцентні світильники, а антену приладу, за необхідністю, ввімкнути в диференційному режимі (перемикач на корпусі антени поставити в положення до білої точки).

Потенційні джерела небезпечних низькочастотних магнітних полів слід перевіряти роздільно, включаючи їх у роботу по черзі.

При дослідженні технічних засобів слід оцінити дальність поширення магнітних полів та особливості їхнього спектра. Для цього спочатку розмістити магнітну антену в безпосередній близькості до досліджуваного об'єкта. Зафіксувати за осцилограмою відносний рівень поля. Віддаляючись від досліджуваного засобу і змінюючи просторове орієнтування антени, оцінити дальність упевненого приймання низькочастотного сигналу.

Стосовно посилювачів звукової частоти, що вони мають вихідний трансформатор, слід оцінити дальність упевненого (розбірливого) приймання мовного (тестового) сигналу. Таке оцінювання може слугувати за основу для правильного вибору місць установлення відповідних засобів стосовно зовнішнього боку приміщення та варіанта їхнього спільного розташування в приміщенні. За необхідності ввімкнути режим SA, проаналізувати спектрограму й записати її до енергонезалежної пам'яті.

Для пошуку прихованої проводки треба послідовно обійти всі стіни приміщення, розташовуючи магнітну антену в безпосередній близькості до них. Зафіксувати область зростання рівня поля й шляхом переміщення антени горизонталлю та вертикаллю визначити проходження траси прихованої проводки.

Можливість виявлення працюючих диктофонів визначається як рівнем магнітного поля, створюваного їхніми двигунами, так і рівнем магнітного

фону приміщення. Для розв'язку цього завдання зазвичай застосовують спеціалізовані засоби з попередньою ретельною підготовкою приміщення. Тому не завжди може бути досягнуто позитивного результату лише при використанні приладу ST – 031 Піранья, надто на відстані поміж диктофоном та магнітною антеною понад 30 см.

### 3.6 Використання приладу для оцінювання ефективності віброакустичного захисту та звукоізолювання приміщень

Поєднання цих напрямків використання приладу спричинено спільністю джерел виникнення каналів витоку інформації (мовний сигнал в акустичному діапазоні), подібністю прийомів контролю та практичною ідентичністю використання можливостей ST– 031 Піранья.

По-перше, і в тому, і в тому разі при підготовці приміщення слід вимкнути прилади й засоби, що вони утворюють додатковий акустичний фон.

По-друге, в обох випадках слід використовувати тестові, а найкраще калібровані джерела звукового сигналу.

По-третє, у суміжних стосовно перевірюваного приміщеннях має бути забезпечено мінімально можливий рівень акустичного фону.

По-четверте, застосовують практично однакові методи аналізу сигналів (на слух, за осцилограми та спектрограми).

Оцінювання ефективності віброакустичного захисту приміщення зазвичай провадиться в два етапи. На першому етапі захисту, якщо його застосовано, має бути вимкнено і зроблено перевірку власне віброакустичних властивостей поверхонь, які огороджують приміщення. Для цього слід віброакустичний давач прикріплювати в різних місцях перевірюваних поверхонь (стін, дверей, вікон, за можливості підлоги та стелі) із зовнішнього стосовно контрольованого приміщення боку.

Увімкнути джерело тестового звукового сигналу. Воно може розміщуватися або в звичайному місці ведення конфіденційних розмов, або на певній відстані від обстежуваної поверхні (наприклад, як показано на рис. 1.6).

Рівень звуку зазвичай встановлюють відповідної до голосової мови (74 дБ). Для каліброваних джерел звуку відстань L обирають у межах 1,0....2,0 м. Спочатку, на якісному рівні, шляхом прямого прослуховування оцінюються віброакустичні властивості обстежуваних поверхонь, а потім, переходом до режиму SA, кількісно оцінюються амплітуди частотних складових тестового сигналу.

На другому етапі, якщо це передбачено, оцінюється ефективність системи віброакустичного захисту. Для цього на кожній поверхні, як якісно – на слух, так і кількісно – за спектрограмою, визначається співвідношення рівнів тестового сигналу й маскувального сигналу, а також виявляються неприкриті складові спектра. Це є об'єктивною основою корекції амплітудно-частотної характеристики джерел маскувального сигналу.

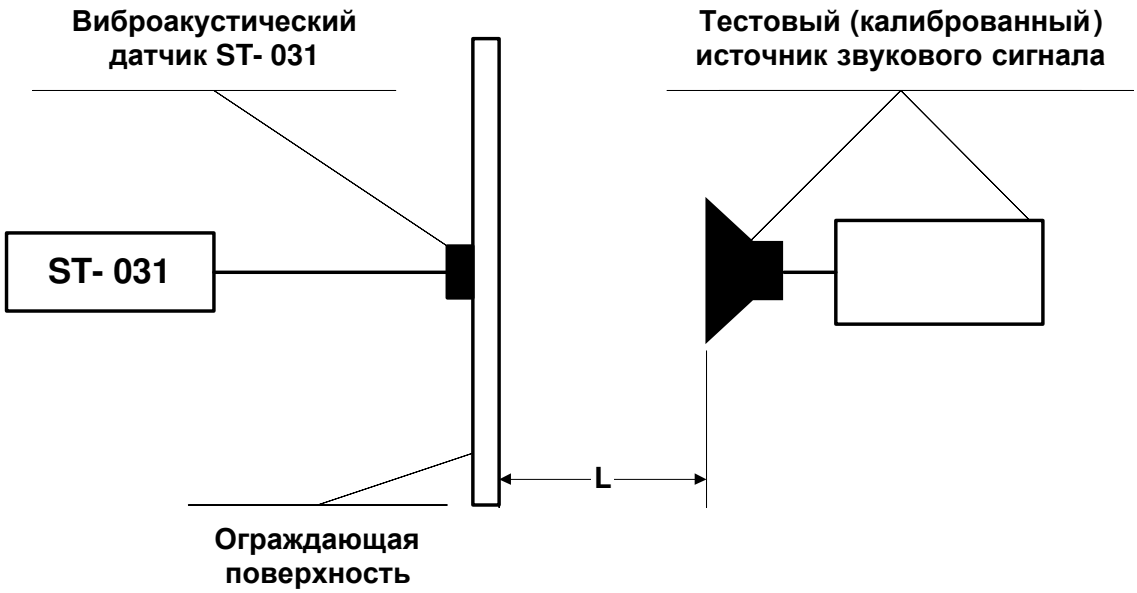



Рисунок 1.6 – Варіант схеми оцінювання віброакустичних властивостей та віброакустичного захисту приміщень

Відповідно до загальноприйнятих правил розбірливість мовних сигналів гарантовано не відновлюється, якщо маскувальний шум (завада) у чотири-п'ять разів (16 дБ) перевищує їхній рівень. Повного вилучення ознак мови досягають за восьмиразового перевищення рівня сигналу завадою, створюваною системою активного захисту.

Оцінювання звукоізолювання приміщень також доцільно проводити в два етапи.

На першому етапі, використовуючи тестове джерело сигналу з рівнем звуку, що він відповідає гучній мові, встановити відповідність поміж цим рівнем та показати приладу ST – 031 Піранья в режимах осцилографа та аналізатора спектра. Для цього розмістити акустичний випромінювач джерела звуку і мікрофон приладу ST – 031 Піранья на певній фіксованій відстані. Зазвичай її обирають у межах 1,0....2,0 м.

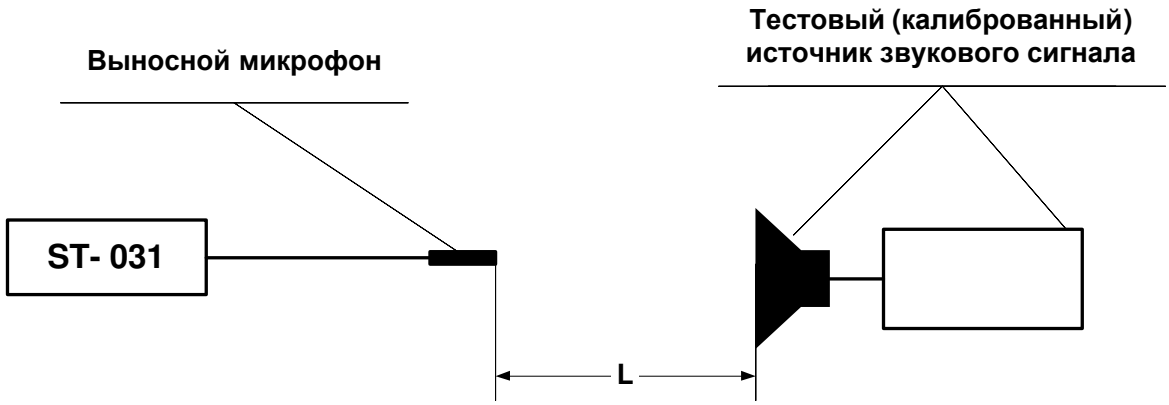



Рисунок 1.7 – Варіант схеми калібрування індикаторів рівня звукового сигнал приладу ST – 031 Піранья

На другому етапі оцінюються звукоізоляційні властивості поверхонь, що вони огороджують приміщення (стін, дверей, вікон, а, якщо можливо, то й підлоги та стелі), ефективність системи активного захисту (зашумлення), а також можливість витоку мовної акустичної інформації через елементи вентиляції, різного роду ніші, наскрізні отвори тощо.

Для оцінювання звукоізоляційних властивостей стін, дверей, підлоги, стелі тестове джерело звуку може бути розташоване або в звичайному місці ведення конфіденційних розмов, або на певній відстані від обстежуваної поверхні. Наприклад, як у варіанті, показаному на рис. 1.8.

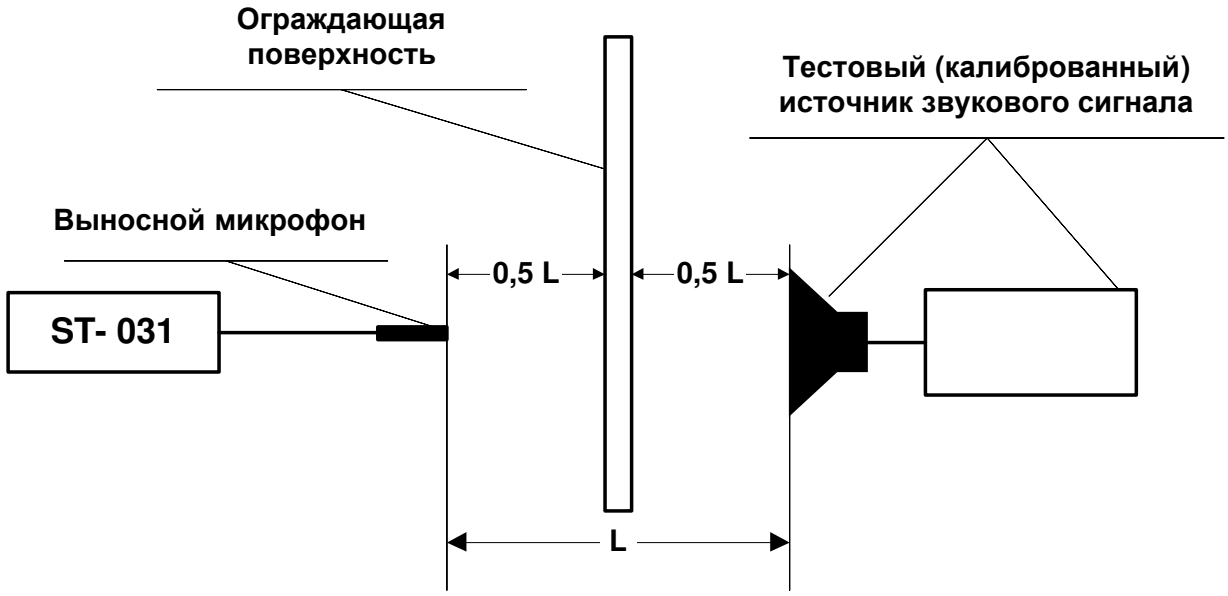



Рисунок 1.8 – Варіант оцінювання звукоізоляції приміщень

Розміщуючи мікрофон у різних місцях суміжних (вище й нижче розташованих) приміщень, якісно – на слух та кількісно – за спектрограмою, визначити дальність перехоплювання мовної інформації з даного приміщення й оцінити зниження рівня звукового сигналу за рахунок властивостей обгороджувальних поверхонь, а також наявність найменш послабленого складового спектра. Останнє дає можливість ухвалити обґрунтоване рішення щодо потреби додаткового захисту, в тому числі й активного, і вибору характеристик засобів захисту.

Оскільки повітропроводи систем вентиляції узвичаєно розглядати як найбільш небезпечні канали витоку мовної (акустичної) інформації, то вони підлягають неодмінній перевірці. Для цього мікрофон приладу ST – 031 Піранья необхідно ввести у вихідний (вхідний) отвір повітропровода кожного з суміжних приміщень, а можливо, й деяких інших. Якісно – на слух – оцінити проходження та розбірливість сигналу від тестового джерела, а за показниками приладу ST – 031 Піранья у режимі осцилографа чи аналізатора спектра – його послаблення при проходженні повітропроводому до місця розміщення мікрофона. При цьому правильна оцінка послаблення може бути отримана лише в тому разі, якщо в наявності є докладна схема системи вентиляції. Її наявність дає можливість враховувати послаблення, внесене різними

елементами конструкції повітропроводів. Так, послаблення мовного сигналу зазвичай становить:

0,15 дБ/м – у прямих металевих повітропроводах;

0,2....0,3 дБ/м – у прямих не металевих повітропроводах;

1,0....3,0 дБ/м – за зміни перетину повітропроводу;

3,0....7,0 дБ/м – на один вигин повітропроводу.

## 8 Зміст протоколу лабораторної роботи

1 Назва лабораторної роботи.

2 Мета проведення роботи.

3 Оцінка результатів пошуку

4 Висновки та рекомендації

## 9 Ключові запитання

1 Основні типи закладних пристроїв.

2 Структурна схема закладного пристрою.

3 Методи виявлення можливих каналів витоку інформації несанкціонованого за допомогою пошукового приладу ST – 031 Піранья.

4 Основне призначення та режими роботи багатофункціонального пошукового приладу ST – 031 Піранья. Можливі канали витоку інформації.

## Лабораторна робота № 2
## Виявлення витоку інформації радіозакладними пристроями, телефонними радіоретрансляторами за допомогою багатофункціонального пошукового приладу ST– 031 „Піранья”.

### 1 Мета роботи

1.1 Вивчення багатофункціонального пошукового приладу ST– 031 „Піранья”;

1.2 Вивчення методів проведення заходів щодо виявлення й локалізування спеціальних технічних засобів таємного добування інформації, виявлення природних та штучно створених каналів витоку інформації.

### 2 Література

2.1 **ST-031 „Піранья”**- Руководство пользователя. Ст.-Петербург, 1999.

2.2 **Хорев А.А.** Технические каналы утечки акустической (речевой) информации. Классификация и характеристика. // Специальная техника, – 1999. – № 3.

2.3 **Василевский И.В.**, **Болдырев А.И.** Одолели „жучки”? Пора проводить „дезинсекцію”.// Конфідент, - 2000. - № 3.

### 3 Основні положення

Сьогодні широкого розповсюдження набуло застосовування підслуховувальної апаратури та закладних пристроїв (ЗП). Для виявлення таємно встановлених радіопередавальних пристроїв використовуються переважно два способи:

– пасивне виявлення (до даного способу належить контроль радіоефіру за допомогою прийомних засобів;

– активне виявлення за допомогою локації. Локація, в свою чергу, може здійснюватися радіолокаційним зондуванням конструкцій на предмет виявлення закладних пристроїв.

Канали витоку інформації в радіочастотному діапазоні можуть бути створені штучно (зумисно), за рахунок спеціальних технічних засобів (радіомікрофони, телефонні радіоретранслятори, несанкціоновано ввімкнені радіостанції, радіомаяки і тощо). Вони можуть виникнути і природно, за рахунок побічних електромагнітних випромінювань (ПЕМВ) технічних засобів опрацьовування інформації (ПЕОМ, телекси, факси і тощо).

Небезпечні радіосигнали може бути створено як внутрішніми, так і зовнішніми джерелами.

Зазвичай, до цілковито внутрішніх небезпечних радіосигналів відносять:

– сигнали радіозакладок (радіомікрофони, телефонні радіотранслятори і тощо);

– сигнали радіомаяків;

– сигнали несанкціоновано ввімкнених у приміщенні радіостанцій та радіотелефонів;

– побічні електромагнітні випромінювання ПЕОМ та інші технічні засоби опрацьовування інформації.

До категорії небезпечних прийнято відносити радіосигнали, джерелами яких можуть бути:

– радіомікрофони з виносним акустичним мікрофоном;

– телефонні радіоретранслятори, установлені на лінії зв'язку за межами приміщення (але поблизу нього);

– радіостетоскопи, встановлені із зовнішнього боку поверхонь, котрі огороджують приміщення;

– винесені передавачі прихованих відеокамер;

– пристрої зовнішнього високочастотного опромінювання.

Як джерела внутрішніх безпечних радіосигналів можуть розглядатися, насамперед, електроприлади, оргтехніка, побутові засоби, а також їхні блоки живлення.

## 3.1 Радіомікрофони

Широкого розповсюдження набули радіомікрофони з параметричною стабілізацією частоти передавача. Основна особливість – великі межі змінювання несучої частоти (до кількох мегагерц) тому для локалізування радіомікрофонів такого типу найбільш доцільне є використання методу акустозав'язки.

Досить широко застосовуються радіомікрофони з кварцовою стабілізацією частоти й вузькосмуговою частотною модуляцією. Тому для пошуку й локалізування такого типу джерел найбільш доцільне є використання амплітудного методу.

У радіомікрофонів, призначених для установлювання в автомобілях та інших транспортних засобах, виокремлюють дві головних особливості – підвищену потужність радіопередавача й більш чистий, без ознак зовнішнього фону, демодульований сигнал (внаслідок звукоізолювальних властивостей корпуса автомобіля).

## 3.2 Телефонні радіо ретранслятори

Незважаючи на різноманіття варіантів виконання телефонних радіоретрансляторів, чітко виокремлюються дві їхні групи за способом підмикання до елементів телефонної лінії – з гальванічним контактом та без нього. При цьому гальванічне підмикання може здійснюватися як послідовно (у розрив одного з проводів телефонної лінії), так і паралельно (водночас до двох проводів телефонної лінії).

Телефонні радіоретранслятори послідовного вмикання відрізняються головною особливістю – з'явленням в ефірі модульованого сигналу лише за піднятої слухавки телефонного апарата. При цьому явно прослуховуються

сигнали АТС («виклик», «зайнято»), клацання при набиранні номера, розмова абонентів після встановлення з'єднання. Локалізування телефонних ретрансляторів даного типу найбільш доцільно здійснювати амплітудним методом. Застосовування методу акустозав'язки може призвести до помилкових висновків щодо наявністі встановленого телефонного радіоретранслятора.

Телефонні радіоретранслятори паралельного ввімкнення можуть мати два різновиди.

Перший різновид передбачає реалізацію лише функції ретранслятора. При цьому в режимі піднятої слухавки на радіочастоті прослуховуються сигнали АТС (виклик, зайнято), клацання при набиранні номера й розмова абонентів. При покладеній слухавки модуляція радіосигналу відсутня, може бути відсутня й сама несуча частота.

В другому різновиді часто сполучують функції телефонного радіоретранслятора та радіомікрофона, він живиться від телефонної лінії й забезпечує контроль акустики приміщення в режимі покладеної слухавки. Такі закладки встановлюються на елементах телефонної лінії в межах контрольованого приміщення. Для їхнього локалізування, за прокладеної слухавки, використовується метод акустозав'язки із застосуванням тестового звукового сигналу. У режимі піднятої слухавки, для локалізування таких закладок, краще застосовувати амплітудний метод.

Слід мати на увазі, що радіоретранслятори гальванічного підмиканння, як правило, не мають власних антен, а використовують замість них провід телефонної лінії.

Телефонні радіоретранслятори негальванічного вмикання (індуктивного знімання інформації) може бути встановлено на будь-якій ділянці телефонної лінії, як правило, поза контрольованим приміщенням на абонентській проводці без порушення ізоляції. Вони формують модульований радіосигнал лише за підняття слухавки телефонного апарата при цьому прослуховуються сигнали АТС (виклик, зайнято), клацання при набиранні номера, розмова абонентів після встановлення з'єднання. Їхнє локалізування здійснюється амплітудним методом в міру обстеження телефонної лінії на всьому її доступному протязі.

### 3.3 Інші джерела потенційно небезпечних радіовипромінювань

Тут варто розглянути, насамперед, радіостетоскопи, приховані відеокамери з радіоканалом передавання інформації, радіозакладки в ПЕОМ, радіомаяки, засоби просторового високочастотного опромінювання, несанкціоновано ввімкнені засоби зв'язку (радіостанції, радіотелефони, телефони з радіоподовжувачами).

Приховані відеокамери з радіоканалом передавання інформації відрізнюються тим, що сигнал, випромінюваний у радіодіапазоні, за структурою є схожий із сигналом каналу яскравості передавачів телевізійного мовлення. Виявлення такого сигналу й локалізування його джерела найбільш

доцільно здійснювати амплітудним методом, доповнюючи цей метод прослуховуванням змінювання тону продетектованого сигналу.

Радіозакладки в ПЕОМ призначено для передавання зображення монітора та цифрових сигналів системного блока й інших елементів фізичної архітектури комп'ютера. Основна їхня особливість полягає в тім, що сигнал, котрий передає зображення монітора, за структурою схожий на сигнал передавача прихованої відеокамери, а в інших випадках містить всі ознаки цифрового передавання. За основу для їхнього виявлення й локалізування слугує амплітудний метод, що він доповнюється аналізом зображень сигналів.

Радіомаяки відрізнюються тим, що їхнє радіовипромінювання не має модуляції акустичним фоном приміщення (об'єкта), є неперервним або чітко вираженим періодичним. Можлива є модуляція тоном. Їхнє виявлення може здійснюватися амплітудним методом у сполученні з прослуховуванням сигналу, а локалізовуваня – лише амплітудним методом.

Засоби просторового високочастотного опромінювання є зовнішніми й використовуються для здобуття інформації з приміщень шляхом орієнтації на нього (переважно через віконні прорізи) потужного гостро спрямованого променя електромагнітного випромінювання високої частоти і приймання перевипроміненого, вже промодульованого сигналу, на частотах вищих гармонік. Основні особливості, що вони забезпечують можливість їх (засобів) виявлення й локалізування полягають у тім, що зондувальний сигнал є стабільним за частотою, його модуляція відсутня, рівень нерівномірний (більш високий у районі вікон, істотно більш низький в коридорі та інших приміщеннях). Окрім того, перевипромінений сигнал за частотою відповідає вищим гармонікам зондувального сигналу і має модуляцію акустичним фоном приміщення. Тому виявлення таких засобів здійснюється амплітудним методом у сполученні з прослуховуванням сигналу, а локалізування напрямку опромінення – лише амплітудним методом.

## 4 Домашнє завдання

4.1 Вивчити можливі канали несанкціонованого витоку інформації;

4.2 Вивчити типи закладних пристроїв;

4.3 Вивчити методи пошуку закладних пристроїв несанкціонованого знімання інформації.

## 5 Контрольні запитання

5.1 Основні типи закладних пристроїв.

5.2 Структурна схема закладного пристрою.

5.4 Основне призначення та режими роботи багатофункціонального пошукового приладу ST – 031 „Піранья”. Можливі канали витоку інформації.

5.3 Методи виявлення можливих каналів витоку інформації несанкціонованого за допомогою пошукового приладу ST – 031 „Піранья”.

## 6 Лабораторне завдання

6.1 Вивчення пошукового приладу ST– 031 „Піранья” та особливостей роботи в різних режимах пошуку.

6.2 Практичне виявлення можливих каналів несанкціонованого витоку інформації за допомогою пошукового приладу ST– 031 „Піранья”.

6.3 Складання протоколу вимірювань.

## 7 Опис лабораторного макету - багатофункціонального пошукового приладу ST– 031 „Піранья”

### 7.1 Призначення та основні можливості

Багатофункціональний пошуковий прилад ST – 031 „Піранья” призначено для проведення заходів щодо виявлення та локалізування спеціальних технічних засобів таємного здобування інформації. Виявлення факту роботи та локалізування місця розташування радіо-випромінювальних спеціальних технічних засобів, які створюють потенційно небезпечні, з огляду витоку інформації, радіовипромінювання.

### 7.2 Режими роботи приладу

Розв’язок контрольно-пошукових завдань забезпечується певною сукупністю режимів роботи приладу.

Схемотехнічна та програмна база дозволяє використання приладу в таких режимах роботи:

- режимі високочастотного детектора-частотоміра;
- режимі сканувального анализатора провідних ліній;
- режимі детектора інфрачервоних випромінювань;
- режимі детектора низькочастотних магнітних полів;
- режимі акустичного приймача.
- режимі віброакустичного приймача;

### 7.3 Порядок управління приладом у режимі високочастотного детектора-частотоміра

Підімкнути телескопічну антену, використовуючи перехідник, або високочастотну антену до розніму RF ANT. Увімкнути живлення приладу.

Встановлення «нульового» порога детектора здійснюється автоматично, при вмиканні. У разі потреби, натисканням кнопок « ◀ » чи « ▶ » встановити вручну поріг детектора, керуючись показаннями додаткової шкали «min---|---max». В разі потреби, натисканням кнопки «▲» повернутися до режиму автоматичного встановлення порога.

Візуально, за кількістю цілковито пофарбованих елементів індикаторів рівня сигналу та «на слух», за частістю клацань у вмонтованому гучномовці або головних телефонах, оцінити рівень прийнятого сигналу.

За потреби натисканням кнопки SET встановити потрібні межі динамічного діапазону: (– 8...16) дБ; (– 8...32) дБ; (– 8...48) дБ.

Натиснути кнопку RUN/STOP і зупинити, за потреби, динамічні вимірювання рівня та частоти радіосигналу. Повторним натисканням цієї кнопки відновити динамічні вимірювання.

Натиснути кнопку ENTER (для переведення звукової індикації до режим AUD), прослухати наявність та зміст потенційно небезпечних модульованих радіовипромінювань.

Натисканнями кнопок «+» та «–» встановити необхідну гучність звукового сигналу (тонального чи демодульованого), виведеного на вмонтований гучномовець або на головні телефони.

Натиснути кнопку OSC і перейти, за потреби, до осцилографічного контролю параметрів сигналу.

Натиснути кнопку SA і перейти, за потреби, до аналізу спектра демодульованого сигналу.

У разі збивання у роботі натиснути кнопку RESET, та здійснити перезапускання приладу.

## 7.4 Порядок керування приладом у режимі скандувального аналізатора провідних ліній

Підімкнути мережний адаптер до розніму PROBES, а його щупи – до провідної лінії (або до лінії електромережі з напругою до 600 В).

Увімкнути живлення приладу.

Дочекатися дво–, трикратного «пробігу» підрядковим маркером діапазону сканування в автоматично встановлених межах 0,0....10,45 МГц.

Встановити необхідні, найбільш раціональні, межі сканування частотного діапазону.

Натиснути кнопку SET, потім кнопку «4». Натисканням кнопок з цифровим маркуванням набрати число, відповідне нижній межі діапазону.

Натисканням кнопки ENTER підтвердити завершення встановлення значення нижньої межі.

Натисканням кнопок з цифровим маркуванням набрати число, відповідне верхній межі діапазону.

Натисканням кнопки ENTER підтвердити встановлення верхньої межі діапазону.

За помилки, в перебігу набирання значень частот нижньої чи верхньої межі діапазону сканування натиснути кнопку « ◂ » й вилучити набране число.

Натиснути кнопку « ◂ » чи « ▸ » й обрати потрібні напрямки та швидкість сканування.

Натиснути кнопку SET, потім кнопку «3», до з’явлення на екрані в четвертому рядку напису: 3 - > ↑↓ THRESHOLD level.

Натисканням кнопки ENTER повернути на екран зображення панорами.

Натисканням кнопок «▲» та «▼» встановити найбільш зручну межу індикації вимірювача рівня сигналу (напис під горизонтальною віссю THRESHOLD level = XX%).

Натиснути кнопку RUN/STOP й зупинити в необхідному місці частотної осі автосканування. Натисканням кнопок «◀» чи «▶» провести точне ручне налаштовування на потрібну частоту. Прослухати демодульований сигнал.

Натисканням кнопки ENTER (AM/FM) обрати вид демодуляції (на слух, за якістю його відтворення).

Натиснути кнопку RUN/STOP і повернутися до автосканування.

Увімкнути систему автоматичної зупинки сканування на найбільш окреслених (за амплітудою) частотних складових панорами.

Натиснути кнопку SET, потім кнопкою «3» встановити в четвертому рядку меню напис 3 - > ↑↓ SQUELCH level.

Натиснути кнопку ENTER.

За допомогою кнопок «▲» та «▼» обрати бажаний рівень автоматичної зупинки автосканування (за положенням короткої горизонтальної риски в правій частині екрана). Після зупинки сканування кнопками «◀» та «▶» зробити уточнення налаштування, за ознакою якості демодульованого сигналу. Для продовження сканування натиснути кнопку RUN/STOP.

Увімкнути (за потреби) режим обчислення спектрів.

Натиснути кнопку SET, потім кнопку «2» та встановити напис «2 - > Difference ON D2-1».

Для початку процедури обчислення спектрів натиснути кнопку ENTER.

Вийти з режиму обчислення спектрів.

Натиснути кнопку SET, потім кнопкою «2» установити напис «Difference OFF».

Натиснути кнопку ENTER.

Записати, за потреби, зображення панорами в енергонезалежну пам'ять.

Натиснути кнопку SAVE, потім кнопку ENTER.

Викликати з пам'яті необхідне зображення панорами.

Натиснути кнопку LOAD.

Натисканням кнопки RUN/STOP повернути на екран панораму, яка динамічно відбивається.

Стерти (вилучити) з пам'яті зображення певної панорами.

Натиснути кнопку LOAD, потім SAVE та ENTER.

Натисканням кнопки OSC перейти, за потреби, до осцилографічного контролю параметрів сигналу.

Натисканням кнопки SA перейти, за потреби, до аналізу спектра сигналу.

У разі збивання у роботі натиснути кнопку RESET і здійснити перезапускання приладу.

# 8 Рекомендації з проведення контрольно-пошукових робіт з використанням приладу ST– 031 „Піранья”

## 8.1 Основні правила та особливості проведення контрольно-пошукових робіт

Початковий этап підготовки проведення контрольно-пошукових робіт полягає в створенні умов, за яких забезпечується мінімально можливий рівень фону електричного поля. Це досягається вимкненням потенційних джерел підвищення фону, якими є засоби оргтехніки, ПЕОМ, перетворювачі та блоки живлення, базові станції безпроводових телефонів, люмінесцентні освітлювальні лампи й інші електронні пристрої та електроприлади. Доцільно також зачинити вікна і двері, спустити (задвинути) штори чи жалюзі.

Надто слід звернути увагу на те, щоби було вимкнено радіотелефони й інші радіопередавальні засоби, а також засоби активного радіотехнічного захисту. Не припускається робота приладу ST – 031 „Піранья” з нелінійними локаторами.

Для створення акустичного фону й активізування радіозакладок з акустопуском слід підготувати та розмістити в контрольованому приміщенні тестове джерело звуку. Таким джерелом може бути магнітофон з добре відомою музичною чи мовною фонограмою. Не рекомендується використовувати для таких цілей радіоприймач чи телевізор, тому що створюваний ними звуковий сигнал, перевипромінюваний радіозакладкою, може збігтися з радіосигналом власної мовної станції. Підготовка самого приладу ST – 031 „Піранья”, після перевірки його працездатності в даному режимі, полягає у встановленні нульового порога детектора, що, фактично, визначає умови для успішного проведення робіт. Заниження порога обов'язково призведе до частих помилкових спрацьовувань індикації, а його завищення – до ймовірного пропускання сигналу радіозакладки. Тому при встановленні нульового порога слід неодмінно дотримуватися кількох найпростіших правил.

**Не можна** провадити встановлення порога в перевіюваному приміщенні, тому що при функціонуванні в ньому вже розміщеної радіозакладки, рівень її радіовипромінювання буде визначено приладом як нульовий.

Під час налаштовування порога **неприпустиме** є використання радіостанцій, радіотелефонів та інших радіовипромінювальних засобів.

**Не слід наближати** антену приладу до ввімкнених ПЕОМ та інших засобів оргтехніки, як джерел ПЕОМ, в діапазоні роботи приладу.

**Не припускати** контакту антени приладу з металевими предметами та проводами, які є джерелами перевипромінюваних високочастотних сигналів.

Якщо об'єктом перевірки є автомобіль чи інший транспортний засіб, то, забезпечивши правильний вибір місця робіт, налаштовування нульового порога слід провадити не ближче за 10....20 м від нього.

Після встановлення нульового порога прилад переміщують у контрольоване приміщення (до контрольованого об'єкта) БЕЗ ВИМИКАННЯ

ЖИВЛЕННЯ, тому кожне наступне його ввімкнення призводить до автоматичного встановлення порога вже стосовно нових умов електромагнітної обстановки.

Пошук автономних радіомікрофонів та телефонних радіоретрансляторів доцільно здійснювати, вимкнувши з розеток електромережі шнури живлення всіх санкціонованих споживачів та освітлювальні прилади з лампами розжарювання.

Якщо не накладаються обмеження на приховання проведення робіт, то найоптимальний ефект дає поєднання амплітудного методу й методу акустозав'язки. При проведенні прихованого пошуку необхідно орієнтуватися на амплітудний метод із прослуховуванням детектованих сигналів через головні телефони. Особлива увага звертається на радіовипромінювання в діапазоні 60....640 МГц, найбільш типовому для використання радіомікрофонами й телефонними радіоретрансляторами.

Пошук здійснюється шляхом планомірного обходу приміщення (об'єкта) з рухом уздовж стін і обстеженням меблів та інших розташованих у ньому предметів. Через доволі велику чутливість високочастотної антени пошук доцільно починати із застосуванням телескопічної антени. При обході антену слід орієнтувати в різних площинах, роблячи плавні, повільні повороти основного блока й домагаючись максимального рівня сигналу. Антену приладу доцільно тримати на відстані не більш 20....25 см від обстежуваних поверхонь та предметів.

При наближенні антени приладу ST – 031 „Піранья" до місця розміщення радіозакладки напруженість електромагнітного поля зростає, відповідно підвищується й рівень сигналу на його вході. З перевищенням рівня сигналу встановленого нульового порога, залежно від виду сигналу, збільшується кількість пофарбованих секторів одного з рядків індикатора рівня й, розпочинаючи з четвертого (відлік від нульової оцінки), зростає частість клацань звукової сигналізації в режимі TONE, а за ввімкнення режиму AUD та динаміка гучномовця виникає акустозав'язка.

У разі перебування джерела з частотно модульованим сигналом збільшуватиметься кількість пофарбованих секторів верхнього індикатора рівня сигналу. При достатньому наближенні до джерела радіочастотомір здійснює захоплення частоти й зазначає в останньому рядку екрана її значення за результатами декількох вимірювань. Шляхом зменшення гучності кнопкою «– », зміни межі динамічного діапазону кнопкою SET, збільшення вручну порога спрацьовування детектора, постійного спостереження за показами частотоміра звужується зона обстеження й тим самим злокалізується місце встановлення радіозакладки з похибкою в межах 10....15 см. Додаткові можливості, насамперед щодо класифікування радіовипромінювань, надає періодичне ввімкнення режиму AUD та прослуховування демодульованого сигналу.

Однак слід пам'ятати, що ефект акустозав'язки й виразне прослуховування демодульованого сигналу спостерігаються не завжди, наприклад, якщо закладки мають маскований радіоканал, тому в підґрунті їхнього пошуку лежить використання амплітудного методу в чистому вигляді.

У разі застосування радіозакладки з цифровими методами модулювання індикація підвищення рівня буде відбиватися на нижньому індикаторі. Індикація частоти прийманого сигналу в даному разі буде випадковою.

У разі застосування в якості радіозакладки телефонів стандарту DECT чи GSM, окрім індикації підвищення рівня сигналу в нижньому рядку, на індикаторі з'явиться напис DECT чи GSM.

Аналогічно до пошуку радіомікрофонів здійснюється пошук телефонних радіоретрансляторів. При цьому, для їхньої активізації, необхідно зняти трубки всіх телефонних апаратів. Власне пошук провадиться в два етапи.

Спочатку на наявність закладних пристроїв перевіряються власне самі телефонні апарати. Встановлений в апараті радіоретранслятор виявляється у такий самий спосіб, як і радіомікрофон. При наближенні антени приладу до такого телефонного апарата реагують засоби звукової (у режимі TONE) індикації, індикатор рівня сигналу та частотомір. При перемиканні до режиму AUD у динаміку чи в головних телефонах прослуховується або неперервний, або переривчастий тональний сигнал телефонної станції. У низці випадків при наближенні мікрофона телефонної слухавки до динаміка приладу ST – 031 Піранья може виникнути ефект акустозав’язки. Не рекомендується перевіряти телефонні апарати в режимі гучномовного зв'язку (якщо його передбачено), тому що в цьому разі може виникнути помилкова акустозав’язка поміж мікрофоном та динаміком самого апарата.

Пошук закамуфльованих радіомікрофонів, що вони живляться від електромережі, й локалізування місця їхнього встановлення здійснюються тими ж самими методами, що їх було схарактеризовано вище. Для їхньої активізації необхідно ввімкнути тестове джерело звуку. По черзі ввімкнути наявні освітлювальні прилади з лампами розжарювання й підімкнути до розеток електромережі шнури живлення санкціонованих споживачів. Послідовно провести обстеження кожного із знову підімкнути засобів.

Пошук радіостетоскопів має певні особливості, зумовлені способами їхнього застосовування (встановлення поза контрольованим приміщенням). Тому для виявлення сигналів радіо стетоскопів слід обстежувати всі реально приступні зовнішні поверхні конструкцій, які огороджують приміщення. Оскільки середовищем поширення віброакустичних коливань можуть бути труби опалення та водопостачання, то перевірці підлягають і ці комунікації.

У переважній більшості радіостетоскопи використовують відкритий радіоканал. Це дає можливість аналізування прийнятого сигналу на слух в режимі AUD. При перевірці трубопровідних комунікацій необхідно виконувати такі ж самі рекомендації, але не припускати контакту антени з металевими поверхнями.

Локалізування радіостетоскопів здійснюється амплітудним методом у суміжних приміщеннях, що доповнюється, потреби, використанням режимів OSC і SA.

Пошук прихованих відеокамер з радіоканалом передавання зображення (часто і звуку) пов’язано з певними труднощами, котрі визначаються подібністю сигналу відеопередавача із сигналом яскравості передавачів

телевізійного мовлення й роботою значної кількості цих пристроїв у діапазоні телестанцій (від 60 МГц до 500 МГц). Тому в перебігу проведення робіт при виявленні такого сигналу першим є завданням його розпізнавання за критерієм зовнішній–внутрішній. Для розпізнавання необхідно закрити вікна шторами чи жалюзями, залишивши ввімкненим внутрішнє освітлення. Зробити кілька разів вмикання й вимикання штучного освітлення. При ввімкненому режимі AUD мають прослуховуватися виразні зміни тону продетектованого сигналу. Для підвищення надійності розпізнавання ввімкнути режим OSC й переконатися в зміненні структури сигналу за осцилограмою при вмиканні й вимиканні освітлення. Вид осцилограми радіосигналу передавання відеоінформації за різних значень параметрів горизонтальної розгортки подано на рисунках 1.9 та 1.10.

Якщо результати зазначеної перевірки є позитивні, то сигнал упевнено можна віднести до категорії внутрішніх, створюваних передавачем відеокамери, тому що зміна освітленості приміщення на параметри сигналу телевізійного мовлення не впливає. Принципово передавачі відеокамер можуть працювати на частотах до 2300 МГц.

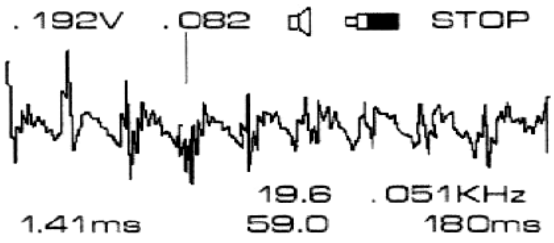



Рисунок 1.9 – Радіосигнал передавання відеоінформації, період розгортки 180 мс

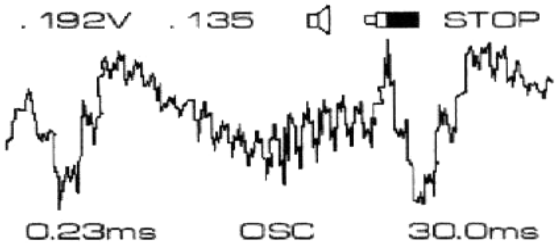



Рисунок 1.10 – Радіосигнал передавання відеоінформації, період розгортки 30 мс

Виявлення сигналу (схожого на сигнал яскравості) на частотах поза діапазоном телевізійного мовлення практично однозначно свідчить про роботу передавача прихованої відеокамери. Локалізування таких засобів здійснюється амплітудним методом.

Стосовно просторового високочастотного опромінювання, головним є завдання виявлення факту створення цього штучного каналу знімання інформації. Зазвичай таке завдання розв'язується у два етапи. На першому етапі виявляється факт опромінення приміщення високочастотним сигналом. На другому етапі відстежується відгук на зондувальний високочастотний сигнал. При цьому слід орієнтуватися на такі моменти. Гостроспрямований промінь електромагнітної енергії може бути сформовано лише на надто високих частотах (800....900 МГц і вище). Особливості поширення радіохвиль цього діапазону (необхідність прямої видимості поміж джерелом випромінювання й опромінюваними предметами) визначають як основні шляхи їхнього проникнення в контрольоване приміщення, насамперед віконні прорізи. Перевипромінюваними об'єктами можуть бути звичайні для даного приміщення технічні засоби, яким є притаманний так званий мікрофонний ефект (паразитні акустоелектричні перетворювачі). До них зазвичай відносять

динаміки побутових гучномовців, акустичні системи навіть вимкненої аудіоапаратури, телефонні апарати з електричним дзвінком й т. п. Перевипромінений сигнал на частотах вищих (найчастіше другої чи третьої) гармонік локалізується в безпосередній близькості від опромінюваних предметів і має модулювання акустичним фоном приміщення.

Виходячи з викладеного, може бути використано такий порядок роботи.

Для виявлення факту високочастотного опромінювання слід обстежувати потенційно небезпечні віконні прорізи. Для цього піднести антену до внутрішнього скла на відстань 5....10 см, зафіксувати рівень та частоту найбільш потужного сигналу. Увімкнути режим AUD і на слух визначити наявність та особливості демодульованого сигналу. За графічним індикатором оцінити стабільність частоти випромінювання. Перейти в кожне з сусідніх приміщень (орієнтованих вікнами в той самий бік) і повторити перевірку в районі кожного з його віконних прорізів.

Для виявлення джерел перевипромінювання необхідно ретельно обстежувати кожний, з потенційно небезпечних предметів, розміщуючи антену приладу в безпосередній близькості до нього. Підставою для ухвалення остаточного рішення щодо опромінювання та наявності у приміщенні перевипромінювальних предметів є покази індикатора рівня приладу ST – 031 Піранья та його частотоміра, а також результати прослуховування в режимі AUD. При цьому запереважні ознаки зазвичай розглядають фіксацію номіналу частоти, кратну максимуму третьої гармоніки опромінювального сигналу та ідентифікацію звукового сигналу в режимі AUD з акустичним фоном приміщення.

Перевірку ПЕОМ на наявність у них радіозакладок, доцільно провадити в останню чергу. Це зумовлено тим, що у ввімкненому стані вони створюють доволі інтенсивні побічні радіовипромінювання в діапазоні до 1000 МГц і вище, тобто є джерелами підвищення електромагнітного фону, що може маскувати випромінювання раніше розглянутих радіозакладних пристроїв. При цьому слід мати на увазі, що радіозакладки можуть передавати як сигнали, що відповідають зображенню на екрані монітора, так і сигнали, котрі несуть цифрову інформацію, опрацьовувану елементами системного блоку. І ті й ті сигнали мають вельми виразні зовнішні ознаки, що вони виявляються на їхніх осцилограмах у режимі OSC. Перші за структурою схожі із сигналом передавачів відеокамер, а другі являють собою чітко позначену імпульсну послідовність.

Для виявлення сигналів радіозакладок слід переміщувати антену приладу ST – 031 Піранья навколо монітора й системного блока, фіксуючи рівень прийнятого сигналу й покази частотоміра. Наявності в ПЕОМ радіозакладки та її роботі на передавання, відповідають різке зростання рівня прийнятого сигналу й відносно висока стабільність частоти. У цьому разі слід зафіксувати положення антени, якому відповідає максимальний рівень, увімкнути режим OSC й візуально оцінити вид сигналу. Для запобігання помилковим висновкам, порівняти його з осцилограмою побічних електромагнітних випромінювань монітора ПЕОМ, вигляд якої подано на рисунку 1.11.

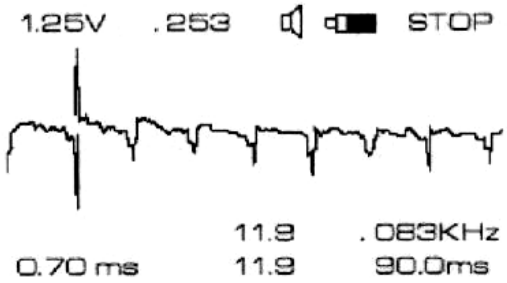



Рисунок 1.11 – ПЕМВ
монітора ПЕОМ

Визначення місця встановлення радіозакладки здійснюється, окрім того, й шляхом послідовного вмикання та вимикання монітора й системного блока.

## 8.2 Використання приладу для виявлення каналів витоку інформації провідними лініями різного призначення

Тут розглядаються прийоми виявлення штучно створених каналів витоку інформації провідними лініями, в основу яких покладено використання спеціальних технічних засобів. Головними видами провідних ліній, для аналізу яких призначено прилад ST – 031 „Піранья", є лінії електромережі (високопотенційні лінії), а також абонентські телефонні лінії та лінії систем пожежної й охоронної сигналізації (низькопотенційні лінії).

Взагалі прийоми й методи, застосовувані для перевірки провідних ліній зазначених видів, є однакові. Підімкнення до них здійснюється з використанням єдиного, універсального адаптера. Аналізування методом сканування підлягає загальний діапазон від 0 до 15 МГц. Висновок результатів сканування надається у вигляді зображення панорами з однотипним поданням (відбиттям) вимірюваних параметрів. Функції органів керування приладом є одинакові (поза залежністю від виду перевірюваної лінії).

Загальні (для всіх ліній) положення методики роботи полягають у такому.

Проведення підготовки контрольованого приміщення полягає в перевірці відповідності кількості та призначення реально існуючих в ньому провідних ліній раніше виготовленим (поданим) схемам їхнього прокладання.

Підготовка самого приладу ST – 031 „Піранья" полягає лише у виборі найбільш зручних наконечників до щупів стосовно типу й особливостей наявних провідних ліній.

Для забезпечення гарантованої надійності щодо не пропускання сигналів закладок за частотою верхню межу діапазону сканування в приладі ST – 031 „Піранья" визначено на рівні 15 МГц.

Рекомендується такий порядок дій оператора:

1 Увімкнути прилад.

2 Дочекатися початку сканування в діапазоні до 10....450 МГц і після завершення двох- трьох циклів встановити верхню межу діапазону на рівні 15МГц. Уважно вивчивши найбільш характерні особливості зображення

панорами, визначити наявність частотних складових, які перевищують рівень загального фону.

3 За необхідності розбити діапазон на окремі інтервали й просканувати їх докладно, зупиняючись насамперед на частотах найбільш інтенсивних складових.

4 Межі інтервалів задаються послідовним натисканням кнопок SET, «4», кнопок з цифровим маркіруванням та кнопки ENTER (або альтернативний варіант із завданням центральної частоти та ширини смуги).

5 Встановити нижній поріг індикації рівня сигналу порядку 10…15 %. Для цього натиснути кнопку SET, кнопкою «3» вивести напис 3 - ↑↓ THRESHOLD level, натиснути кнопку ENTER і кнопками «▲» та «▼» домогтися встановлення цього порога індикації. В подальшому, подальшому залежно від характеру зображення панорами, обрати найбільш зручний для аналізу рівень порога.

6 Запускання й зупинка сканування здійснюються натисканням кнопки RUN/STOP.

7 Після проходу декількох циклів сканування можна обґрунтовано встановити поріг «автостопа» для чого натиснути кнопку SET, обрати кнопкою «3» режим SQUELCH LEVEL, підтвердити вибір кнопкою ENTER і, маніпулюючи кнопками «▲» та «▼», поставити курсор на необхідний рівень. Після зупинки на частоті того чи іншого сигналу слід зробити точне налаштовування кнопками «◀» та «▶», водночас аналізуючи сигнал «на слух» почерговим ввімкненням детекторів AM та FM кнопкою ENTER. Для аналізу слабких сигналів можна обрати кнопками SET «5» та ENTER більш зручний амплітудний діапазон (0,1…1 мВ).

8 За потреби доповнити можливості аналізу сигналів у провідних лініях перемиканням приладу в режими OSC та SA, тому що зображення осцилограм та спектрограм сигналів, виведених на екран дисплея, дають більш докладну характеристику параметрів. У цьому можна переконатися порівнянням зображень панорами й осцилограми того самого цифрового сигналу передавання мовної інформації (див. рис.1.12 та рис.1.13).

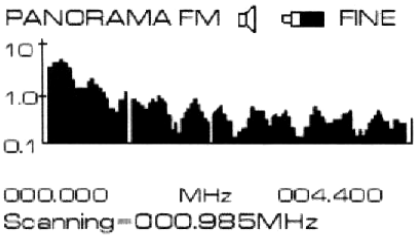



Рисунок 1.12 – Панорама цифрового сигналу передавання мовної інформації в провідній лінії

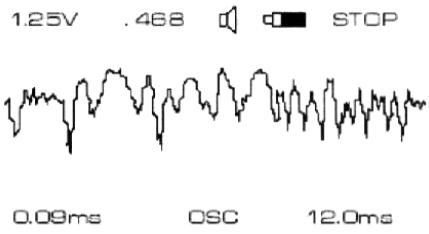



Рисунок 1.13 – Осцилограма цифрового сигналу передавання мовної інформації в провідній лінії (цей самий сигнал)

Якщо приміщення включено до плану регулярних періодичних перевірок, то доцільно зберегти в енергонезалежній пам'яті панораму (осцилограму, спектрограму) необхідних частотних інтервалів. Для збереження натиснути кнопки SAVE та ENTER. Для виклику з пам'яті потрібної панорами

(осцилограми, спектрограми) натискати кнопку LOAD. Разом з тим необхідно враховувати й певні особливості, зумовлені специфікою ліній кожного виду.

Перевірку наявності в електромережі спеціальних технічних засобів, які приймають акустичні сигнали з приміщення, що вони живляться від мережі й передають інформацію на високій частоті її проводами, доцільно розпочинати з мережних розеток. Для зменшення рівня фону слід вимкнути (з механічним від'єднанням від розеток) всі електроприлади й апаратуру, розміщену в контрольованому приміщенні.

Підімкнути прилад до мережі, використовуючи для цього кожну з розеток (як правило, енергозабезпечення приміщення здійснюється від однієї фази або, принаймні, від одного розподільного щитка).

Провести аналіз зображення панорами.

Якщо виявлено сигнал, що він містить ознаки модуляції акустикою приміщення, то для локалізування його джерела може бути використано метод акустозав'язки за почергового підмикання до всіх розеток у перевірюваному приміщенні.

Аналогічну перевірку провести на елементах ліній, котрі живлять електроосвітлювальні прилади.

Після перевірки силових ліній та ліній, що вони живлять освітлювальні прилади, необхідно перевірити трійники, подовжувачі та інші електроспоживальні засоби шляхом їхнього почергового підмикання до електромережі.

Перевірка провідних ліній систем пожежної й охоронної сигналізації, а також ліній невідомого призначення, є аналогічно до перевірки ліній електромережі, тому що аналогічні є власне самі технічні засоби, використовувані на цих комунікаціях.

При перевірці абонентських телефонних ліній, окрім пошуку описаних вище спеціальних технічних засобів, слід, розв'язувати завдання виявлення факту використання лінії для знімання акустичної інформації з приміщення за рахунок лінійного високочастотного нав'язування. Ознакою факту лінійного високочастотного нав'язування є наявність в лінії немодульованого стабільного зондувального сигналу на частотах не нижче за 150 кГц. При цьому порядок підмикання приладу та процедура аналізу стосовно перевірки ліній електромережі не відрізняються від викладеного.

## 9 Зміст протоколу

9.1 Структурна схема закладного пристрою.

9.2 Структурна схема пошукового процесу;

9.3 Опис проведення процесу пошуку закладних пристроїв в різних режимах роботи .

9.4 Оцінка результатів пошуку (висновки).

## Лабораторна робота № 3
## Виявлення витоку інформації за рахунок інфрачервоних випромінювань, низькочастотними магнітними полями за допомогою багатофункціонального пошукового приладу ST– 031 „Піранья”

### 1 Мета роботи

1.1 Вивчення багатофункціонального пошукового приладу ST– 031 „Піранья”;

1.2 Вивчення методів проведення заходів щодо виявлення й локалізування спеціальних технічних засобів таємного добування інформації за рахунок інфрачервоних випромінювань та низькочастотними магнітними полями.

### 2 Література

2.1 **ST-031 „Піранья”**- Руководство пользователя. Ст.-Петербург, 1999.

2.2 **Хорев А.А.** Технические каналы утечки акустической (речевой) информации. Классификация и характеристика. // Специальная техника, – 1999. – № 3.

2.3 **Василевский И.В.**, **Болдырев А.И.** Одолели „жучки”? Пора проводить „дезинсекцію”.// Конфідент, - 2000. - № 3.

### 3 Основні положення

Сьогодні широкого розповсюдження набуло застосовування підслуховувальної апаратури та закладних пристроїв (ЗП). Для виявлення таємно встановлених технічних засобів для знімання інформації, котрі мають у своєму складі напівпровідникові компоненти, й перебувають як у ввімкненому, так і у вимкненому стані, використовуються переважно два способи:

– пасивне виявлення (до даного способу належить контроль радіоефіру за допомогою прийомних засобів;

– активне виявлення за допомогою локації. Локація, в свою чергу, може здійснюватися радіолокаційним зондуванням конструкцій на предмет виявлення закладних пристроїв.

Небезпечні радіосигнали може бути створено як внутрішніми, так і зовнішніми джерелами.

Зазвичай, до цілковито внутрішніх небезпечних радіосигналів відносять:

– сигнали радіозакладок (радіомікрофони, телефонні радіотранслятори і тощо);

– сигнали радіомаяків;

– сигнали несанкціоновано ввімкнених у приміщенні радіостанцій та радіотелефонів;

– побічні електромагнітні випромінювання ПЕОМ та інші технічні засоби опрацьовування інформації.

До категорії небезпечних, у сполученні внутрішні — зовнішні, прийнято відносити радіосигнали, джерелами яких можуть бути:

– радіомікрофони з виносним акустичним мікрофоном;

– телефонні радіоретранслятори, установлені на лінії зв'язку за межами приміщення (але поблизу нього);

– радіостетоскопи, встановлені із зовнішнього боку поверхонь, котрі огороджують приміщення;

– винесені передавачі прихованих відеокамер;

– пристрої зовнішнього високочастотного опромінювання.

Чисто зовнішні джерела радіовипромінювання, як правило, прямої небезпеки, з погляду витоку інформації, не становлять. До їхнього числа можна віднести широкомовленєві радіостанції, станції телевізійного мовлення, засоби радіозв'язку і тощо.

Як джерела внутрішніх безпечних радіосигналів можуть розглядатися, насамперед, електроприлади, оргтехніка, побутові засоби, а також їхні блоки живлення.

## 4 Домашнє завдання

4.1 Вивчити можливі канали несанкціонованого витоку інформації;

4.2 Вивчити типи закладних пристроїв, які працюють з випромінюванням в інфрачервоному діапазоні;

4.3 Вивчити методи пошуку закладних пристроїв несанкціонованого знімання інформації.

## 5 Контрольні запитання

5.1 Основні типи закладних пристроїв.

5.2 Структурна схема закладного пристрою.

5.4 Основне призначення та режими роботи багатофункціонального пошукового приладу ST – 031 „Піранья”. Можливі канали витоку інформації.

5.3 Методи виявлення можливих каналів витоку інформації несанкціонованого за допомогою пошукового приладу ST – 031 „Піранья”.

## 6 Лабораторне завдання

6.1 Вивчення пошукового приладу ST– 031 „Піранья” та особливостей роботи в різних режимах пошуку.

6.2 Практичне використання методів виявлення можливих каналів несанкціонованого витоку інформації за допомогою пошукового приладу ST– 031 „Піранья”.

6.3 Складання протоколу вимірювань.

## 7 Опис лабораторного макету - багатофункціонального пошукового приладу ST– 031 „Піранья”

### 7.1 Призначення та основні можливості приладу ST – 031 „Піранья”.

Багатофункціональний пошуковий прилад ST – 031 „Піранья” призначено для проведення заходів щодо виявлення та локалізування спеціальних технічних засобів таємного здобування інформації. З використанням приладу ST – 031 „Піранья” можливе розв’язування таких контрольно-пошукових завдань:

1 Виявлення й локалізування місця розташування спеціальних технічних засобів, які працюють з випромінюванням в інфрачервоному діапазоні. До таких засобів, у першу чергу, відносять:

- закладні пристрої здобування акустичної інформації з приміщень, з її наступним передаванням каналом в інфрачервоному діапазоні;
- технічні засоби систем просторового опромінювання в інфрачервоному діапазоні.

2 Виявлення та локалізування місця розташування джерел електромагнітних полів з перевагою (наявністю) магнітної складової поля, трас прокладання прихованої (непозначеної) електропроводки, потенційно придатної для встановлення закладних пристроїв, а також дослідження технічних засобів, що вони опрацьовують мовну інформацію.

До таких джерел та технічних засобів узвичаєно відносити:

– вихідні трансформатори посилювачів звукової частоти;

– динамічні гучномовці акустичних систем;

– електродвигуни магнітофонів та диктофонів.

### 7.2 Режими роботи приладу

Розв’язок контрольно-пошукових завдань забезпечується певною сукупністю режимів роботи приладу.

Схемотехнічна та програмна база дозволяє використання приладу в таких режимах роботи:

- режимі високочастотного детектора-частотоміра;
- режимі сканувального аналізатора провідних ліній;
- режимі детектора інфрачервоних випромінювань;
- режимі детектора низькочастотних магнітних полів;
- режимі акустичного приймача.
- режимі віброакустичного приймача;

### 7.3 Органи керування приладом

Керування приладом здійснюється за допомогою 16 – кнопкової клавіатури, яка забезпечує керування приладом в усіх його режимах.

Призначення кнопок:

– MUTE – здійснює ввімкнення (вимикання) вмонтованого гучномовця;

– HELP – дозволяє дістати контекстну допомогу, яку можна змінювати за допомогою кнопок”∇” та ”Δ”;

– OSC – здійснює осцилографічний контроль параметрів сигналу;

– SA – здійснює ввімкнення спектрального контролю параметрів сигналу;

– SAVE – забезпечує запис осцилограми в пам’ять;

– LOAD – здійснює виклик на екран з пам’яті осцилограми чи спектрограми;

– RUN/STOP – здійснює пуск/ зупин. динамічних вимірювань параметрів сигналу;

– SET – дозволяє здійснювати вибір різноманітних варіантів аналізування спектра сигналу;

– ENTER – забезпечує виведення для слухового контролю тонального або де модульованого сигналу;

– RESET – здійснює перезапускання приладу.

## 7.4 Порядок керування приладом в режимі детектора інфрачервоних випромінювань

Підімкнути інфрачервоний давач до з’єднувального кабелю, а сам кабель – до розніму PROBES.

Увімкнути живлення приладу.

Встановлення «нульового» порога детектора здійснюється автоматично, при вмиканні. У разі потреби, натисканням кнопок « ◂ » чи « ▸ » встановити вручну поріг детектора, керуючись показами додаткової шкали «min - - -|- - - max». Якщо буде потрібно, натисканням кнопки « ▲ » повернутися до автоматичного встановлення порога.

Візуально, за кількістю цілковито пофарбованих елементів 21-сегментної шкали та «на слух», за частістю клацань у вмонтованому гучномовці чи то головних телефонах, оцінити рівень прийнятого інфрачервоного випромінювання.

Натисканням кнопки RUN/STOP зупинити, за потреби, динамічні вимірювання рівня інфрачервоного випромінювання. Повторним натисканням цієї кнопки відновити динамічні вимірювання.

Натисканням кнопки ENTER (для переведення звукової індикації до режиму AUD) прослухати наявність та зміст потенційно небезпечних модульованих інфрачервоних радіовипромінювань.

Натиснути кнопку MUTE й наступними натисканнями кнопок «+» та «–» встановити необхідну гучність звукового сигналу (тонального чи демодульованого), виведеного на вмонтований гучномовець, чи на головні телефони.

Натисканням кнопки OSC перейти, за потреби, до осцилографічного контролю параметрів демодульованого сигналу.

Натисканням кнопки SA перейти, за потреби, до аналізування спектра демодульованого сигналу.

У разі збивання у роботі натиснути кнопку RESET – і здійснити перезапускання приладу.

## 7.5 Порядок керування приладом в режимі детектора низькочастотних магнітних полів

Підімкнути зовнішню магнітну антену до з'єднувального кабелю, а сам кабель – до розніму PROBES.

Увімкнути живлення приладу. Осцилографічний контроль параметрів прийнятого по магнітному полю сигналу вмикається автоматично.

Візуально, за амплітудою та характером сигналу, на осцилограмі та на слух, за його тональністю, у вмонтованому гучномовці чи головних телефонах, оцінити рівень магнітного поля та присутність фону електромережі 220 В × 50 Гц чи її гармонік. За потреби, в разі високого рівня фону електромережі, перемикачем на її корпусі (положення до білої точки) увімкнути диференційний режим антени.

Натисканням кнопки RUN/STOP зупинити, за потреби, динамічні вимірювання. Повторним натисканням цієї кнопки відновити виведення на екран осцилограми, яка буде динамічно змінюватиметься.

Натиснути кнопку MUTE і наступними натисканнями кнопок «+» та «–» встановити потрібну гучність сигналу, виведеного на вмонтований гучномовець або на головні телефони.

Натиснути кнопку SA і перейти, за потреби, до аналізу спектра прийнятого сигналу.

У разі збивань у роботі натиснути кнопку RESET і здійснити перезапускання приладу.

## 7.6 Порядок керування вмонтованим осцилографом, аналізатором спектра та енергонезалежною пам'яттю

Після ввімкнення осцилографічного контролю сигналу автоматично чи вручну через кнопку OSC (у режимах високочастотного детектора-частотоміра, сканувального аналізатора провідних ліній, детектора інфрачервоних випромінювань) встановлюється такий порядок використання органів керування приладом:

Натиснути кнопку «▲» чи «▼» та виставити, вручну, необхідне значення межі вертикальної розгортки.

Натиснути кнопку «◀» чи «▶» й обрати найбільш зручне, для переглядання осцилограми, значення межі горизонтальної розгортки.

Натиснути кнопку SET, далі кнопку «3» й обрати необхідний варіант оцифрування сигналу. Натисканням кнопки ENTER підтвердити вибір.

Натиснути кнопку SET, далі кнопку «4» й обрати необхідний режим синхронізації. Натисканням кнопки ENTER підтвердити вибір.

Натиснути кнопку SET, далі кнопку «5» і встановити необхідний варіант умови синхронізації. Натисканням кнопки ENTER підтвердити вибір.

Якщо відсутня потреба використання чисельних значень параметрів сигналів, котрі відбиваються на осцилограмі, натиснути кнопку MUTE. Її повторне натискання повертає на екран зображення індикації чисельних значень параметрів аналізованого сигналу.

Натиснути кнопку RUN/STOP і ввімкнути, за потреби, режим курсорних вимірювань. Натисканням кнопок «◄» та «►» встановити вертикальний маркер в необхідне місце осцилограми.

Натиснути кнопку RESET та провести, за потреби, відносні вимірювання тимчасових інтервалів.

Натисканням кнопки RUN/STOP вийти з режиму курсорних вимірювань.

Натисканням кнопки ENTER перевести осцилограф до двоканального режиму з подаванням сигналу другим каналом через додатковий рознім OSC2. Повторним натисканням кнопки ENTER передати функції вимірювання та індикації на другий канал по входу OSC2.

Натисканням кнопки RESET знову запустити прилад в активованому режимі, потім кнопкою OSC повернути режим одноканального осцилографа .

Двічі, з інтервалом у 2 с, натисканням кнопки OSC, перевести осцилограф до одноканального режиму, з подаванням сигналу лише по додатковому входу OSC2.

Натисканням кнопки RESET знову запустити прилад до активованого режиму, потім кнопкою OSC повернути попередній осцилографічний режим.

Натисканням кнопки SAVE, далі кнопки ENTER записати необхідну осцилограму в енергонезалежну пам'ять.

Натисканням кнопки LOAD вивести на екран зображення кожної із записаних до пам'яті осцилограм.

Натисканням кнопки RUN/STOP, повернути режим роботи осцилографа до попереднього стану.

Натисканням кнопки LOAD, потім кнопки SAVE та ENTER стерти, вилучити з пам'яті осцилограму, яка не становить інтересу.

Натисканням кнопки SA увімкнути аналізатор спектра.

Натиснути кнопку «▲» чи «▼» й виставити, за потреби, відповідне значення межі вертикального розгорнення.

Натиснути кнопку «◄» чи «►» й обрати найбільш зручне значення межі горизонтальної розгортки.

Натиснути кнопку SET, далі однією з кнопок – «2», «3», «4», «5» та «6» – обрати необхідний варіант режиму аналізування спектра. Зроблений вибір бажано щоразу потверджувати натисканням кнопки ENTER.

Якщо відсутня потреба використання чисельних значень параметрів сигналів, котрі відбиваються на спектрограмі, натиснути кнопку MUTE. Повторне натискання цієї кнопки повертає на екран індикацію чисельних значень параметрів аналізованого сигналу.

Натисканням кнопки RUN/STOP увімкнути, за потреби, режим курсорних вимірювань. Натисканням кнопок «◄» та «►» встановити вертикальний маркер на необхідну частотну складову спектрограми.

Натисканням кнопки RESET провести, за потреби, відносні вимірювання частотних інтервалів.

Натисканням кнопки RUN/STOP вийти з режиму курсорних вимірювань.

Натисканням кнопки ENTER перевести аналізатор спектра до двоканального режиму з подаванням сигналу другим каналом через додатковий рознім OSC2. Повторним натисканням кнопки ENTER передати функції вимірювання та індикації на другий канал по входу OSC2.

Натисканням кнопки RESET знову перевести прилад до активованого режиму, потім кнопкою SA повернути аналізатор спектра до попереднього одноканального режиму.

Двічі, з інтервалом у 2 с, натисканням кнопки SA перевести аналізатор до одноканального режиму з подаванням сигналу лише по додатковому входу OSC2.

Натисканням кнопки RESET знову перевести прилад до активованого режиму, потім кнопкою SA повернути попередній режим аналізатора спектра.

Натисканням кнопки SAVE, потім кнопки ENTER записати необхідну спектрограму до енергонезалежної пам'яті.

Натисканням кнопки LOAD вивести на екран зображення кожної із записаних до пам'яті спектрограм.

Натисканням кнопки RUN/STOP повернути аналізатор спектра до попереднього стану.

Натисканням кнопки LOAD, потім кнопок SAVE та ENTER стерти (вилучити) з пам'яті спектрограму, яка не становить інтересу.

# 8 Рекомендації з проведення контрольно-пошукових робіт з використанням приладу ST– 031 „Піранья”

## 8.1 Використання приладу для виявлення каналів витоку інформації в інфрачервоному діапазоні

Принципово слід розглядати два види таких каналів витоку інформації. Один з них утворюється за рахунок застосовування спеціальних технічних засобів з передавання перехоплюваної інформації в інфрачервоному діапазоні. Інший канал грунтується на опроміненні віконних скляних прорізів спрямованим променем джерела інфрачервоних випромінювань та прийманні відбитого сигналу, промодульованого акустикою приміщення.

Для виявлення обох каналів витоку слід провести однакові підготовчі заходи. Насамперед слід правильно обрати час проведення перевірки, а саме такий, коли у вікна контрольованого приміщення не потрапляють прямі сонячні промені. У самому приміщенні необхідно вимкнути лампи розжарювання та джерела інтенсивного теплового випромінювання. Доцільно також вимкнути,

якщо він є, кольоровий телевізор, тому що давач приладу може реагувати на теплі тони зображення.

Специфіка інфрачервоних закладок визначає необхідність забезпечення прямої видимості поміж передавачем закладки та приймачем інфрачервоних випромінювань. Тому в приміщенні шлях слідування випромінювання передавача назовні може пролягати лише через віконні прорізи. З урахуванням цих особливостей пошук небезпечних сигналів слід розпочинати від вікон приміщення, пересуваючись у глиб його. Оскільки в передавача може бути досить вузька діаграма спрямованості, а кут зору давача приладу становить $30^{o}$C, необхідно плавно змінювати просторове орієнтування давача. Ознакою наявності інфрачервоного випромінювання є з'явлення пофарбованих сегментів шкали індикатора рівня та клацання звукової індикації в режимі TONE після фарбування 4-го елемента шкали. Аналіз виявлених сигналів може провадитися на слух в режимі AUD, а також візуально, з використанням вмонтованих осцилографа та аналізатора спектра. Локалізування джерел інфрачервоного випромінювання найбільш точно здійснюється поєднанням амплітудного методу та методу акустозав'язки. При цьому порядок діє такий самий, як і при роботі в режимі високочастотного детектора-частотоміра.

Для виявлення зовнішніх потенційно небезпечних інфрачервоних випромінювань слід обстежувати кожен віконний проріз. При цьому давач орієнтується в бік вікна. Плавно змінюючи його просторове положення, провести обстеження всієї площі віконного прорізу. Оскільки зондувальний сигнал не має модуляції, то його наявність може бути оцінено лише за показниками індикатора рівня та тональної індикації в режимі TONE.

## 8.2 Використання приладу для виявлення каналів витоку інформації низькочастотними магнітними полями

Для таких каналів характерне є те, що вони виникають при використанні за цільовим призначенням санкціонованих засобів (ПЕОМ, переговорних пристроїв, систем звукопідсилення, магнітофонів, телефонів тощо). Тому за одне з головних завдань слід вважати дослідження таких засобів на наявність, інтенсивність та дальність низькочастотного магнітного поля. Супутніми можуть вважатися завдання пошуку прихованої (несанкціоновано прокладеної) проводки та виявляння працюючих диктофонів.

Перед проведенням робіт доцільно вимкнути в приміщенні люмінесцентні світильники, а антену приладу, за необхідністю, ввімкнути в диференційному режимі (перемикач на корпусі антени поставити в положення до білої точки).

Потенційні джерела небезпечних низькочастотних магнітних полів слід перевіряти роздільно, включаючи їх у роботу по черзі.

При дослідженні технічних засобів слід оцінити дальність поширення магнітних полів та особливості їхнього спектра. Для цього спочатку розмістити магнітну антену в безпосередній близькості до досліджуваного об'єкта. Зафіксувати за осцилограмою відносний рівень поля. Віддаляючись від

досліджуваного засобу і змінюючи просторове орієнтування антени, оцінити дальність упевненого приймання низькочастотного сигналу.

Стосовно посилювачів звукової частоти, що вони мають вихідний трансформатор, слід оцінити дальність упевненого (розбірливого) приймання мовного (тестового) сигналу. Таке оцінювання може слугувати за основу для правильного вибору місць установлення відповідних засобів стосовно зовнішнього боку приміщення та варіанта їхнього спільного розташування в приміщенні. За необхідності ввімкнути режим SA, проаналізувати спектрограму й записати її до енергонезалежної пам'яті.

Для пошуку прихованої проводки треба послідовно обійти всі стіни приміщення, розташовуючи магнітну антену в безпосередній близькості до них. Зафіксувати область зростання рівня поля й шляхом переміщення антени горизонталлю та вертикаллю визначити проходження траси прихованої проводки.

Можливість виявлення працюючих диктофонів визначається як рівнем магнітного поля, створюваного їхніми двигунами, так і рівнем магнітного фону приміщення. Для розв’язку цього завдання зазвичай застосовують спеціалізовані засоби з попередньою ретельною підготовкою приміщення. Тому не завжди може бути досягнуто позитивного результату лише при використанні приладу ST – 031 „Піранья”, надто на відстані поміж диктофоном та магнітною антеною понад 30 см.

## 9 Зміст протоколу

9.1 Структурна схема закладного пристрою.

9.2 Структурна схема пошукового процесу;

9.3 Опис проведення пошуку закладних пристроїв в різних режимах роботи .

9.4 Оцінка результатів пошуку (висновки).

## Лабораторна робота № 4
## Вимірювання витоку інформації акустоелектричним каналом за допомогою комплексу „Бумеранг - 2Г”

### 1 Мета роботи

Вивчення методів оцінювання захищеності об’єктів інформаційної діяльності від витоку інформації акустоелектричним каналом.

Вивчення комплексу „Бумеранг - 2Г”.

### 2 Домашнє завдання

а) вивчити параметри мови та мовного сигналу;

б) вивчити типи розбірливості мови;

в) вивчити причини виникнення акустоелектричного каналу витоку інформації.

### 3 Зміст роботи

а) розглядання особливостей фізичних процесів за витоку інформації акустоелектричним каналом;

б) вивчення апаратурного комплексу „Бумеранг - 2Г”;

в) проведення вимірювання захищеності об’єктів інформаційної діяльності від витоку інформації акустоелектричним каналом;

г) складання протоколу вимірювань.

### 4 Зміст протоколу вимірювань

а) схема вимірювання захищеності об’єкта інформаційної діяльності від витоку інформації акустичним та віброакустичним каналами;

б) таблиця результатів вимірювань;

в) оцінка результатів вимірювань (висновки).

### 5 Ключові положення

Акустоелектричні технічні канали витоку інформації виникають за рахунок електроакустичних перетворювань акустичних сигналів на електричні і включають перехоплення акустичних коливань через допоміжні технічні засобі й системи з "мікрофонним ефектом", а також шляхом "високочастотного нав'язування".

Ефект електроакустичного перетворювання акустичних коливань на електричні часто називають "мікрофонним ефектом".

Деякі елементи допоміжних технічних засобів та систем, у тому числі трансформатори, котушки індуктивності, електромагніти вторинних електрогодинників, дзвінки телефонних апаратів, дроселі ламп денного світла,

електрореле тощо, мають властивість змінювати свої параметри (ємність, індуктивність, опір) під впливом акустичного поля, створюваного джерелом акустичних коливань. Змінювання параметрів призводить чи то до виникнення на цих елементах електрорушійної сили, яка змінюється за законом змінювання впливово інформаційного акустичного поля, чи то до модулювання струмів, які протікають цими елементами, інформаційним сигналом. Наприклад, акустичне поле, впливаючи на якір електромагніта викличного телефонного дзвінка, спричинює його коливання, внаслідок чого змінюється магнітний потік осердя електромагніта. Змінювання цього потоку спричинює виникнення електрорушійної сили самоіндукції в котушці дзвінка, котра змінюється за законом змінювання акустичного поля.

Допоміжні технічні засобі й системи, окрім зазначених елементів, можуть містити безпосередньо електроакустичні перетворювачі. До таких допоміжних технічних засобів та систем належать деякі давачі пожежної сигналізації, гучномовці ретрансляційної мережі тощо. Ефект електроакустичного перетворювання акустичних коливань на електричні часто називають "мікрофонним ефектом", причому з допоміжних технічних засобів та систем з "мікрофонним ефектом" найбільшу чутливість до акустичного поля мають абонентські гучномовці й деякі давачі пожежної сигналізації.

Перехоплення акустичних коливань у певному каналі витоку інформації здійснюється шляхом безпосереднього з підмикання до з’єднувальних ліній допоміжних технічних засобів та систем з "мікрофонним ефектом", спеціальних високочутливих низькочастотних підсилювачів. Наприклад, підмикаючи такі засоби до з’єднувальних ліній телефонних апаратів з електромеханічними викличними дзвінками, можна прослуховувати розмови, що ведуться в приміщеннях, де встановлено ці апарати.

Технічний канал витоку інформації шляхом "високочастотного нав'язування" може бути здійснено шляхом несанкціонованого контактного впровадження струмів високої частоти від відповідного генератора в лінії (кола), які мають функціональні зв'язки з нелінійними чи параметричними елементами допоміжних технічних засобів та систем, на яких відбувається модуляція високочастотного сигналу інформаційним. Інформаційний сигнал у даних елементах допоміжних технічних засобів та систем виникає внаслідок електроакустичного перетворювання акустичних сигналів на електричні. Внаслідок того, що нелінійні чи параметричні елементи допоміжних технічних засобів та систем для високочастотного сигналу зазвичай являють собою неузгоджене навантаження, змодульований високочастотний сигнал відбиватиметься від нього й поширюватиметься у зворотньому напрямку лінією чи випромінюватися. Для приймання випромінюваних чи відбитих високочастотних сигналів використовуються спеціальні приймачі з вельми високою чутливістю. Задля запобігання впливові зондувального й перевідбитого сигналів можуть використовуватися імпульсні сигнали.

Найбільше часто такий канал витоку інформації використовується для перехоплювання розмов, які ведуться в приміщенні, через телефонний апарат, який має вихід за межі контрольованої зони. Задля запобігання впливові

високочастотного сигналу на апаратуру АТС у лінію, що йде в її бік, установлюється спеціальний високочастотний фільтр.

## 6 Умови проведення вимірювань

Прилад “Бумеранг-2Г” обладнано вимірювальним мікрофоном з рівномірною амплітудно-частотною характеристикою, що дозволяє провадити вимірювання звукоізолювальних огороджувальних конструкцій в потрібному діапазоні частот.

Визначення ефективності звукоізоляції виокремлених приміщень провадиться по кожній огороджувальній конструкції (також по міжповерхових перекриттях) на робочих частотах 500, 1000, 2000, 4000 Гц.

Ефективність звукоізоляції зовнішніх (вуличних) стін виділених приміщень, що їх розташовано вище за перший поверх, оцінюється за звукоізолювальними властивостями приміщення, аналогічного за будівельними характеристиками (матеріал стін, стелі, підлоги й т. і.) на першому поверсі тієї самої будівлі.

Якщо у виокремлено му приміщенні розгорнуто систему звукопосилення, то вона може використовуватися для посилення тестових сигналів, створюваних блоком 2 приладу “Бумеранг-2Г”. При цьому система звукопосилення на момент проведення контрольних вимірювань має працювати з номінальною вихідною потужністю.

Нормованою величиною звукоізолювальних властивостей огороджувальних конструкцій є показник звукоізоляції (Ro).

Необхідно обирати час для проведення вимірювань, коли сторонні акустичні завади мають мінімальний рівень, а також вимкнути:

– всі технічні засоби, що вони створюють акустичні завади;

– електрообладнання, не призначене для даних вимірювань.

### 6.1 Порядок проведення вимірювань

Підготувати прилад “Бумеранг-2Г” до роботи відповідно до інструкції з експлуатації.

Для підготовки до роботи блока 1:

– ручки регуляторів блока 1 повернути проти годинникової стрілки до упору;

– всі кнопки перемикачів мають перебувати у відтисненому стані;

– натиснути кнопки ПИТ та U, стрілка приладу має перебувати в межах виокремленого сектору шкали;

– натиснути кнопку “**+/–**“, стрілка приладу має залишитися в межах сектора.

Для підготовки блока 2:

– ввімкнути блок до системи захисного заземлення;

– ручки регуляторів блок 2 повернути проти годинникової стрілки до упору;

– тумблер ЛИН – ГР встановити в положення ГР, інші тумблери – в положення ВЫКЛ;

– перевірити справність запобіжника та відповідність його номіналові, зазначеному на панелі.

Для роботи з блоком 1:

– натиснути кнопку ПИТ;

– перемикачем частот настроювання встановити необхідну смугу частот приймача – 0,5 кГц (ШИР-0,5-1,0-2,0-4,0);

– натиснути кнопку ВД**.**

Для роботи з блоком 2: – ввімкнути тумблер СЕТЬ;

– перемикач ЛИН – ГР встановити в положення ГР;

– рознім ВД блока 1 з'єднати з розеткою "КОНТРОЛЬ" блока 2 за допомогою з'єднувального кабелю СШКИ.468222.500, що він входить до комплекту приладу "Бумеранг-2Г";

– частоту генератора блока 2 встановити грубо за допомогою перемикача 0,5-1,0-2,0-4,0 в положення 0,5 кГц;

– ручку УРОВЕНЬ встановити приблизно на середину і ручкою ЧАСТОТА встановити точно частоту 0,5 кГц за максимальним показником стрілки вимірювального пристрою блока 1;

– вимкнути рознім ВД блока 1 з розетки КОНТРОЛЬ блока 2;

– ввімкнути вимірювальний мікрофон до входу блока 1 (гніздо ВД, перемикач входу блока 1 має залишатися в положенні ВД);

– встановити блоки 1 та 2 на відстані 2,0 м один від одного (акустична система блока 2 має бути спрямована на вимірювальний мікрофон блока 1);

– за допомогою регулювання рівня вихідної напруги генератора блока 2 домогтися максимально можливого звукового тиску на відстані 2,0 м від акустичної системи блока 2 (який дорівнює приблизно 100 дБ);

– виконати вимірювання рівня сигналу $U_{c1}$ (мкВ), пропорційного звуковому тискові, який створює блок 2 на зазначеній відстані 2,0 м;

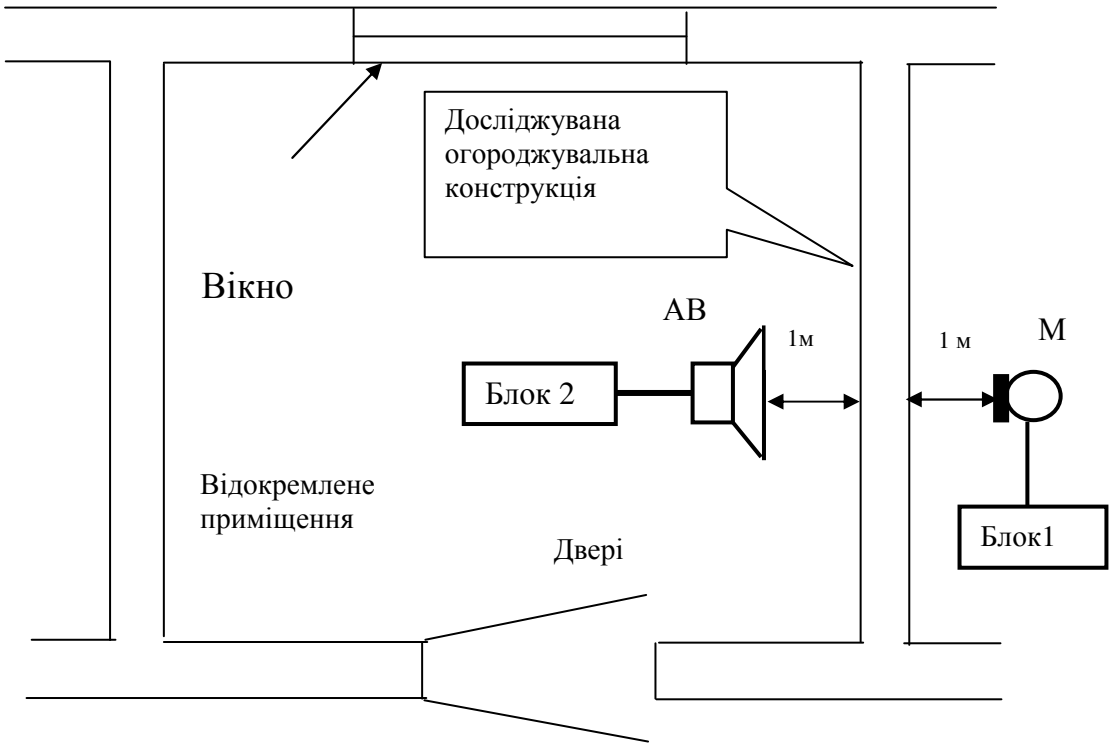
– встановити акустичну систему блока 2 на відстані 1,0 м від досліджувальної огороджувальної конструкції; при цьому акустична система має бути спрямована на досліджувану огороджувальну конструкцію й за відсутності дверних та віконних пройомів встановлена в її центрі (рис. 1.13);

– встановити вимірювальний мікрофон з блоком 1 із зовнішнього боку досліджуваної огороджувальної конструкції у відповідності з рис. 1.13;

– зачинити всі двері, вікна, кватирки, зсунути віконні штори в перевірюваному приміщенні;

– ввімкнути блоки 1, 2;

– виміряти рівень сигналу $U_{c2}$ (мкВ), пропорційний до звукового тиску на відстані 1,0 м із зовнішнього боку досліджуваної огороджувальної конструкції.




М – вимірювальний мікрофон; АВ – акустичний випромінювач

Рисунок 1.13 – Схема проведення вимірювань

Виміряні значення $U_{c1}$, $U_{c2}$ внести до таблиці 2.1.

Вимірювання провадити за стрілковим індикатором блока 1 з урахуванням світлодіодного множника в мкВ/мВ.

Показник звукоізоляції визначається за формулою:

$$R_{зв} = 10 \lg (U_{c1}/U_{c2}), \qquad (1.1)$$

де: $U_{c1}$ – рівень сигналу, пропорційний до звукового тиску, виміряного у перевірюваному приміщенні;

$U_{c2}$ – рівень сигналу, пропорційний до звукового тиску, виміряного із зовнішнього боку перевірюваної огороджувальної конструкції.

Результати вимірювань $U_{c1}$ та $U_{c2}$ внести до табл. 4.1, обчислити значення $R_{зв}$.

За показник звукоізоляції всього перевірюваного приміщення приймається мінімальне значення із усіх $R_{зв}$, обчислених для кожної контрольної частоти.

Для визначення ефективності звукоізоляції перевірюваного приміщення треба порівняти значення $R_{зв}$, здобуті внаслідок розрахунків, з нормованими значеннями звукоізоляції $R_o$, наведеними в табл. 1.1. Якщо виконуються умови $R_{зв} >> R_o$ для кожної контрольної частоти, то ефективність звукоізоляції перевірюваного приміщення є достатня; якщо не виконуються – слід рекомендувати вживання заходів з підвищення звукоізолювальних

властивостей приміщення або встановлення активних засобів захисту мовної інформації.

Таблиця 1.1 – Показники звукоізоляції на контрольних частотах

| Перевірювана конструкція | Контрольні частоти, Гц | Рівні сигналу, пропорційні до звукового тиску, мкВ | | Показник звукоізоляції $R_{зв}$, дБ |
|---|---|---|---|---|
| | | $U_{c1}$ | $U_{c2}$ | |
| Стіна 1 | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |
| Стіна 2 | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |
| Стіна 3 (з вікном) | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |
| Стіна 4 (з дверима) | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |
| За стелею | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |
| Під підлогою | 500 | | | |
| | 1000 | | | |
| | 2000 | | | |
| | 4000 | | | |

## 6.2 Проведення вимірювань акустоелектричних перетворювань технічних засобів, лінії яких виходять за межі виокремленого приміщення

До таких технічних засобів належать: телефонні апарати, концентратори, автонабірні пристрої, пульти зв'язку, які мають вихід до міської мережі та системи зв'язку, гучномовці систем радіотрансляції та оповіщення, давачі пожежної, охоронної сигналізації, кондиціонери, вторинні електрогодинники та ін.

До проведення вимірювань необхідно:

а) Обрати час для проведення вимірювань, коли сторонні електромагнітні завади мають мінімальний рівень, для чого вимкнути з мережі електроживлення за можливості:

– всі технічні засоби, що вони створюють електромагнітні завади;

– електрообладнання, не призначене для даних вимірювань.

б) Встановити на відстані 0,6....1,0 м від досліджуваного пристрою акустичну систему блока 2 комплексу “Бумеранг-2Г” відповідно до рис. 1.14. При цьому мають виконуватися умови D > = 5,5 d,

де: D – відстань від акустичної системи до першої огороджувальної поверхні;

d – відстань від акустичної системи до досліджуваного пристрою.

(це не завжди є можливе через те, що розміри приміщення, де провадяться вимірювання, можуть бути менш за D (d = 0,6....1,0 м, тоді D = 3,3....5,5 м)).

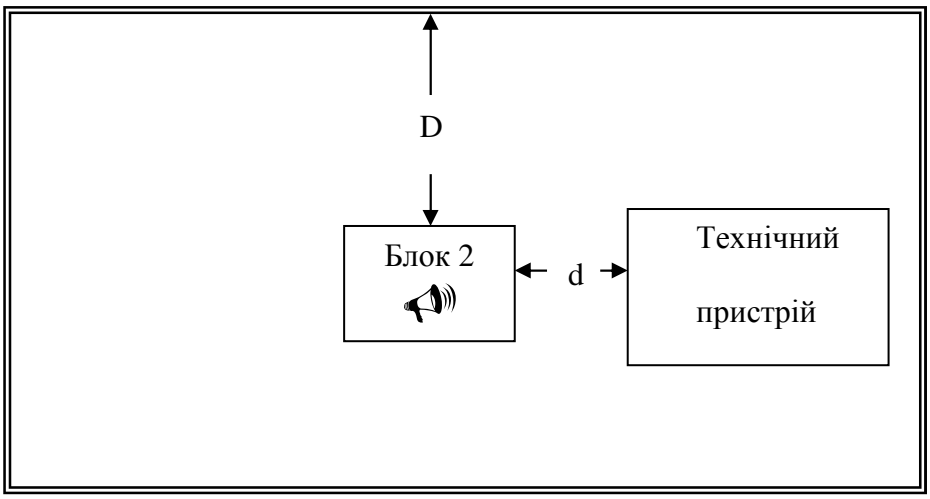



Рисунок 1.14 – Розташування комплексу “Бумеранг-2Г” відносно блоку 2

Для підготовки до роботи блока 1 ручки регуляторів повернути проти годинникової стрілки до упору. Всі кнопки перемикачів мають перебувати у відтисненому стані.

– натиснути кнопки ПИТ та U. Стрілка приладу має перебувати в межах відокремленого сектора шкали;

– натиснути кнопку “+/–“. Стрілка приладу має залишитися в межах сектора.

Для підготовки блок 2 ручки регуляторів повернути проти годинникової стрілки до упору. Тумблер ЛИН – ГР встановити в положення ГР, інші тумблери – в положення ВЫКЛ. Перевірити справність запобіжника та відповідність його номіналові, зазначеному на панелі. Ввімкнути блок до системи захисного заземлення.

Для роботи з блоком 1 натиснути кнопку ПИТ. Перемикачем частот налаштовування встановити потрібну смугу частот приймача – 1,0 кГц (ШИР – 0,5; 1,0; 2,0; 4,0). Натиснути кнопку ВД.

Для роботи з блоком 2 ввімкнути тумблер СЕТЬ. Перемикач ЛИН – ГР встановити в положення ГР.

Рознім ВД блока 1 з'єднати з розеткою КОНТРОЛЬ блока 2 за допомогою з'єднувального кабелю СШКИ.468222.500, що він входить до комплексу "Бумеранг-2Г".

Частоту генератора блока 2 встановити грубо за допомогою перемикача 0,5 – 1,0 – 2,0 – 4,0 в положення 1,0 кГц, ручку УРОВЕНЬ виставити приблизно на середину й ручкою ЧАСТОТА встановити точно частоту 1,0 кГц за максимальним показником стрілки вимірювального приладу блока 1. Вимкнути роз`ім "ВД" блока 1 з розетки КОНТРОЛЬ блока 2.

УВАГА: При висвітленні світлодіоду ПЕР – натиснути кнопку мкВ/мВ.

Порядок проведення вимірювань

Для проведення вимірювань слід скласти схему у відповідності з рис. 1.15, попередньо вимкнувши досліджуваний пристрій з лінії й навантажити на опір навантаження $R_н$ = 600 Ом, потужністю 0,5….2 Вт.

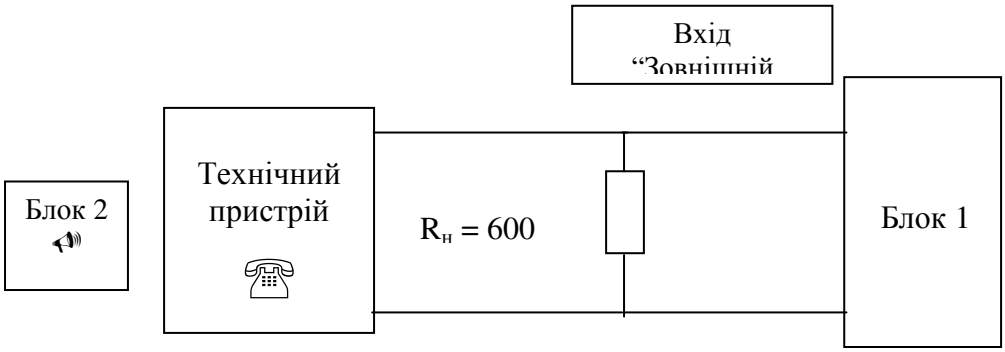



Рисунок 1.15 – Схема підмикання досліджуваного пристрою для проведення вимірювань рівня акустоелектричних перетворювань

Налаштувати генератор блока 2 на частоту $F_c$ = 1000 Гц та встановити максимальний вихідний рівень ($U_{вих. ген.}$ = 94 дБ).

Провести взаємне орієнтування акустичної системи блока 2 та досліджуваного пристрою, домагаючись максимального показника стрілкового індикатора блока 1. Для цього можна взяти досліджуваний пристрій (наприклад, телефонний апарат) в руки й повертати його відносно акустичної системи блока 2.

При проведенні вимірювань для унеможливлення акустичної зав'язки (самозбудження схеми вимірювань) слід уникати вмикання блока 1 до перевірюваного пристрою у безпосередній близькості від нього. Треба додержуватися умов на відстань поміж блоком 1 та досліджуваним пристроєм (за можливості, не менш за 1,5….2,0 м).

Виконати аналогічні вимірювання на всіх виходах досліджуваного пристрою (наприклад, для телефонного апарата – на телефонній парі; у разі, коли є в наявності паралельні телефонні апарати, незалежно від того, розташовані вони у виокремленому чи у іншому приміщенні, – на телефонній парі кожного телефонного апарата).

Результати вимірювань занести у табл. 1.2.

Таблиця 1.2 – Результаті вимірювань рівня небезпечного сигналу

| № п/п | Найменування технічного засобу, тип, зав. або інвентарний номер | Наявність акустоелектричних перетворювань та рівень небезпечного сигналу $U_{с.вим}$, мкВ | Примітки |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

## 7 Зміст протоколу лабораторної роботи

1 Назва лабораторної роботи.

2 Мета роботи.

3 Структурна схема вимірювання рівня захищеності об’єкта інформаційної діяльності від витоку інформації акустоелектричним каналом.

4 Таблиці результатів вимірювань.

5 Висновки.

## 8 Ключові запитання

1 Основні параметри мовного сигналу.

2 Визначення витоку інформації акустоелектричним каналом.

3 Джерела акустоелектричних перетворювань.

4 Особливості захисту від витоку інформації акустоелектричним каналом.

## Лабораторна робота № 5
## Пошук закладних пристроїв несанкціонованого знімання інформації за допомогою нелінійного локатора MS-888

### 1 Мета роботи

Вивчення засад нелінійної локації та методів пошуку закладних пристроїв несанкціонованого знімання інформації; вивчення нелінійного локатора MS-888.

### 2 Домашнє завдання

а) вивчити засоби нелінійної локації;
б) вивчити типи закладних пристроїв;
в) вивчити методи пошуку закладних пристроїв несанкціонованого знімання інформації.

### 3 Зміст роботи

а) вивчення нелінійного локатора MS-888;
б) практичне використання методів пошуку закладних пристроїв несанкціонованого знімання інформації за допомогою нелінійного локатора;
в) складання протоколу вимірювань.

### 4 Склад протоколу вимірювань

а) опис методики проведення пошуку закладних пристроїв;
б) структурна схема пошукового процесу;
в) оцінка результатів пошуку (висновки).

### 5 Ключове положення

Сьогодні широкого розповсюдження набуло застосовування підслуховувальної апаратури та закладних пристроїв (ЗП). Поєднання відносно невеликої ціни та високої якості таких пристроїв, а також відсутність строгих правових норм перетворюють цей канал витоку інформації на один з найнебезпечніших та найдоступніших.

Для виявлення в будівельних конструкціях приміщень та предметах інтер'єру таємно встановлених радіопередавальних пристроїв та інших технічних засобів для знімання інформації, котрі мають у своєму складі напівпровідникові компоненти й перебувають як у ввімкненому, так і у вимкненому стані, переважно використовуються два способи:

а) пасивне виявлення (до даного способу належить контроль радіоефіру за допомогою приймальних засобів та активне виявлення (за допомогою локації). Локація, в свою чергу, може здійснюватися радіолокаційним

зондуванням конструкцій на предмет виявлення чужорідних тіл, котрі мають більш високу щільність, або більш надійним нелінійним зондуванням;

б) активне виявлення, в основу котрого покладено властивість виявляти вироби радіоелектроніки нелінійним зондуванням за допомогою нелінійного локатора, базоване на фізичній властивості напівпровідникових компонентів, котра полягає в тому, що при їхньому опромінюванні зондувальним сигналом відбувається перетворення частоти сигналу на кратні гармоніки з їхнім подальшим випромінюванням в ефір. При цьому процес перетворення не залежить від технічного стану радіоелектронного пристрою (активного чи пасивного), котрий опромінюється.

Локатор поєднує високоефективне радіопередавання з високочутливим прийманням надзвичайно високою вибірністю, що супроводжує одночасне випромінювання та аналіз сигналу на різних, точно визначених частотах. Метою, результатом є збудження напівпровідникових елементів, ініціювання їхнього реакції в процесі пошуку, що потім може бути оцінено для підтвердження їх існування та місця розташування.

Транзистори та діоди, їхні нелінійні p-n переходи мають властивість відгукуватися, коли їх опромінюють хвилями певної частоти – збуджуються та перевипромінюють сигнал у простір на відповідних гармоніках радіохвиль, котрі їх опромінюють.

Приймання локатором будь-якої вищої гармоніки власного випромінювання рівнозначно встановлює наявність в зоні зондування напівпровідникового p-n переходу, що може свідчити про наявність замаскованого радіоелектронного пристрою. Отже, нелінійний локатор (НЛ) є ефективним засобом для виявлення пристроїв, котрі мають в собі напівпровідникові компоненти (НПК).

Всі нелінійні локатори за характером зондувального сигналу поділяються на локатори імпульсного та неперервного випромінювання, а також такі, що поєднують в собі технологічні можливості обох типів.

Сигнали відгуку гармонік можуть виявлятися і в разі відсутності напівпровідникових елементів. Приміром, два неоднорідних метали, зчеплені, або зварені, а також метали, піддаванні корозії, також викликають відбиття гармонійних сигналів.

Найбільш поширеною проблемою, котра виникає при використанні НЛ, є хибні сигнали (відгуки). Звичайні побутові електронні прилади, такі як телефон, чи то електронний годинник, збуджуватимуть в НЛ сигнал відгуку, тому що до їхнього складу входять електронні напівпровідникові компоненти. На практиці подібні відгуки, спричинювані побутовими приладами, можна легко відрізнити візуально. Також хибні відгуки можуть бути спричинювані металевими об'єктами, котрі взагалі не мають у своєму складі жодних напівпровідникових компонентів.

## 5.1 Опис роботи нелінійного локатора MS-888

- Перемикач живлення POVER, до моменту повного складання комплекту для режиму пошук, має перебувати в положенні ВИМКН – OFF.
- ЗАБОРОНЯЄТЬСЯ вмикати локатор під час заряджання вмонтованого чи ввімкненого зовнішнього акумулятора.
- ЗАБОРОНЯЄТЬСЯ спрямовувати антену ввімкненого локатора в бік людей, які перебувають поруч.

## 5.2 Технічні характеристики

Робоча частота – 888 МГц
Режим випромінювання – неперервний
Потужність випромінювання – 250 мВт
Робоча гармоніка, її індикація – друга
Максимальна глибина пошук – до 80 см (залежно від матеріалу переділки).

## 5.3 Принцип дії

Антена локатора MS-888 випромінює сигнал, а напівпровідниковий елемент (діод, транзистор, мікросхема) при опроміненні перетворює та перевипромінює сигнал опромінювальної частоти на кратні гармоніки (основна частота опромінення виробу – 888 МГц, а сигнал другої гармоніки буде виявлено на частоті 1776 Гц). Це свідчить проте, що наявність базового сигналу та сигналу будь-якого відгуку дозволяє з великою ймовірністю визначити наявність напівпровідникових елементів, загальновідомих як нелінійні з'єднання, з котрих на 70....80% складаються закладні пристрої.

В приладі MS-888 закладено принципи роботи в галузі локаторів нелінійностей. MS-888 може бути використано для визначення пошуку електронних пристроїв в місцях, недосяжних для візуального оглядання:

стіни зсередини;

стеля;

інженерні комунікації й тощо.

У зв'язку з тим, що MS-888 виявляє напівпровідникові елементи, не аналізуючи сигнал, котрий випромінюється підслуховувальними пристроями, він є ефективний навіть тоді, коли ці пристрої вимкнено. На відміну від більшості інших методів нелінійний локатор дозволяє виявляти:

непрацюючі ЗП (з вимкненим електроживленням);

ЗП з дистанційним керуванням котрі перебувають в режимі очікування;

ЗП зі спеціальними технологіями передавання інформації, котрі слугують для підвищення утаємничення їхньої роботи (вузькосмугова модуляція, передавання сигналів короткими серіями, після їхнього попереднього накопичування в пристрої пам'яті;

використання кількох несучих частот;

різноманітні складні види модуляції тощо).

Ця особливість нелінійних локаторів має важливе практичне значення, оскільки дозволяє при проведенні пошукових робіт не враховувати можливість дистанційного вимкнення ЗП стороною, котра підслуховує, а також підвищує ймовірність виявлення ЗП.

Водночас за допомогою нелінійного локатора не можна віднайти так звані пасивні закладки, котрі не мають в своєму складі напівпровідникових елементів. Такі ЗП використовуються вельми рідко, у зв'язку як з вельми значною великою вартістю як їхнього виготовлення, встановлення, так і з дорожнечею в експлуатації.

Пошукове обладнання, розроблене останнім часом на базі приймальних пристроїв, виявляє сигнал, котрий випромінюється ЗП, але під час пошуку прихованих дротових відеокамер, диктофонів чи неактивних передавачів, котрі ввімкнено чи вони перебувають в режимі чергового приймання, – воно є неефективне. MS-888 призначено для оперативного, швидкого пошуку саме таких пристроїв. MS-888 проводить пошук не сигналу, котрий випромінює закладний пристрій, а власне самого пристрою.

## 5.4 Порядок роботи з нелінійним локатором

1) До місця "А" ("3") ввімкнути антенний штекер шляхом фіксації в антенному гнізді обертанням за годинниковою стрілкою

2) До місця "В" ("4") ввімкнути другий антенний штекер шляхом загвинчування наглухо в антенному гнізді.

3 ) Ручку регулювання гучності VOLUME ("10") та ручку регулювання глибини контролю RANGE ("11") встановити в ліве крайнє положення.

4 ) Перемикач TONE/NOISE встановити в положення "12" TONE.

5 ) Включити живлення локатора шляхом встановлення вмикача живлення POVER в положення ON ("1").

УВАГА! – світіння індикатора зеленим кольором свідчить про працездатність батареї живлення;

– світіння індикатора червоним кольором свідчить про розряд батареї живлення та про необхідність її підзарядження;

– відсутність світіння індикатору вказує на цілковите розрядження батареї (про необхідність її заміни, про можливе ввімкнення зовнішньої, резервної батареї), або про необхідність заміни запобіжника FUSE, розміщеного з правого боку базового блока в ніші, котра має знімну кришку.

6 ) Для перезаряджання внутрішньої батареї слід під'єднати до багатоштекерного гнізда CHARGE/EXT.BATT ("8") зарядний пристрій з комплекту.

УВАГА! ЗАБОРОНЯЄТЬСЯ вмикати локатор під час заряджання внутрішньої батареї (про заряд свідчить світіння червоного індикатора на бічній кришці зарядного пристрою). Заряджання батареї повинно тривати 12 годин.

7 ) Для використання зовнішньої батареї необхідно:

– за допомогою окремого багатоштекерного кабелю з'єднати гніздо на бічній стінці зовнішньої батареї з багатоштекерним гніздом CHARGE/EXT.BATT (“8”) на лицьовій панелі базового блока локатора.

УВАГА! Світіння індикатора зеленим кольором свідчить про працездатність батареї живлення;

– світіння індикатора червоним кольором свідчить про розрядження батареї живлення та про необхідність її підзарядження;

– відсутність світіння індикатора вказує на цілковите розрядження батареї, про необхідність її заміни або про необхідність заміни запобіжника FUSE, розміщеного з правого боку базового блока в ніші, котра має знімну кришку.

## 5.5 Перевірка працездатності локатора на тестовій закладці

Скласти комплект та перевірити працездатність живлення.

Лицьова панель (відповідно до рис. 1.16) та призначення її складових частин:

- “1- 2” – положення вмикача живлення (POVER):
- положення ON – живлення локатора ввімкнено;
- положення OFF – живлення локатора вимкнено.
- “5” – іпереведенні перемикача живлення в положення ON свідчить про працездатність батарендикатор BATT – світіння індикатора зеленим кольором при ї живлення;
- світіння індикатора червоним кольором при переведенні перемикача живлення в положення ON свідчить про розрядження батареї живлення та про необхідність підзарядження батареї;
- відсутність світіння індикатора вказує на цілковите розрядження батареї, про необхідність її заміни, або про необхідність заміни запобіжника FUSE, розміщеного з правого боку базового блока в ніші, котра має знімну кришку.
- “6” – індикатор SIGNAL – зазначає наявність та величину сигналу відгуку.
- “7” – гніздо триконтактне PHONE, місце для підмикання головних телефонів.
- “8” – багатоштекерне гніздо CHARGE/EXT.BATT, призначене для підмикання зовнішньої батареї живлення, або для підмикання багатоштекерного з’єднувального кабелю від зарядного пристрою для підзарядження внутрішньої батареї.
- “9” – гучномовець, вмонтований для слухового контролю сигналу відгуку.
- “10” – ручка VOLUME, для регулювання гучності контрольного акустичного сигналу.

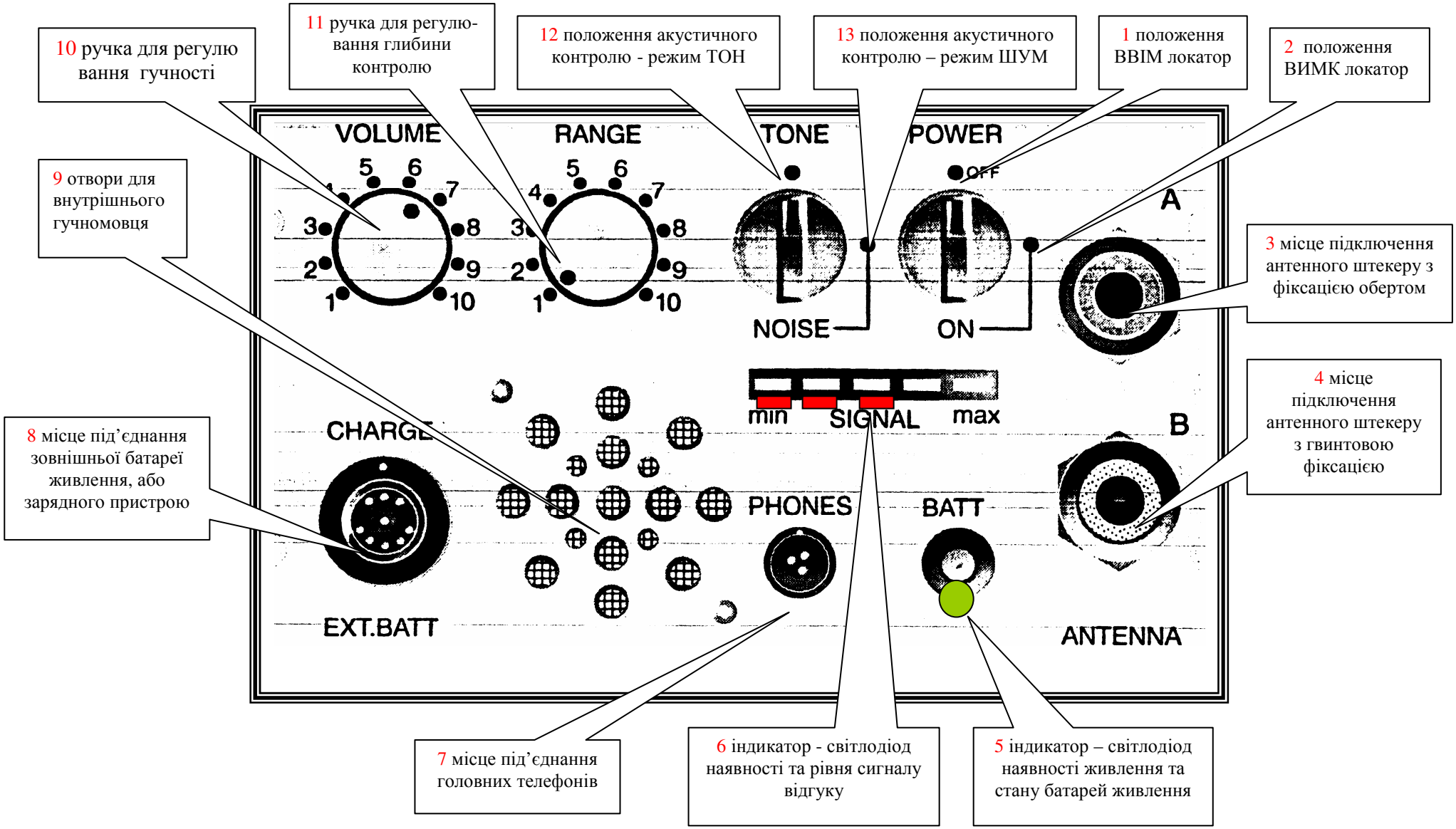



Рисунок 1.16 – Лицьова панель нелінійного локатора MS-888

- “11” – ручка RANGE, для змінювання глибини контролю шляхом регулювання потужності, випромінюваної через антену.
- “12 - 13” – положення перемикача ТОН(TONE)/ЗАВАДА(NOISE):

– в положенні ручки TONE оператор, при наближенні антени локатора до місця можливого розміщення закладного пристрою, почує в головних телефонах або на вмонтованому гучномовці (9) потріскуючий акустичний сигнал, котрий змінюватиметься від мінімального значення при віддалені антени до максимального значення при наближенні антени.

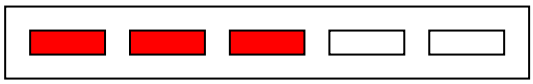
– в положенні ручки NOISE оператор, при наближенні антени локатора до місця можливого розміщення закладного пристрою, почує в головних телефонах, або на вмонтованому гучномовці (9) акустичний сигнал шуму, котрий змінюватиметься від максимального значення при віддалені антени до мінімального значення при наближенні антени.

- “3” – місце “А” для вмикання антенного штекера з фіксацією в антенному гнізді обертанням за годинниковою стрілкою.
- “4” – місце “В” для вмикання антенного штекера з фіксацією шляхом загвинчування наглухо в антенному гнізді.

1 Розмістити антену локатора над середньою частиною верхньої кришки коробки для транспортування локатора, за умови паралельного розміщення площин антени й кришки, та на відстані 10....20 см площини антени від площини кришки.

2 Про наявність тестової закладки буде свідчити:

– світлова індикація наявності та рівня сигналу відгуку;



**min SIGNAL max**

– звукова індикація:

– ручка “12” в положенні TONE, оператор при наближенні антени локатора до середини кришки футляра почує в головних телефонах або на вмонтованому гучномовці (9) потріскуючий акустичний сигнал, котрий змінюватиметься при наближенні антени до кришки від мінімального значення до максимального значення;

– звукова індикація: ручка “12” в положенні NOISE, оператор при наближенні антени локатора до середини кришки футляра почує в головних телефонах або на вмонтованому гучномовці (9) акустичний сигнал шуму, котрий змінюватиметься від максимального значення до мінімального значення.

3 Ручку регулювання глибини контролю RANGE (“11”) встановити в праве крайнє положення. При цьому антену локатора необхідно підняти над поверхнею кришки футляра на висоту 80....100 см, наявність індикації сигналу відгуку свідчитиме про технічну можливість розміщення закладних пристроїв (неоднорідностей) на різній глибині залягань.

4 Зміна горизонтального положення площини антени локатора вбік від середини кришки футляра призведе до зменшення рівня відгуку.

5 Зміна вертикального положення антени локатора на кут +/– 45°С з діями, зазначеними в попередньому пункті, дозволить за максимальним (в режимі TONE) чи мінімальним (в режимі NOISE) рівнем сигналу відгуку віднайти ціль з максимальною точністю площі розміщення до 5 кв. см.

6 УВАГА! Для гарантованого віднайдення цілі швидкість сканування (переміщення площини локатора) не повинна перевищувати 30 см/с.

## 6 Методика пошуку закладних пристроїв

1 Виконати складання комплекта локатора.

2 Виконати перевірку живлення та працездатності на тестовій закладці.

3 За необхідності використання головних телефонів (в разі підвищення таємності пошуку чи в разі необхідності зменшення енерговитрат батарей живлення) ввімкнути головні телефони до гнізда триконтактного PHONE (“7”) на лицьовій панелі базового блока.

4 Ручкою регулювання гучності VOLUME (“10”) встановити комфортний для себе рівень гучності.

5 Ручкою регулювання глибини контролю RANGE (“11”) встановити максимальну глибину пошуку в праве крайнє положення 63.6. З місця пошуку (приміром, з приміщення) винести всі електронні предмети, (засоби зв'язку, телебачення, тестові закладки, і т. д., все те, що має в своєму складі напівпровідникові елементи).

6 Відрегулювати головку антени та довжину штанги (шляхом розкручування та фіксування кільцевих зажимів) в зручне положення для проведення обстеження.

7 Площинну поверхню антени наблизити на максимально малу відстань від обстежуваного об'єкта. Зона пошуку (обстеження) відповідає розмірам площі антени.

8 Швидкість пересування антени обстежуваною площею, не повинна перевищувати 30 см/с.

9 Під час пересування (сканування) антени в межах обстежуваної площі водночас неодмінно слід змінювати вертикальне положення (відносно площини обстежування) антени локатора на кут +/– 45°С, що дозволить за найбільшим (чи то найменшим залежно від режиму пошуку) рівнем сигналу відгуку віднайти ціль з максимальною точністю (площа до 5 кв. см).

Під час пошуку:

– локатор сам собою не виявляє підозрілих цілей без оператора!

– в локаторі MS-888 не існує точного визначення, що віднайдений відгук може бути відгуком закладного пристрою;

– практично не завжди можна повторити точну копію відгуку та відповідне положення цілі, тому для зменшення ймовірності змінювання поля та сили випромінювання необхідно провадити обстеженню за абсолютної відсутності сторонніх осіб (окрім оператора);

– відгук вкаже на наявність та місцезнаходження підозрілого предмета, тому обов'язково необхідне фізичне обстеження підозрілого предмета, ділянки й т.п., котре провадиться у відповідності з "Методикою на фізичне обстеження". Фізичне обстеження повинно дати гарантію стосовно ідентифікації підозрілого об'єкта, його походження, всіляких загроз, котрі він, цей об'єкт, може здійснити;

– відстань, на якій зареєстровано відгук, також його рівень не зазначають розмірів підозрілого об'єкту, тому кожен відгук окремо має оцінюватися;

– локатор MS-888 екрановані закладні пристрої не віднаходить.

При одержанні сигналу відгуку в режимі TONE необхідно перевести локатор в режим NOISE (шум).

Якщо віднайдений відгук належить до напівпровідникових елементів – тоді при наближенні антени локатора до підозрілого об'єкта аудіошум зменшуватиметься майже до нуля (ефект загасання).

В разі, коли знайдений відгук належить до неоднорідностей (іржа, металеві скрутки, спайки), – тоді при наближенні антени локатора до підозрілого об'єкта аудіошум збільшуватиметься.

Окрім того, якщо за наявності сигналу відгуку постукувати резиновим молоточком по підозрілому місцю, тоді, за наявності в підозрілому місці напівпровідника, змінювання аудіошуму не відбудеться, а за наявності неоднорідного з'єднання при постукуванні – в головних телефонах буде відчутне потріскування.

При застосовуванні локатора в пошукових заходах можливі не лише виявлення електронних пристроїв, а й їхня класифікація в режимі аудіо демодуляції (NOISE).

Так, наприклад, при виявленні деяких звукозаписувальних засобів можна почути аудіосигнал головки запису. Більш того, часто можливе прослуховування синхроні-зувальних імпульсів при виявленні прихованих відеокамер.

## 7 Зміст протоколу лабораторної роботи

1 Назва лабораторної роботи.
2 Мета проведення роботи.
3 Структурна схема пошуку закладних пристроїв.
4 Опис результатів пошуку закладних пристроїв.
5 Висновки.

## 8 Ключові запитання

1 Основні типи закладних пристроїв.
2 Структурна схема закладного пристрою.
3 Принцип нелінійної локації закладних пристроїв.
4 Основні типи нелінійних локаторів.

# Лабораторна робота № 6
# Вимірювання витоку інформації акустичним та віброакустичним каналами за допомогою комплексу “Ореол-А”

## 1 Мета роботи

а) вивчення методів оцінювання захищеності об’єктів інформаційної діяльності від витоку інформації акустичним та віброакустичним каналами;

б) вивчення вимірювального комплексу „Ореол-А”.

## 2 Домашнє завдання

а) вивчити параметри мови та мовного сигналу;

б) вивчити типи розбірливості мови;

в) вивчити характеристики та параметри акустичних полів та методи їхнього вимірювання.

## 3 Зміст роботи

а) розглядання особливостей фізичних процесів від витоку інформації акустичним та віброакустичним каналами;

б) вимірювання розбірливості мови(формантної та складової);

в) вивчення апаратурного комплексу „Ореол-А”;

г) складання протоколу вимірювань.

## 4 Склад протоколу вимірювань

а) схема вимірювання захищеності об’єкта інформаційної діяльності від витоку інформації акустичним та віброакустичним каналами;

б) таблиця результатів вимірювань;

в) оцінка результатів вимірювань (висновки).

## 5 Ключові положення

### 5.1 Формування і сприймання мовного сигналу

Акустичний канал виникає внаслідок утворення звукових хвиль стискування, які створюються голосовим апаратом людини, й поширення їх в повітряному просторі, а також проникнення через несучі стіни будівель, вікон, дверей, вентиляційних повітроводів через пори, щілини тощо.

Існує два основних погляди на формування та сприймання мовних сигналів, виходячи з основних понять теорії розбірливості й теорії інформації:

– з точки зору аналогових перетворювань мовних сигналів;

– з точки зору дискретних перетворювань мовних сигналів.

Мовний тракт являє собою складний акустичний фільтр з низкою резонаторів, які створюються порожнинами рота, носа, носоглотки. При вимовлянні звуків мови через мовний тракт проходить чи тональний імпульсний сигнал (дзвінкі звуки), або шумовий (глухі звуки), або обидва разом. Внаслідок цього рівномірний спектр (тональний чи шумовий) перетворюється на спектр з рядом максимумів, які називаються формантами, й мінімумів, які називаються антиформантами. Поза як найбільш інформативними є глухі приголосні, то за впливу шумів розбірливість мови знижується, насамперед через маскування глухих звуків.

Вухо людини має властивість дискретного сприймання на частотному й динамічному діапазонах. Слухове відчуття є пропорційне до логарифму подразнювальної сили I:

$$E \text{ дБ} = 10\lg (I / I_{ПС}), \qquad (1.2)$$

де: $I_{ПС}$ – подразнювальна сила на порозі чутності.

Величину E називають рівнем відчуття, причому

$$E = L1 - LПС, \qquad (1.3)$$

де: $L_1 = 10 \lg I + 120$ – рівень інтенсивності звуку I, Вт/м$^2$.

Рівень відчуття, який являє собою рівень над порогом чутності, неточно характеризує суб'єктивне відчуття, тому в акустиці застосовується поняття рівня гучності (голосності) звуку (чи шуму), тобто рівня в децибелах рівноголосного з ним чистого тону 1000 Гц.

У відповідності до кривих однакової гучності, за рівня 30....40 фон (рівень гучності в дБ на частоті 1000 Гц) в діапазоні частот 250….500 Гц відбувається зменшення гучності приблизно на 6 дБ. Тому за приймання елементів мови технічними засобами це зниження можна скомпенсувати частотним коригуванням, що неможливо здійснити за приймання мови людини.

Сприймання мови значною мірою залежить від рівня акустичних шумів, які спричинюються джерелами – як зовнішніми, які перебувають за межами приміщення, так і внутрішніми. Як правило, при розрахунках розглядаються стаціонарні шуми, але впродовж тривалого періоду (день–ніч, робочі дні – вихідні) шуми можуть набувати нестаціонарного характеру, тобто змінюватись з часом. Маскувальні властивості шумів виявляються тим сильніше, чим більше їхнє перевищення над корисним сигналом по всій смузі частот мовного діапазону. Найбільший маскувальний ефект мають широкосмугові завади з „гладким" спектром, але задовільна розбірливість мови може бути досягнута навіть у тому разі, якщо рівень мови буде на кілька децибелів нижче за рівень шуму.

Вузькосмугові завади, навіть високого рівня, не можуть забезпечити необхідного ступеня зашумлення мови, тому що вони, як правило, мають періодичний характер, що дозволяє їх частково скомпенсовувати за допомогою різноманітних фільтрів.

Для визначення максимально припустимого рівня шуму в приміщеннях, у відповідності із санітарними нормами, застосовуються граничні спектри (ГС).

Число при ГС означає рівень шуму в октавній смузі із середньогеометричною частотою 1000 Гц. Оскільки санітарні норми обмежують максимальне значення рівня шуму для різних типів приміщень, то граничні спектри можна використовувати для обчислення розбірливості мови в конкретних випадках. Рівні інтенсивної мови в октавних смугах і деякі значення граничних спектрів шумів наводяться в табл. 1.3.

Таблиця 1.3 – Рівні інтенсивної мови в октавних смугах та граничні спектри шумів

| № октави | Середня Частота f сер, Гц | Рівні мови і граничні спектрі шумів, дБ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | мова | ГС-20 | ГС-25 | ГС-30 | ГС-35 | ГС-40 | ГС-45 | ГС-50 | ГС-55 |
| 1 | 250 | 67,9 | 31 | 35 | 40 | 45 | 49 | 55 | 59 | 63 |
| 2 | 500 | 66,9 | 24 | 29 | 34 | 39 | 44 | 49 | 54 | 59 |
| 3 | 1000 | 61,5 | 20 | 25 | 30 | 35 | 40 | 45 | 50 | 55 |
| 4 | 2000 | 57,0 | 17 | 22 | 27 | 32 | 37 | 42 | 47 | 52 |
| 5 | 4000 | 53,0 | 14 | 20 | 25 | 30 | 35 | 4 | 44 | 50 |
| 6 | 6000 | 48,5 | 13 | 18 | 23 | 28 | 33 | 38 | 43 | 49 |
| Сумарні рівні, дБ | | 71 | 32,3 | 36,6 | 41,6 | 47 | 51 | 60 | 61 | 65 |

Значення рівнів шумів, виміряні на частоті 1000 ГЦ в різних місцях наведено в табл. 1.4.

## 5.2 Розбірливість та зрозумілість мови

Розбірливістю називають відносну чи відсоткову кількість прийнятих спеціально тренованими слухачами (артикулянтами) елементів мови із загальної кількості передаваних тракту. Оскільки в якості елементів мови застосовуються звуки, склади, слова та фрази, то має місце звукова, складова, словесна та фразова розбірливість. Всі вони при випробовуванні однієї й тієї самої системи виражатимуться різними чисельними величинами. Поза як відсоток правильних оцінок для передбачуваного повідомлення є завжди вище, аніж для непередбачуваного, ступінь же передбачання при прослуховуванні фрази є вище, аніж при прослуховуванні окремих слів чи складів. Але всі види розбірливості пов’язані один з одним однозначними функціональними залежностями, які подаються зазвичай в вигляді кривих чи таблиць.

Таблиця 1.4 – Рівні шумів, виміряні на частоті 1000 Гц

| Джерело шуму та місце його вимірювання | Рівень шуму, дБ (f = 1000 Гц) |
|---|---|
| Акустичні шуми зовні приміщень: | |
| Тихий сад | 20 |
| Тиха вулиця (без руху транспорту) | 30...35 |
| Звичайний середній шум на вулиці | 55...60 |
| Шумна вулиця без трамвайного руху | 60...75 |
| Трамвай на відстані 10...20 м | 80...85 |
| Тролейбус на відстані 5 м | 77 |
| Вантажний автомобіль в місті на відстані 10...20 м | 60...75 |
| Легковий автомобіль в місті на відстані 10...20 м | 50...65 |
| Електропоїзд на естакаді на відстані 6 м | 90 |
| Акустичні шуми в приміщеннях: | |
| Звичайний заклад, житлове приміщення | 40 |
| Шепіт на відстані 1 м | 20...25 |
| Спокійна розмова трьох осіб в кімнаті середнього розміру | 45...50 |
| Гучна музика по радіо | 80 |
| Розмова на відстані 1 м: | |
| Звичайна | 55...60 |
| Гучна | 65...70 |
| Гучна розмова по телефону | 55 |
| Шумні збори | 65...70 |
| Коридори | 35...40 |
| Бухгалтерія без відвідувачів | 30...35 |
| Шумна кімната | 40...50 |
| Тиха кімната | 25...30 |
| Кабінет за одного працюючого | 20...25 |

За формантною розбірливістю $A_Ф$ визначають складову W, словесну S, фразову розбірливість та зрозумілість мови. Залежність поміж формантною $A_Ф$ (сумарною ймовірністю приймання формант), складовою W та словесною S розбірливістю мови наведено в табл. 1.5.

Таблиця 1.5 – Залежність поміж формантною, складовою та словесною розбірливістю

| $A_Ф$, відн. ед. | S, % | W, % | $A_Ф$, відн. ед. | S, % | W, % |
|---|---|---|---|---|---|
| 0,05 | 5,0 | 30,0 | 0,55 | 84,0 | 98,5 |
| 0.10 | 15,0 | 63,0 | 0,60 | 87,0 | 98,8 |
| 0,15 | 26,0 | 76,0 | 0,65 | 90,0 | 99,0 |
| 0,20 | 36,0 | 85,0 | 0,70 | 92,5 | 99,2 |
| 0,25 | 46,0 | 90,0 | 0,75 | 95,2 | 99,4 |
| 0,30 | 54,0 | 93,0 | 0,80 | 96,5 | 99,6 |
| 0,35 | 62,5 | 94,5 | 0,85 | 98,0 | 99,7 |
| 0,40 | 69,0 | 96,0 | 0,90 | 99,0 | 99,8 |
| 0,45 | 75,0 | 97,0 | 0,95 | 99,5 | 99,9 |
| 0,50 | 80,0 | 98,0 | 1,00 | 100,0 | 100,0 |

Форманти звуків мови заповнюють весь частотний діапазон 150….7000 Гц.

Цей частотний діапазон поділяють на 20 смуг однакової розбірливості. Ймовірність виникнення формант в кожній смузі однакової розбірливості дорівнює 0,05.

При прослуховуванні мови в умовах шумів розбірливість є менше, аніж за їхньої відсутності.

Коефіцієнт W, який визначає це зменшення, називають коефіцієнтом сприймання або коефіцієнтом розбірливості, тобто в кожній смузі однакової розбірливості ймовірність приймання формант дорівнює

$$\Delta A = 0{,}05\ W. \qquad (1.4)$$

Коефіцієнт розбірливості W визначається рівнем відчуття формант:

$$ЕФ = ВР - ВШ, \qquad (1.5)$$

де: $B_Р$ – середній спектральний рівень мови,

$B_Ш$ – спектральний рівень шумів.

Для практики застосовування смуг однакової розбірливості є незручне, тому що діставанні частотні смуги є нестандартні.

Для кожної смуги однакової розбірливості коефіцієнт розбірливості W в загальному випадку буде різний, тому в акустичних вимірюваннях використовуються октавні або 1/3 – октавні частотні смуги.

Значення коефіцієнтів розбірливості мови W, відповідні певним рівням відчуття формант $E_ф$, наведено в табл. 1.6.

Зрозумілість мови, яка є фонетичною характеристикою розбірливості, визначається в перебігу звичайних телефонних переговорів для нетренованих спеціально абонентів.

При цьому зрозумілість вважається:

– відмінною, якщо переговори відбуваються без перепитувань;

– доброю, якщо виникають окремі перепитування слів, невідомих прізвищ, назв тощо, які рідко вживаються й про які не можна здогадатися за змістом;

– задовільною, якщо потрібно часткове перепитування і слухачі повідомляють, що важко розмовляти;

– гранично припустимою, якщо потрібне часткове перепитування одного й того ж самого матеріалу за передавання окремих слів по літерах з потужною напругою слухачів.

Таблиця 1.6 – Значення коефіцієнтів розбірливості W, відповідних певним рівням відчуття формант $E_Ф$

| $E_{Ф,}$ дБ | $W_3$, відн. од. | Еф, дБ | $W_3$, відн. од. | Еф, дБ | $W_3$, відн. од. |
|---|---|---|---|---|---|
| – 12 | 0,010 | -1 | 0,17 | 22 | 0,900 |
| – 11 | 0,015 | 0 | 0,20 | 23 | 0,915 |
| – 10 | 0,020 | 3 | 0,30 | 24 | 0,930 |
| – 9 | 0,030 | 6 | 0,40 | 25 | 0,945 |
| – 8 | 0,040 | 9 | 0,50 | 26 | 0,960 |
| – 7 | 0,050 | 12 | 0,60 | 27 | 0,970 |
| – 6 | 0,060 | 15 | 0,70 | 28 | 0,980 |
| – 5 | 0,075 | 18 | 0,80 | 29 | 0,985 |
| – 4 | 0,095 | 19 | 0,83 | 30 | 0,990 |
| – 3 | 0,110 | 20 | 0,86 | 33 | 0,995 |
| – 2 | 0,140 | 21 | 0,88 | 36 | 1,000 |

Градації зрозумілості мови й відповідні до них значення складової S та словесної W розбірливості, виміряні артикулянтами й доповнені значеннями формантної $A_Ф$ розбірливості (сумарної ймовірності приймання формант), взятої з табл. 1.5, наведено в табл. 1.7.

Таблиця 1.7 – Градації зрозумілості мови й відповідні до них значення формантної ($A_ф$), складової (S) та словесної (W) розбірливості

| Зрозумілість | Розбірливість | | |
|---|---|---|---|
| | формантна, $A_Ф$ | складова, S | словесна, W |
| Гранично припустима | 15....22 | 25....40 | 75....87 |
| Задовільна | 22....31 | 40....56 | 87....93 |
| Добра | 31....50 | 56....80 | 93....98 |
| Відмінна | 50 та вище | 80 та вище | 98 та вище |

Враховуючи, що сприймання людиною формант має властивість адитивності, тобто кожна ділянка мовного діапазону вкладає свій внесок в загальну розбірливість мови, можна обчислити внески октавних смуг для формантної розбірливості.

## 6 Порядок роботи з вимірювальним комплексом „Ореол-А”

Комплекс „Ореол-А” призначено для вимірювання акустичних та віброакустичних властивостей приміщення в смузі частот мовного сигналу.

Установлення комплексу здійснюється у відповідності зі схемою рис. 1.17.

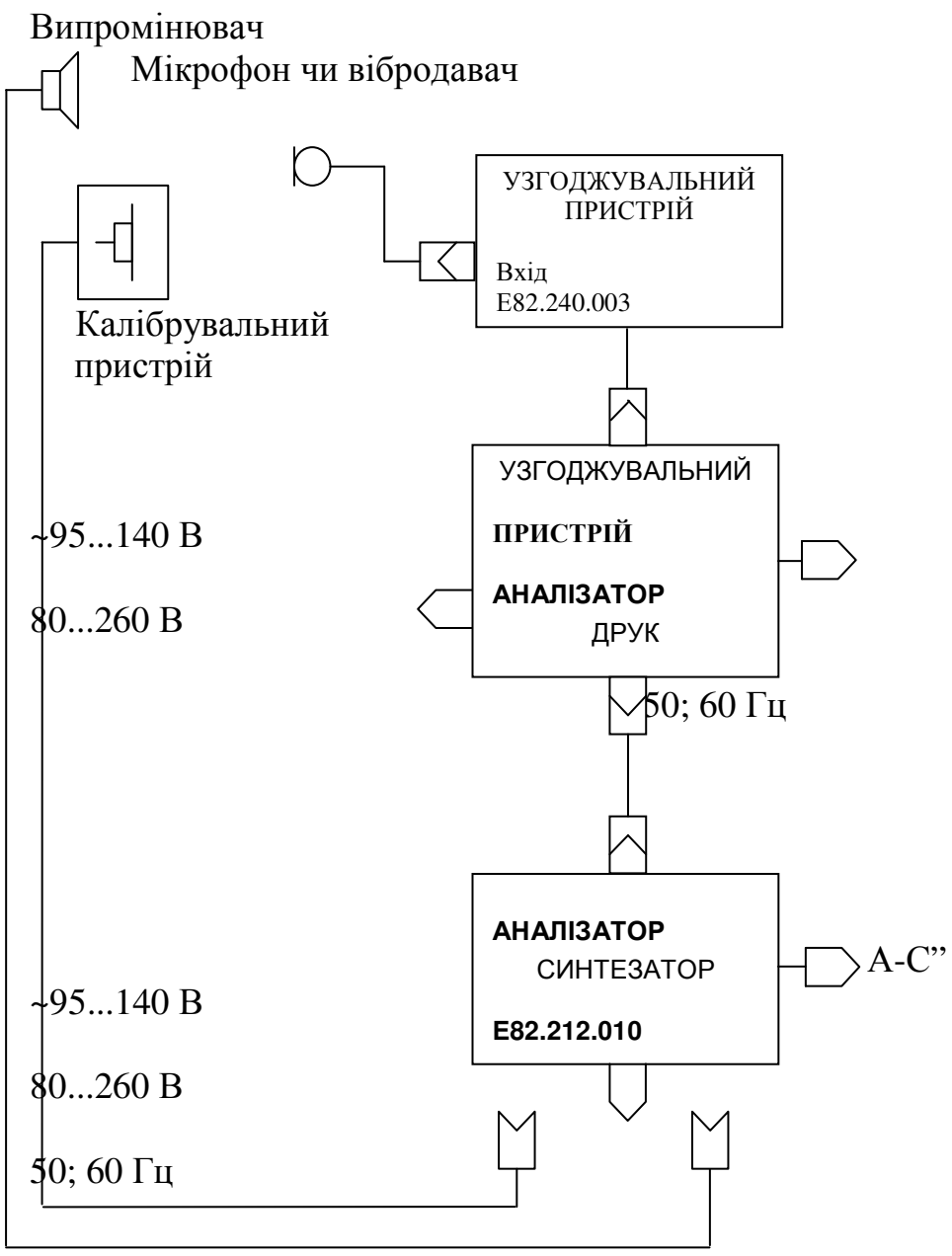



Рисунок 1.17 – Схема підмикання блоків комплексу „Ореол-А”

Друкувальний пристрій, зі необхідності, підмикається до розніму ДРУК аналізатора. До розніму ВИПРОМІНЮВАЧ синтезатора підімкніть калібрувальний пристрій. Підімкніть кабелі живлення аналізатора синтезатора до мережі електроживлення й переведіть тумблери вмикання в положення ВКЛ. При цьому на блоці синтезатора засвітиться світлодіод МЕРЕЖА, а на блоці аналізатора – світлодіод над клавішею АДАПТ і на індикаторі №

ВИМІРЮВАННЯ індикується «00». Час прогрівання приладу після ввімкнення має бути не менш за 5 хвилин.

Калібрування приладу:

Встановіть мікрофон у гніздо калібрувального пристрою і натисніть послідовно клавіші СКИДАННЯ та КАЛІБР. При цьому на індикаторі ЧАСТОТА індикується повідомлення СА, засвічується світлодіод ШУМ і звучить тестовий сигнал. Покази індикатора ВИМІРЮВАННЯ мають відповідати значенню (80+/–6) дБ. В противному разі регулюванням резистора МК, виведеного під шліц на пристрої, можна домогтися необхідного значення. Замість калібрувального пристрою до розніму ВИПРОМІНЮВАЧ синтезатора підімкнуть випромінювач.

Установіть мікрофон на кронштейні випромінювача. Натисніть клавіші СКИДАННЯ та КАЛІБР. Показ індикатора ВИМІРЮВАННЯ має відповідати (80+/–6) дБ. Після цього натисніть клавішу СКИДАННЯ.

Вибір режиму роботи визначається оператором виходячи з конкретних умов експлуатації комплексу. Більш оптимальним є адаптивний режим роботи, тому що вимірювання в цьому режимі здійснюється за коротший проміжок часу. Стаціонарний режим роботи використовується в разі, якщо неможливо забезпечити кабельний зв'язок поміж аналізатором та синтезатором.

### 6.1 Режим роботи – адаптивний

Вилучіть мікрофон з підтримувача випромінювача. Встановіть аналізатору такий спосіб, щоби забезпечити розміщення штатного давача в контрольній точці. Установіть давач. Для проведення вимірювання натисніть клавішу ПУСК. При цьому на індикаторі № ВИМІРЮВАННЯ індикується „01”, а решту індикаторів погашено. Після проведення вимірювання на індикаторі ЧАСТОТА з'являється повідомлення про частоту. У той самий момент часу вмикається світлодіод СКЛАД, а на індикаторі ВИМІРЮВАННЯ індикується значення складової розбірливості у відсотках.

Якщо в одній чи кількох частотних смугах формантна розбірливість дорівнює нулеві, то значення послаблення й відношення сигнал / шум у смугах можуть бути невірогідними, тобто виміряти рівень сигналу на високому рівні шумів вірогідно є неможливо.

Невірогідність значень відзначається переривчастою індикацією. Якщо невірогідність виявлено в кількох частотних смугах, переривчастою індикацією відзначається лише одна найнизькочастотна смуга. За чергового натискання на клавішу ПУСК на індикаторі № ВИМІРЮВАННЯ індикується порядковий номер виконуваного вимірювання. Після закінчення чергового вимірювання здійснюється індикація значення складової розбірливості. Клавіша ПУСК натискається стільки разів, скільки вимірювань поспіль потрібно виконати в даній контрольній точці, але не більш за вісім. Результати вимірювань виводяться на індикацію лише після виконання останнього вимірювання з усієї серії, а під час вимірювань індикується лише вимірювання, виконуваного в даний момент. Якщо поточне значення номера вимірювання дорівнює 34,

натискання клавіші ПУСК не призводить до виконання нового вимірювання. Для того щоб повторити якесь вимірювання з певним номером, необхідно клавішами «  » або « ! », що належать до групи № ВИМІРЮВАННЯ встановити номер вимірювання на одиницю менше за необхідний і натиснути клавішу ПУСК; при цьому попередні значення параметрів буде замінено на нові.

За зміни номера вимірювання зберігаються обрані за індикації попереднього вимірювання частотна смуга й параметр.

За необхідності виконання нової серії вимірювань виконується очищення пам'яті натисканням клавіш ПУСК та СИНХР одночасно.

### 6.2 Режим роботи – стаціонарний.

Після проведення калібрування для переведення комплексу до стаціонарного режиму роботи натисніть клавішу СТАЦ і здійсніть синхронізування шляхом натискання клавіші СИНХР.

Вимкніть кабель А – З від синтезатора.

УВАГА! Вимкнення кабелю хоча б одного з блоків призводить до блокування клавіші СИНХР. Синхронна робота комплексу забезпечується на протязі 1 години з моменту натискання клавіші СИНХР. Після закінчення зазначеного часу вмикається індикатор ЗРИВ. СИНХР, що сигналізує про необхідність повторення синхронізації.

Вимикання аналізатора з мережі не впливає на роботу схеми відліку часу.

Після проведення зазначених операцій блок аналізатора підготовлено до вимірювань, його може бути вимкнено з мережі і разом зі штатним давачем перенесено у піддаваному контролеві місці.

Після ввімкнення комплексу до мережі натисніть клавішу СТАЦ і виконайте вимірювання.

При виведенні результатів вимірювань на АЦПУ установіть на індикаторі клавішею «!», що належить до групи № ВИМІРЮВАННЯ, «00» і натисніть клавішу ВИСНОВОК. Під час друкування на індикатор № ВИМІРЮВАННЯ виводиться повідомлення «Pr» (Printer), а інші індикатори погашено. Вийти з режиму можна, натиснувши клавішу СКИДАННЯ. Якщо клавішею СКИДАННЯ не користуватися, то на АЦПК видаються результати з усіх виконаних вимірювань.

### 6.3 Методика виявлення акустичних та віброакустичних каналів

Аналізуючи канали витоку інформацій в обстежуваному приміщенні (акустика, віброакустика), слід визначити шляхи витоку інформації. Наприклад, до акустичних каналів можна віднести такі шляхи: двері, вікна, різноманітні технологічні, побутові отвори (вентиляція), різного роду ходи, тунелі – взагалі там, де акустичні коливання поширюються за межі КЗ із найменшим загасанням.

До віброакустичних каналів належать такі шляхи, де має місце перетворювання акустичних коливань на механічні з подальшим поширенням,

це: труби опалення, шини заземлення, вентиляція, скло у вікнах, стіни, підлога, стеля, комунікації, як відкриті, так і сховані в стіні під фальшстелею тощо.

Підготовка до проведення серії вимірювань переважно стосується лише комплексу „Ореол-А", за винятком того, що в приміщенні всі двері, вікна має бути зачинено, активні пристрої зашито (генератор просторового зашумлення з набором вібродавачів та випромінювачів) слід вимкнути, якщо такі є в наявності. Підготовка комплексу „Ореол-А" здійснюється у відповідності з пунктом «Порядок установки».

Що стосується вимірювань параметрів досліджуваного комплексом „Ореол-А" то його обладнання, закладені у приладі алгоритми опрацьовання даних побудовано у такий спосіб, що операторові, працюючому з комплексом „Ореол-А", буде вельми легко й швидко здійснити серію вимірювань з виявлення акустичних та віброакустичних каналів витоку інформації.

Методика вимірювання параметрів акустичного каналу полягає в так: виносний давач (мікрофон) розташовується за вікном чи то за дверима в найбільш імовірному місці витоку інформації, чи то по центру вікна чи дверей на відстані не більш за 1 м від досліджуваної поверхні. Щільно зачиняються двері (вікно) і провадяться вимірювання. Для більш об'єктивних результатів вимірювання провадяться кількаразово (два – п'ять разів), а при черговому вимірюванні випромінювач комплексу „Ореол-А" бажано розгорнути на третину кола (120 градусів). По закінченні вимірювань результати необхідно проаналізувати й обрати середнє значення. Найоптимальним є адаптивний режим роботи.

Методика вимірюваннння параметрів віброакустичного каналу полягає в такому: виносний вібродавач, попередньо закріпивши його в спеціальний щуп, ввімкнути до СУ замість мікрофона. Обстеження віброакустичного каналу розпочинають з батареї опалення. Щуп з давачем розташовується горизонтально на стояку (на трубі, а не на радіаторі). Місце з'єднання щупа з поверхнею труби має бути очищене (від фарби, іржі тощо) до металу. Ступінь натискання – середній. Також під час вимірювання щуп з давачем мають бути нерухомими, всілякі обертання, рухи слід виключити. Вимірювання провадять кількаразово (два – п'ять разів), а за черговому вимірювання, випромінювач комплексу „Ореол-А" бажано розгорнути на третину кола (120 градусів) для здобуття більш об'єктивних результатів. За необхідності також перевіряються вентиляція, шини заземлення, різні комунікації, підлога, стеля, стіни виходячи з конкретних умов експлуатації комплексу обирається режим роботи. Якщо неможливо забезпечити кабельний зв'язок поміж аналізатором та синтезатором, то використовується стаціонарний режим роботи.

Результати вимірювань зберігаються в енергонезалежній пам'яті. За бажання оператора результати можна вивести на індикатор, розташований на передній панелі, або на АЦПК через порт комп'ютера «COM-1» у вигляді таблиці з такими характеристиками:

– частота f, кГц;

– рівень шуму, дБ;

– відношення сигнал/шум, дБ;
– послаблення, дБ;
– формантна розбірливість, %;
– складова розбірливість, %.

Акустична та віброакустична захищеність оцінюється двома характеристиками: складова розбірливість, відношення сигнал/шум, він же є нормованим.

Якщо на частотах вище чи нижче за мовний діапазон (приблизно 5....3,0 кГц) відношення сигнал/шум виходить за межі норми, то вельми незначно, й ним можна знехтувати, тому що при розгляданні залежності спектральної густини потужності мовного сигналу від частоти видно, що спектральна складова на частоті вище чи нижче (0,5....3,0 кГц) має надто малий рівень і перебуває нижче за межу сприймання людського вуха.

## 7 Зміст протоколу лабораторної роботи

1 Назва лабораторної роботи.
2 Мета проведення роботи.
3 Схема вимірювання рівня захищеності об’єкта інформаційної діяльності від витоку інформації акустичним та віброакустичним каналами.
4 Таблиця результатів вимірювань.
5 Висновки.

## 8 Ключові запитання

1 Основні параметри мовного сигналу.
2 Визначення витоку інформації акустичним та віброакустичним каналами.
3 Різновиди розбірливості мови.
4 Які чинники впливають на розбірливість мови?
5 Означення октавних смуг.

## Лабораторна робота №7
## Захист ЦОВ від витоку інформації технічними каналами за рахунок ПЕМВН.

### 1 Мета роботи

Метою лабораторної роботи є:

- надання практичних навиків у визначенні потенційно-інформативних ПЕМВН від складових ПК;
- визначення їхнього енергетичного рівня;
- застосування різних заходів для зниження небезпеки перехоплення ПЕМВН.

### 2 Література

2.1 Савицький Л.Ю.., Кононович В.Г., Тардаскін М.Ф. Технічна експлуатація систем захисту інформації. Частина 1. Захист інформації по технічних каналах витоку. Навч. посібник/ За редакцією М.В. Захарченка. – Одеса: ОНАЗ, 2004. – С. 204.

2.2 ТР ЕОТ - 95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами ПЕМВН.

2.3 ТР ПЕМВН - 95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами ПЕМВН.

### 3 Основні положення

Центр обслуговування викликів – це спеціалізована телекомунікаційна система, що використовує технології побудови комп'ютерних мереж. Питання виникнення ПЕМВН у комп'ютері та захист від них є складною технічною проблемою, вирішенню якої в останній час приділяється підвищена увага.

**Побічні електромагнітні випромінювання і наведення (ПЕМВН)** — це паразитні електромагнітні випромінювання радіодіапазону, створені в навколишньому просторі пристроями, спеціальним образом для цього не призначеними.

Побічні електромагнітні випромінювання, що генеруються електронними пристроями, обумовлені протіканням струмів в їхніх електричних ланцюгах. Спектр ПЕМВН цифрового електронного обладнання являє собою сукупність гармонійних складових у деякому діапазоні частот.

Сукупність складового спектра ПЕМВН, породжувана протіканням струмів у ланцюгах, по яких передаються сигнали, що містять конфіденційну (таємну, комерційну і т.д.) інформацію, називають **потенційно-інформативними випромінюваннями і наведеннями (потенційно-інформативними ПЕМВН).**

Для персонального комп'ютера потенційно-інформативними ПЕМВН є випромінювання, формовані наступними ланцюгами:

- ланцюг, по якому передаються сигнали від контролера клавіатури до порту введення-виведення на материнській платі;
- ланцюг, по якому передається відеосигнал від відеоадаптера до електродів електронно-променевої трубки монітора;
- ланцюги, що формують шину даних системної шини комп'ютера;
- ланцюги, що формують шину даних усередині мікропроцесора, і т.д.

**Технічні засоби виявлення і виміру ПЕМВН.**

Для виявлення і виміру ПЕМВН використовуються спеціальна контрольно-вимірювальна апаратура – селективні радіоприймачі високого класу точності, що володіють змінюваною шириною пропущення радіотракту і різні режими виміру, що мають, у тому числі піковий. У комплекті з приймальними антенами дані приймачі є вимірювачами напруженості електромагнітного поля.

Використовуючи спеціальні методики виявлення, виміру і розрахунку, можна з впевненістю визначити рівень захищеності використовуваних ПК. У випадку невідповідності нормативним вимогам по заданому параметру, варто застосовувати організаційні, організаційно-технічні і технічні заходи для зниження небезпеки перехоплення ПЕМВН. До технічних засобів активного захисту відносяться широкополосні генератори шумового сигналу з відповідними антенними системами. Використання ПК у захищеному (екранованому) виконанні є застосуванням засобів пасивного захисту від розповсюдження ПЕМВН.

## 4 Домашнє завдання

4.1 Вивчити фізичні принципи виникнення побічних електромагнітних випромінювань у ПК і можливі заходи для зниження їхнього рівня.

4.2 Вивчити функціональний склад ПК і, керуючись характером оброблюваної на ПК інформації, визначити найбільш уразливі вузли.

4.3 Визначити перелік необхідних організаційних заходів, що знижують ризик перехоплення ПЕМВН.

## 5 Контрольні запитання

5.1 Які функціональні вузли персонального комп’ютера є найбільш потенційно важливими з точки зору характеру та технології обробки інформації?

5.2 Які загрози витоку інформації з ПК є найбільш ймовірними?

5.3 Які заходи необхідно провести на об’єкті ЕОТ, щоб виявити, оцінити можливі канали витоку інформації та зменшити ризик втрати інформації?

5.4 Які послуги інформації можуть бути скомпрометовані шляхом витоку інформації технічними каналами?

5.5 Що таке потенційно-інформативні ПЕМВН та які загрози інформації вони являють?

5.6 Які випадкові антени можуть бути розташовані на об'єкті ЕОТ, їхня класифікація?

5.7 Які заходи захисту витоку інформації шляхом наводок на випадкові антени необхідно виконувати на об'єкті ЕОТ?

5.8 Які існують вимоги для формування пошукового тестового сигналу від складових частин ПК?

5.9 Які існують вимоги для формування вимірювального тестового сигналу від складових частин ПК?

5.10 Які існують типи захисту від ПЕМВН, їхні переваги та недоліки?

5.11 В якому діапазоні частот випромінюють складові частини ПК?

5.12 Які складові частини потенційно-інформативного сигналу від ПК треба вимірювати?

5.13 Які технічні характеристики складових частин ПК найбільш впливають на спроможність перехоплення ПЕМВН?

5.14 Як потрібно розташовувати приймальну антену відносно ПК і чому саме так?

5.15 Які вимоги існують до вимірювальної апаратури? Чим вони відрізняються від вимог до перехоплювальної апаратури?

5.16 Які технічні засоби треба встановлювати у кола випадкових антен? Загальні вимоги для цих засобів.

5.17 Що визначає поняття „контрольована зона" відповідно загрозам витоку інформації технічними каналами?

5.18 Як впливає на рівень потенційно-інформативного сигналу від ПК розташування в приміщенні інших ПК?

5.19 Які шляхи екранування можливо використати на об'єкті ЕОТ?

5.20 Який державний орган уповноважений здійснювати контроль за станом захисту інформації в АС, що оброблюють державну ІзОД?

5.21 Вимоги яких нормативних документів встановлюють порядок та об'єм робіт з питань ТЗІ на об'єктах обчислювальної техніки?

## 6 Лабораторне завдання

6.1 Виконати завантаження системи, а потім завантажити з дискети тестову програму *grtstm.exe* р з параметрами: частота тестового сигналу – 0,5 Гц; тип контролера – VGA; розмір зображення – 640x400 точок.

6.2 Увімкнути селективний мікровольтметр SMV-8.5. Дати прогрітися апаратурі 10-15 хвилин.

6.3 Підключити до мікровольтметра SMV-8.5 антенний кабель, а до того підключити антену DP-1.

6.4 Встановити органи управління мікровольтметра SMV-8.5 в початковий стан.

6.5 Встановити пошуковий режим тестового сигналу натиснувши послідовно на клавіатурі F4, F3.

6.6 Знайти тестовий сигнал з монітора, змінюючи частоту прийому органами управління мікровольтметра SMV-8.5.

6.7 Знайти такий напрям положення антени DP-1 від монітора, в якому сигнал буде найбільший.

6.8 Розташувати антену DP-1 на відстані 1 метр від монітора, це положення повинно бути сталим.

6.9 За допомогою вимірювальної лінійки встановити такий розмір диполя, що відповідає частоті знайденого сигналу.

6.10 За допомогою атенюаторів вимірюваного сигналу, встановити такий його рівень, що дозволяє провести найбільш точніше вимірювання.

6.11 Встановити режим тестового сигналу - виміру інформативної складової, натиснувши на клавіатурі F1.

6.12 Провести вимір тестового сигналу та записати результат у бланк вимірів.

6.13 Встановити режим тестового сигналу - виміру рівня завади, натиснувши на клавіатурі F2.

6.14 Провести вимір рівня завадової складової та записати результат у бланк вимірів.

6.15 Перейти до п. 6.5 і, змінюючи частоту прийому органами управління мікровольтметра SMV-8.5, виконуючи послідовно п.п. 6.6 – 6.14, провести вимір тестового сигналу у діапазоні 26 МГц – 300 МГц.

6.16 Змінити приймальну антену, встановивши антену DP-3.

6.17 Провести вимір тестового сигналу у діапазоні 300 МГц – 1000 МГц аналогічно вимогам п. 6.15.

6.18 На будь-якій частоті знайденого тестового сигналу, віддаляючи антенну DP-1 від монітора на деяку відстань, переконатись, що сигнал з віддаленням слабшає, що є доказом можливості простими організаційними заходами зменшити ризик перехоплення ПЕМВН від ПК.

Таким же чином знайти та провести вимірювання тестового сигналу від ПК, його електричній та магнітній складових у діапазоні 10 КГц – 30 МГц за допомогою мікровольтметра SMV-11 та антенного комплексу FMA- 11.

## 7 Опис лабораторного макета

7.1 На ПК, що належить дослідженню на виток інформації шляхом ПЕМВН, встановлюється тестова програма *grtstm.exe*, що запускається в режимі сумісності з MS-DOS.

7.2 До складу вимірювальної апаратури входять:

- селективний мікровольтметр SMV-8.5, коаксіальний ВЧ-кабель LE 60, антени DP-1 та DP-3, струмові пробники ТК- 11 та ТК-12;
- селективний мікровольтметр SMV-11, коаксіальний ВЧ-кабель LE 112, антенний комплекс FMA- 11 з антенами.

7.3 Перед проведенням вимірювань мікровольтметри SMV-8.5 та SMV-11 повинні буди підключеними до системи захисного заземлення, електроживлення слід подавати через мережний фільтр типу М-17 або ФСП-1.

## Додаток. Селективний мікровольтметр і вимірювач завад напруг SMV- 8,5

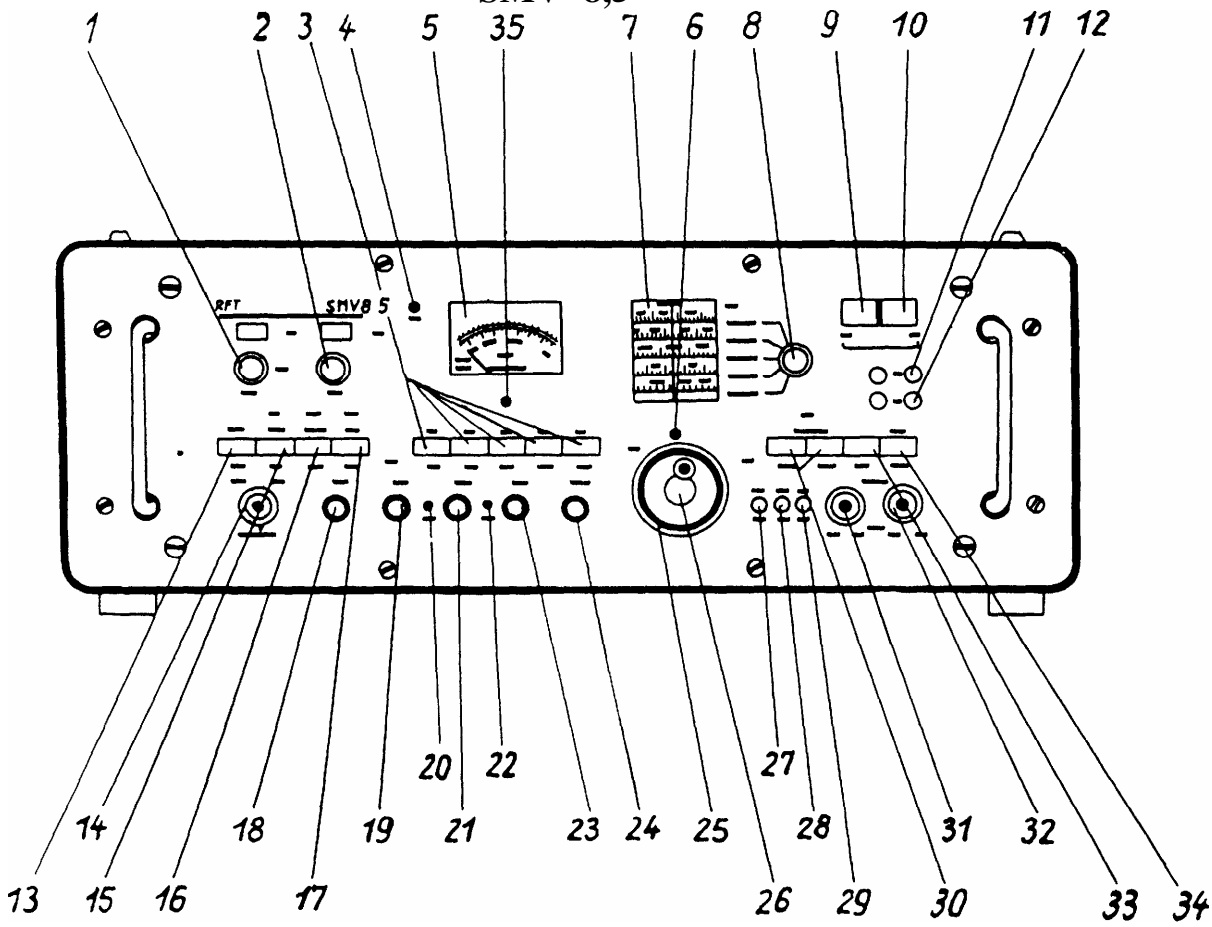



Рисунок 1.18 – Селективний мікровольтметр і вимірювач завад напруг SMV- 8,5 (вид спереду ).

Таблиця № 1.8 Пояснення органів управління і символів на рис. 1.18

| Поз. | Позначення | Примітка |
|---|---|---|
| (1) | Дільник напруги ВЧ | Від 0 до 60 дБ., (ступенями по 10 дБ.) |
| | Калібровка частоти | На вхід приймача подаються частотні мітки 5 мГц або 20 мГц |
| (2) | Дільник напруги ПЧ | Від 0 до 55 дБ., (ступенями по 5 дБ) |
| (3) | Перемикач виду робіт | Індикаторний прилад показує при не натиснутих кнопках працюючу напругу приладу |
| | Калібровка 1 | Кнопка натиснута: індикатор показує напругу калібровочного генератора |
| | Вимірювання середнього значення АМ сигналів , | Межа відліку 20 дБ |
| | Вимірювання пікового значення АМ-сигналів | |
| | Вимірювання квавазипікового значення імпульсних напруг | Квазипікова характеристика відповідно вимогам МСКР |

| | | |
|---|---|---|
| | Вимірювання середнього значення АМ-сигналів | Межа відліку 40 дБ.. |
| (4 ) | Лампа індикації настройки | Працює тільки при ширині смуги частот 120 кГц ( кнопки ( 30 ) не натиснугі); не працює при живленні від батареї 12 В. |
| (5) | Індикаторний прилад | Верхня шкала: межа відліку 20 дБ, нижня шкала: межа відліку 40 дБ.. |
| (6) | Гвинт для корекції візерної лінії | |
| (7) | Шкала частот | |
| (8) | Перемикач поддіапазонів частот | |
| (9) | Вимикач мережі | Прилад працює з живлення від мережі або від батареї 16-30 В.. |
| (10) | Вимикач батареї | Прилад працює з живлення від батареї 12 В.. Кнопки ( 9 ) і ( 10 ) натиснугі. Зарядка зовнішньої батареї 15 В. від мережі. |
| (11) | Вихід головного телефона | Для підключення головного телефона або гучнрмовця. |
| (12) | Вихід самописця | Для підключення самописця або другого індикаторного приладу |
| (13) | Перемикач " Вимірювання-калібровка " | Кнопка не натиснута: калібровка, приймач з єднан з калібровочним генератором<br>Кнопка натиснута: вимірювання, приймач з єднан з вхідним гніздом. |
| (14) | Вхід приймача | |
| (15) | Калібровка підсилення | Кнопка не натиснута: калібровка вручну за допомогою регулятора (21)<br>Кнопка натиснута: автоматична калібровка підсилення. |
| (16) | Частотні мітки | Кнопка не натиснута: 20 мГц<br>Кнопка натиснута: 5 мГц |
| (17) | Автоматична підстройка частоти | Кнопка не натснута: АПЧ приймача на припустиму частоту<br>Кнопка натиснута: АПЧ калібровочного генератора на припустиму частоту |
| ( 18) | Регулятор гучності | |
| (19) | Регулятор компенсаційної напруги | Для вимірювання пікового значення АМ-сигналів. |
| (20) | Електрична нульова точка | При виду робіт "QP" для корекції нульової точки індикаторного приладу. |
| (21 ) | Регулятор калібровки підсилення | Для установки підсилення приймача вручну. |
| (22) | Регулятор корекції | Корекція автоматичної |

| | | |
|---|---|---|
| | калібровки підсилення | калібровки підсилення. |
| (23) | Регулятор калібровки 1 | Для установлення напруги калібровочного генератора. |
| (24) | Підстройка генератора | Для підстройки частоти калібровочного генератора. |
| (25) | Точна настройка приймача | |
| (26) | Груба настройка приймача | |
| (27) | Вихід для підключення осцилографа. | |
| (28) | Вихід для подачі напруги коливання | Коливання частоти 3-го гетеродина приймача |
| (29) | Вихід прміжної частоти | 3-яПЧ,г=1,67мГц. |
| (30) | Перемикач ширини смуги частот | Кнопки " 20 кНг " і" 1 кНг " не натснутп: ширина смуги частот 120 кГц |
| | Перемикач ширини смуги частот | Кнопка натиснута: ширина смуги 20 кГц, індикаторна лампа не горить<br>- якщо кнопка (15) знаходиться |
| | | в положенні " V ", то |
| | Перемикач смуги частот | відключений генератор НЧ для АПЧ калібровочного генератора,<br>-якщо кнопка (15) знаходиться в положенні " V ", то<br>включена ширина смуги частот 120 кГц<br>Кнопка натиснута: ширина смуги частот 1 кГц, індикаторна лампа настройки ( 4 ) не горить |
| (31) | Вихід калібровочного генератора | Від 26 мГц до 300 мГц |
| (32) | Вихід калібровочного генератора | Від 300мГц до 1000 мГц |
| (33) | Вимикач калібровочного генератора | Кнопка натиснута: генератор включений, пристрій для прослухання не працює. |
| (34) | Перемикач виду демодуляції | Кнопка не натиснута: детектирование АМ-сигналів,<br>Кнопка натиснута: детектирование ЧМ-сигналів, індикаторна лампа настройки (4 ) не горить. |
| (35) | Механічна корекція нульової точки індикаторного приладу | |

## Лабораторна робота №8
## Захист серверних від витоку інформації технічними каналами за рахунок ПЕМВН та несанкціонованого доступу до обладнання серверних.

### 1 Мета роботи

Метою лабораторної роботи є:

- реалізація заходів захисту від несанкціонованого доступу до обладнання серверних;
- застосування різних заходів для зниження небезпеки перехоплення ПЕМВН;
- надання практичних навиків у визначенні потенційно-інформативних ПЕМВН від складових ПК;
- визначення їхнього енергетичного рівня.

### 2 Література

2.1 Савицький Л.Ю.., Кононович В.Г., Тардаскін М.Ф. Технічна експлуатація систем захисту інформації. Частина 1. Захист інформації по технічних каналах витоку. Навч. посібник/ За редакцією М.В. Захарченка. – Одеса: ОНАЗ, 2004. – С. 204.

2.2 ТР ЕОТ - 95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами ПЕМВН.

2.3 ТР ПЕМВН - 95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами ПЕМВН.

### 3 Основні положення

Побічні електромагнітні випромінювання і наведення (ПЕМВН) — це паразитні електромагнітні випромінювання радіодіапазону, створені в навколишньому просторі пристроями, спеціальним чином для цього не призначеними.

Побічні електромагнітні випромінювання, що генеруються електронними пристроями, обумовлені протіканням струмів в їхніх електричних ланцюгах. Спектр ПЕМВН цифрового електронного обладнання являє собою сукупність гармонійних складових у деякому діапазоні частот.

Сукупність складового спектра ПЕМВН, породжувана протіканням струмів у ланцюгах, по яких передаються сигнали, що містять конфіденційну (таємну, комерційну і т.д.) інформацію, називають потенційно-інформативними випромінюваннями і наведеннями (потенційно-інформативними ПЕМВН).

Для персонального комп'ютера потенційно-інформативними ПЕМВН є випромінювання, формовані наступними ланцюгами:

- ланцюг, по якому передаються сигнали від контролера клавіатури до порту введення-виведення на материнській платі;

- ланцюг, по якому передається відеосигнал від відеоадаптера до електродів електронно-променевої трубки монітора;
- ланцюги, що формують шину даних системної шини комп'ютера;
- ланцюги, що формують шину даних усередині мікропроцесора, і т.д.

## 4 Організаційні заходи захисту серверних

4.1 Установчим наказом керівника організації повинні бути призначені відповідні за вівідування приміщень серверних сторонніми особами, за виконання правил протипожежної охорони та ін. Повинен вестися журнал виконаних у приміщенні робіт.

4.1 Для запобігання несанкціонованого доступу до приміщень серверних ці приміщення повинні бути обладнані системою охорони з трьома незалежними рубежами охоронної сигналізації;

- на дверях;
- на вікнах;
- об’ємна сигналізація.

Ця сигналізація повинна бути виведена до центрального пульту в приміщенні охорони та мати контрольний монітор на території управління телекомунікаційних систем (чергової служби).

4.2 Для обмеження доступу усі двері службових приміщень повинні бути обладнані автоматизованою системою доступу або кодовими замками.

4.3 Якщо серверна має вікна, вони повинні бути обладнані залізними ставнями або ролетами.

## 5 Технічні вимоги до приміщень серверних

5.1 Для запобігання витоку інформації через електромагнітні випромінювання приміщення для розміщення серверних повинні мати екрановані стіни (коефіцієнт екранування не менше 20 дБ в діапазоні частот 0,1 - 1000 МГц по електричній складовій та діапазоні 0,1-30 МГц по магнітній складовій.

5.2 Для запобігання витоку інформації через наводи усі кабелі локальної мережі телекомунікації повинні бути екранованими. Введення кабелів і проводів необхідно виконувати через металеві короби чи труби з поперечним розміром не більше 50 мм та довжиною не менше трьох метрів, які повинні уварюватися в екран приміщення по всьому периметру вводу. Якщо ці заходи не забезпечують необхідний коефіцієнт екранування, використовують, мережеві лінійні фільтри.

5.3 Для запобігання витоку інформації внаслідок взаємних наводів, кабелі окремих систем (пакети кабелів) повинні мати взаємну відстань не менше 20 см.

При використанні в серверних спеціальних меблів, в яких є монтажний жолоб для прокладки кабелів (телефон, мережа змінного струму, інші кабелі),

звертайте увагу на недопущення паралельного пробігу на малій відстані кабелів окремих систем.

5.4 Для запобігання можливості зняття інформації з системи заземлення вона повинна мати загальний опір не більше 0,5 Ом та не мати виходів за межі контрольованої зони. Рекомендується для цього мати окремий контур заземлення, до якого підключаються лише абоненти серверних.

5.5 Для екранування вентиляційних каналів можна встановлювати на вхідних-вихідних отворах системи вентиляції екрануючу сітку з вічком 6х6 мм, яка повинна мати надійний електричний контакт з металевим коробом вентиляційного каналу по всьому периметру (зварювання або пайка). Краще для цього використати хвилеводну стільникову решітку, яка зварюється з металевих кутиків з розміром вікна А не більше 50 мм та висотою "хвилевода" 2А.

5.6 Трубопроводи водяного охолодження і опалення в місцях входу в екрановане приміщення повинні мати з екраном приміщення хороший електричний контакт з допомогою приварки по всьому периметру. В місцях вводу в екрановане приміщення неметалевих труб (наприклад. поліетиленових труб кондиціонерів, систем заволоження повітря) встановлюються металеві патрубки діаметром не більше 50 мм і довжиною не менше двох діаметрів (так звані хвилевидні патрубки), які уварюються в екран приміщення по периметру.

## 6 Екранування приміщень

6.1 Екранування стін, стелі та підлоги приміщення може виконуватись за допомогою листів сталі (Ст.3 чи Ст.20) чи оцинкованого заліза товщиною від 0,5 до 3 мм. З'єднання сталевих листів виконується внапуск зварюванням по всій довжині безперервним швом. Величина напуску повинна бути не менше за 10 мм.

Перед монтажем екрану поверхню стін бажано вирівняти по вертикалі. З метою зменшення кількості швів зварювання доцільно використати листи самого великого розміру, які є в наявності. Для спрощення зварювання екран можна зварювати фрагментами на підлозі.

Для попередження корозії зварні шви бажано захистити фарбуванням оліфою чи кузбаслаком. Перед штукатуркою на екран закріплюється штукатурна сітка, або елементи кріплення сухої штукатурки.

Для екранування можна використовувати жерсть, з'єднану фальцем з наступною пропайкою місць з'єднання безперервним швом. Також допускається використовувати металеву сітку, яка має електричні з'єднання (зварювання) у всіх перетинах дротів, з розміром вічка не більше 6х6 мм. З'єднання окремих полотен сітки повинно виконуватися безперервним швом, або в окремих точках з максимально допустимими проміжками між точками з'єднання 10 мм. Не допускається для екранування стін, стелі та підлоги використовувати сітку «Рабиця». Також не рекомендується використовувати для екранування радіотканину РН-3, так як вона не забезпечує потрібний коефіцієнт екранування на низьких частотах (0,15 - 400 Мгц) та практично не екранує магнітну складову поля.

6.2 Екранування дверних прорізів виконується за допомогою одинарних металевих дверей. Основне призначення дверей – забезпечення надійного екранування приміщень серверних від витоків електромагнітного випромінювання. Це вирішується за рахунок виготовлення металевих дверей та забезпечення надійного електричного контакту дверей з дверною коробкою по всьому периметру прилягання дверей. Виходячи з цього, поверхні прилягання повинні мати надійний в часі електричний контакт по всьому периметру. При виготовлені дверей забороняється фарбувати поверхні, що призначені для електричного контакту. Коробка дверей виготовляється з металевих кутиків, які зварені між собою. При цьому потрібно забезпечити паралельність дверної коробки в площині, що забезпечить в майбутньому надійний контакт з дверима.

По всьому контуру прилягання дверей на дверній коробці прокладається металева полоса із нержавіючої сталі товщиною 2-3 мм, яка кріпиться до добре зачищеної поверхні коробки гвинтами, відстань між якими не повинна перевищувати 50 мм, і яка служить для електричного контакту з контактним пристроєм дверей.

Двері також зварюються з кутиків, які обшиваються сталевими листами товщиною від 0,5 до 3 мм, які зварені безперервним швом.

Для забезпечення надійного і електричного контакту дверей з коробкою по всьому периметру дверей встановлюються контактні пристрої, які можуть бути двох типів:

- гребінчасті контакти з пружного матеріалу товщ. 0,3 - 0,5 мм, наприклад з берилієвої бронзи;

- екрануюче обплетення з кабеля, сріблене або луджене, всередину якого вставлено гумовий джгут діаметром приблизно 15мм.

Для забезпечення надійного прилягання дверей, вони обладнуються замковим пристроєм (наприклад ригельного типу), який притискує двері до контактної планки коробки. Висота та ширина дверей вибираються згідно з типом обладнання, що використовується.

6.3 Екрани віконних прорізів використовують таких типів: металеві сітчасті штори з вічком не більше 6х6 мм, які мають електричні з'єднання (зварювання) у всіх перетинах дротів, металеві ставні з листової сталі, хвилевідні стільникові решітки. Останні з естетичних міркувань можна виготовити не лише з елементів квадратного перерізу, а, наприклад, з відрізків труб, обов'язково забезпечуючи при цьому зварення сусідніх елементів по всій довжині безперервним швом. Методи виконання екрану та забезпечення його електричного контакту по всьому периметру з коробкою для віконних прорізів такі ж, як і для дверних. Якщо екран складається з двох стулок, то між ними також по всій довжині повинен бути забезпечений електричний контакт.

## 7 Рекомендації по вибору та встановленню фільтрів

7.1 Мережеві та лінійні фільтри використовують тоді, коли після проведення робіт по екрануванню приміщення та проведення вимірів, отриманий коефіцієнт екранування менше 20 дБ.

Фільтри вибираються в залежності від призначення електричних кіл, що проходять через них. При цьому необхідно враховувати тип струму (постійний або змінний), його частоту, напругу, величину струму, необхідне робоче затухання-в заданому діапазоні частот.

7.2 Фільтри рекомендується встановлювати із зовнішньої сторони екранованого приміщення поблизу місця введення електричних проводів, але якщо це неможливо, фільтри можна встановити всередині екранованого приміщення. Електричні проводи між фільтром і екраном приміщення укладаються в екрануючу конструкцію (обплетення або металева труба), яка з'єднана як з фільтром, так і з екраном по всьому периметру.

7.3 Для вводу силових мереж можна використовувати мережеві фільтри типу ФПС, ФП, Ф-002, Ф-010, ФСП-1, або їм подібні. Для телефонних мереж використовують фільтри типу ФПТ (ФПТ-1-12-0,25- 250/127), ФПУ.2, «Контакт 15» або їм подібні. Для ланцюгів радіооповіщення можна використовувати фільтри типу ФПУ-3-5-5 00-220, або аналогічні.

## 8 Технічні засоби виявлення і вимірювання ПЕМВН

8.1 Для виявлення і вимірювання ПЕМВН використовуються спеціальна контрольно-вимірювальна апаратура – селективні радіоприймачі високого класу точності, що мають змінювану ширину пропущення радіотракту і різні режими вимірювань, у тому числі піковий. У комплекті з приймальними антенами дані приймачі є вимірювачами напруженості електромагнітного поля.

8.2 Використовуючи спеціальні методики виявлення, вимірювання і розрахунку, можна з впевненістю визначити рівень захищеності використовуваних ПК. У випадку невідповідності нормативним вимогам по заданому параметру, варто застосовувати організаційні, організаційно-технічні і технічні заходи для зниження небезпеки перехоплення ПЕМВН. До технічних засобів активного захисту відносяться широкополосні генератори шумового сигналу з відповідними антенними системами. Використання ПК у захищеному (екранованому) виконанні є застосуванням засобів пасивного захисту від розповсюдження ПЕМВН.

8.3 Приміщення, де розміщене технологічне обладнання, телекомунікаційні системи та лінійно-кабельні мережі, повинні задовольняти відповідним технічним вимогам. Зокрема вони повинні мати контрольовану зону не менше 10м. Під контрольованою зоною розуміється зона, куди заборонений доступ сторонніх осіб (або передбачене контрольоване перебування сторонніх осіб).

Нові приміщення серверних та електронної пошти, що проектуються та будуються, не повинні мати вікон. По можливості, приміщення серверних розміщують у внутрішній частині будівлі, або із сторони внутрішнього двору.

## 9 Домашнє завдання

9.1 Вивчити фізичні принципи виникнення побічних електромагнітних випромінювань у ПК і можливі заходи для зниження їхнього рівня.

9.2 Вивчити функціональний склад ПК і, керуючись характером оброблюваної на ПК інформації, визначити найбільш уразливі вузли.

9.3 Визначити перелік необхідних організаційних заходів, що знижують ризик перехоплення ПЕМВН.

## 10 Контрольні запитання

10.1 Які функціональні вузли персонального комп'ютера є найбільш потенційно важливими з точки зору характеру та технології обробки інформації?

10.2 Які загрози витоку інформації з ПК є найбільш ймовірними?

10.3 Які заходи необхідно провести на об'єкті ЕОТ, щоб виявити, оцінити можливі канали витоку інформації та зменшити ризик втрати інформації?

10.4 Які послуги інформації можуть бути скомпрометовані шляхом витоку інформації технічними каналами?

10.5 Що таке потенційно-інформативні ПЕМВН та які загрози інформації вони являють?

10.6 Які випадкові антени можуть бути розташовані на об'єкті ЕОТ, їхня класифікація?

10.7 Які заходи захисту витоку інформації шляхом наводок на випадкові антени необхідно виконувати на об'єкті ЕОТ?

10.8 Які існують вимоги для формування пошукового тестового сигналу від складових частин ПК?

10.9 Які існують вимоги для формування вимірювального тестового сигналу від складових частин ПК?

10.10 Які існують типи захисту від ПЕМВН, їхні переваги та недоліки?

10.11 В якому діапазоні частот випромінюють складові частини ПК?

10.12 Які складові частини потенційно-інформативного сигналу від ПК треба вимірювати?

10.13 Які технічні характеристики складових частин ПК найбільш впливають на спроможність перехоплення ПЕМВН?

10.14 Як потрібно розташовувати приймальну антену відносно ПК і чому саме так?

10.15 Які вимоги існують до вимірювальної апаратури? Чим вони відрізняються від вимог до перехоплювальної апаратури?

10.16 Які технічні засоби треба встановлювати у кола випадкових антен? Загальні вимоги для цих засобів.

10.17 Що визначає поняття „контрольована зона” відповідно загрозам витоку інформації технічними каналами?

10.18 Як впливає на рівень потенційно-інформативного сигналу від ПК розташування в приміщенні інших ПК?

10.19 Які шляхи екранування можливо використати на об’єкті ЕОТ?

10.20 Який державний орган уповноважений здійснювати контроль за станом захисту інформації в АС, що оброблюють державну ІзОД?

10.21 Вимоги яких нормативних документів встановлюють порядок та об’єм робіт з питань ТЗІ на об’єктах обчислювальної техніки?

## 11 Лабораторне завдання

11.1 Виконати завантаження системи, а потім завантажити з дискети тестову програму *grtstm.exe* р з параметрами: частота тестового сигналу – 0,5 Гц; тип контролера – VGA; розмір зображення – 640x400 точок.

11.2 Увімкнути селективний мікровольтметр SMV-11. Дати прогрітися апаратурі 10-15 хвилин.

11.3 Підключити до мікровольтметра SMV-11 антенний кабель, а до того підключити електричну антену.

11.4 Встановити органи управління мікровольтметра SMV-11 в початковий стан.

11.5 Встановити пошуковий режим тестового сигналу натиснувши послідовно на клавіатурі F4, F3.

11.6 Знайти тестовий сигнал з монітора, змінюючи частоту прийому органами управління мікровольтметра SMV-11.

11.7 Знайти такий напрям положення антени FMA-11 від монітора, в якому сигнал буде найбільший.

11.8 Розташувати антену FMA-11 на відстані 1 метр від монітора, це положення повинно бути сталим.

11.9 За допомогою атенюаторів вимірюваного сигналу, встановити такий його рівень, що дозволяє провести найбільш точніше вимірювання.

11.10 Встановити режим тестового сигналу - виміру інформативної складової, натиснувши на клавіатурі F1.

11.11 Провести вимір тестового сигналу та записати результат у бланк вимірів.

11.12 Встановити режим тестового сигналу - виміру рівня завади, натиснувши на клавіатурі F2.

11.13 Провести вимір рівня завадової складової та записати результат у бланк вимірів.

11.14 Перейти до п. 6.5 і, змінюючи частоту прийому органами управління мікровольтметра SMV-11, виконуючи послідовно п.п. 6.6 – 6.13, провести вимір тестового сигналу у діапазоні 9 kГц – 26 МГц.

11.15 Змінити приймальну антену, встановивши магнітну антену.

11.16 Провести вимір тестового сигналу у діапазоні 9 kГц – 26 МГц аналогічно вимогам п. 6.15.

11.17 На будь-якій частоті знайденого тестового сигналу, віддаляючи антенну від монітора на деяку відстань, переконатись, що сигнал з віддаленням слабшає, що є доказом можливості простими організаційними заходами зменшити ризик перехоплення ПЕМВН від ПК.

Таким же чином знайти та провести вимірювання тестового сигналу від ПК, його електричній та магнітній складових у діапазоні 26 МГц – 1000 МГц за допомогою мікровольтметра SMV-8,5 та антен DP-1, DP-3. Роботу з мікровольтметром SMV-8,5 розглянуто у попередній лабораторній роботі.

## 12 Опис лабораторного макета

12.1 На ПК, що належить дослідженню на виток інформації шляхом ПЕМВН, встановлюється тестова програма *grtstm.exe*, що запускається в режимі сумісності з MS-DOS.

12.2 До складу вимірювальної апаратури входять:

- селективний мікровольтметр SMV-8.5, коаксіальний ВЧ-кабель LE 60, антени DP-1 та DP-3, струмові пробники ТК- 11 та ТК-12;
- селективний мікровольтметр SMV-11, коаксіальний ВЧ-кабель LE 112, антенний комплекс FMA- 11 з антенами.

12.3 Перед проведенням вимірювань мікровольтметри SMV-8.5 та SMV-11 повинні буди підключеними до системи захисного заземлення, електроживлення слід подавати через мережний фільтр типу М-17 або ФСП-1.

## Додаток. Селективний мікровольтметр і вимірювач завад напруг SMV- 11

Зовнішній вигляд педньої панелі селективного мікровольтметра показано на рис. 1.19. Органи управління мають таке призначення:

1 -

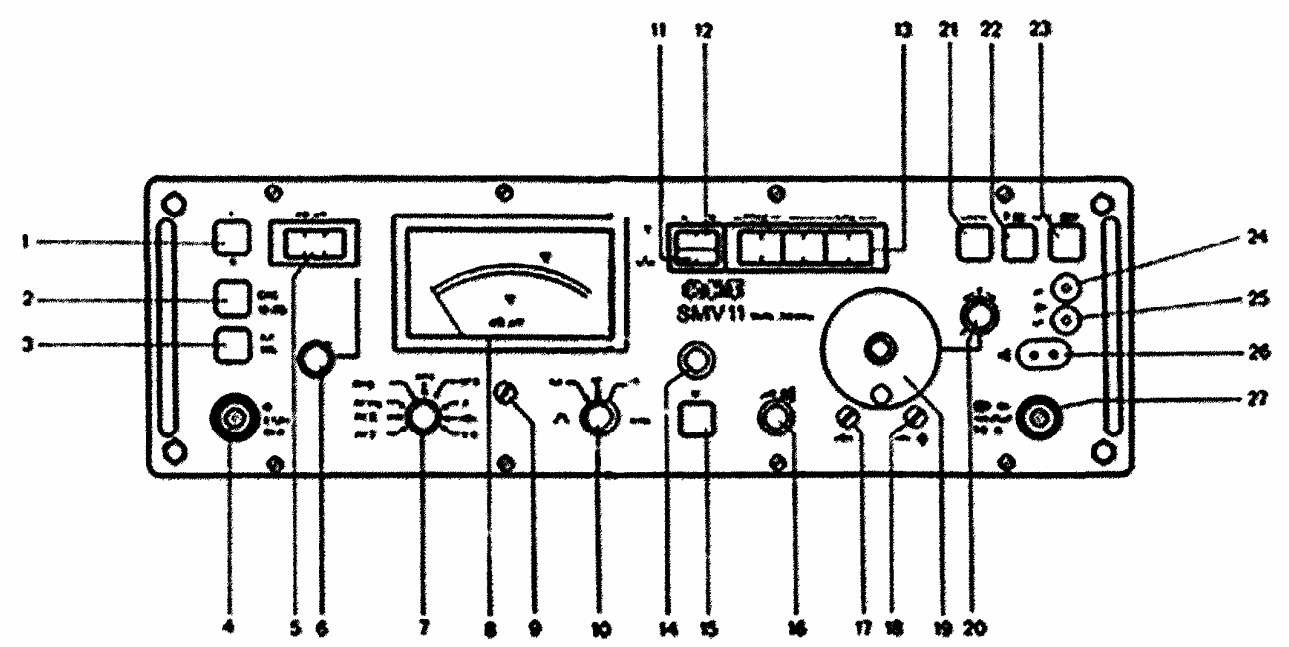



Рис. 1.19 Селективний мікровольтметр і вимірювач завад напруг SMV- 11 (вид спереду )

# Глава 2
# Системи розпізнавання на базі біометричних даних

## 2.1. Основні поняття про біометрію

Слово біометрія має грецьке походження - "bio" - життя, "metron" - вимірювання. Саме поняття "біометрія" з'явилося наприкінці дев'ятнадцятого століття і має на увазі розділ науки, що займається кількісними біологічними експериментами з залученням методів математичної статистики. Наприкінці двадцятого століття інтерес до біометрії значно зріс завдяки тому, що ця галузь науки знайшла своє застосування в розробках нових технологій безпеки, суть яких зводиться до використання комп'ютерних систем розпізнавання особистості за унікальним генетичним кодом людини.

Фізіологічні особливості, наприклад, такі, як папілярний візерунок пальця, геометрія особи, температура шкіри обличчя, модель райдужної оболонки ока, геометрія долоні, сітківка ока, структура ДНК, форма вуха, характеристики клавіатурного набору, особливості підпису та багато інших є постійними і незмінними характеристиками людини. Ваш голос відкриває двері будинку, де ви живете, модель райдужної оболонки ока дозволяє пройти в офіс знайомої вам компанії, відбиток вашого пальця відкриває доступ до комп'ютерної системи. Таким чином, ви самі є ключем.

### 2.1.1 Біометричні характеристики людини

Біометричні характеристики людини називається його вимірювана фізична характеристика або персональна поведінкова риса. Ідентифікація людини реалізується в процесі перевірки БХЛ на ідентичність зареєстрованому користувачеві.

Перелічимо основні біометричні характеристики людини, за допомогою яких здійснюється їх ідентифікація:

- відбитки пальців;
- форма і геометрія обличчя;
- форма і будова черепа;
- сітківка ока;
- райдужна оболонка ока;
- геометрія долоні, кисті руки або пальця;
- термографія особи, термографія руки;
- малюнок вен на долоні або пальці руки;
- ДНК;
- запах тіла;
- форма вуха.
- динаміка підпису;
- динаміка клавіатурного набору;
- голос;

- рух губ;
- хода;
- особливості накреслення рукописного тексту.

Ідеальна характеристика повинна легко збиратись, бути універсальною, унікальною и постійною.

Універсальність – можливість представлення людини однією характеристикою.

Унікальність означає, що не повинно бути двох осіб з ідентичними характеристиками.

Сталість (перманентність) – характеристика не повинна змінюватися з часом.

Збирання (вимірюваність) – можливість швидко і легко одержати і деталізувати характеристику від індивідуума.

Таблиця 2.1 – Експертна оцінка властивостей БХЛ: (+ + + – висока оцінка,+ + – середня, + – низька)

| Характеристика | Універсальність | Унікальність | Сталість | Вимірюваність |
|---|---|---|---|---|
| Відеообраз обличчя | +++ | + | ++ | +++ |
| Термограмма обличчя | +++ | +++ | + | +++ |
| Відбиток пальця | ++ | +++ | +++ | ++ |
| Геометрія руки | ++ | ++ | ++ | +++ |
| Райдужна оболонка ока | +++ | +++ | +++ | ++ |
| Сітківка | +++ | +++ | ++ | + |
| Підпис | + | + | + | +++ |
| Голос | ++ | + | + | ++ |
| Відбиток губ | +++ | +++ | ++ | + |
| Особливості вуха | ++ | ++ | ++ | ++ |
| Динаміка підпису | +++ | +++ | + | +++ |
| Хода | +++ | ++ | + | + |

### 2.1.2 Біометричні системи та технології

Протягом останніх десятиліть дорогі та складні біометричні системи використовуються в зонах підвищеної безпеки. Існує цілий ряд біометричних технологій, заснованих на біометричних характеристиках голови (зображення обличчя, райдужна оболонка ока, сітчаста оболонка ока, форма вуха, ...), тіла (сканування відбитків пальців, геометрія руки, аналіз крові, ДНК, ...) або поведінки (голос, рукописна підпис, хода, клавіатурний почерк, ...). Тільки деякі з вище перерахованих технологій технічно доступні і готові до масового продажу за прийнятною ціною.

Біометрична система – це автоматизована система, що вирішує задачі реєстрації користувачів і їх ідентифікації. Ця система реалізує наступні функції:

- фіксація біометричних характеристик;
- вилучення біометричних даних з вибірки;
- порівняння біометричних даних з одним або великою кількістю еталонів;
- прийняття рішень про відповідність даних;
- формування результату про дійсність;
- прийняття рішень про повторення, закінчення або зміну процесу ідентифікації або автентифікації.

Біометричні технології - це методи отримання біометричних характеристик людини. При цьому використовуються як фізичні, так і поведінкові характеристики людини.

У біометричних системах ідентифікаційними ознаками є особистість людини. В основі ідентифікації і автентифікації цього типу лежить процедура зчитування представленої біометричної ознаки користувача і її порівняння з попередньо отриманим шаблоном.

Біометричні системи ідентифікації особистості розрізняються ще по ряду показників:

- пропускна здатність;
- вартість;
- надійність з позиції ідентифікації;
- простота і зручність у використанні;
- ступінь психологічного комфорту;
- можливість обману системи;
- спосіб зчитування;
- точність встановлення автентичності;
- збільшена продуктивність;
- витрати на обслуговування;
- інтеграція;
- конфіденційність.

Пропускна здатність системи в цьому випадку характеризується часом, необхідним для обслуговування одного користувача. Вона залежить, зокрема, від режиму роботи пристрою (проводиться ідентифікація або автентифікація). При ідентифікації користувача потрібно більше часу, ніж для автентифікації, оскільки необхідно порівняти зі зразком майже всі еталони з бази даних. У режимі автентифікації користувач повинен набрати на клавіатурі свій персональний код (номер еталона в базі даних), і системі досить порівняти пред'явлений зразок з одним еталоном. У багатьох системах ці режими може вибрати адміністратор.

Вартість є одним з визначальних чинників широкого використання біометричних систем. Вартість цих систем досить висока в самих країнах-виробниках і значно зростає, коли системи доходять до кінцевих споживачів. Тут позначаються і митні тарифи, і прибуток, який закладається продавцями. Трохи краще в ціновому аспекті справи з вітчизняними розробками. Причому якість ідентифікації багатьох з них вище західних аналогів. Одна ж із серйозних

проблем, що стримують поширення наших розробок, – рівень виробництва, що не дозволяє вийти на закордонний ринок.

Говорячи про надійність біометричної системи з позиції ідентифікації, ми маємо дві ймовірності. Йдеться про ймовірність «помилкових відмов» (система не визнала свого) і «помилкових допусків» (система прийняла «чужого» за «свого»). Це особливо важка і складна область біометрії, тому що система повинна пропускати менше число самозванців і в той же час відкидати менше число законних користувачів.

Простота і зручність у використанні багато в чому визначають споживчі властивості біометричних систем. Адже всі часто задають наступні питання. Наскільки легко встановити дану біометричну систему? Чи потребує система активної участі користувача або отримання характеристик надто обтяжливо? Чи потребує система тривалого навчання? Чи не станеться так, що обтяжлива або громіздка біометрична система автентифікації буде відкинута так само, як ми відмовляємося від використання систем, що вимагають введення довгих паролів? Ступінь психологічного комфорту визначає, наскільки ті чи інші системи та методи визначення біометричних характеристик здатні викликати у користувачів негативну реакцію, страх чи сумнів. Наприклад, окремі люди побоюються, скажімо, дактилоскопії, а інші не бажають дивитися у об’єктив відеокамери з лазерною підсвіткою.

Можливість обману системи пов'язана з використанням різних «дублікатів»: зліпків, магнітофонних записів і т.д. Найбільш «легковірними» вважаються системи ідентифікації по обличчю й голосу.

Спосіб зчитування визначає, чи потрібно користувачеві прикладати свій палець до зчитувача, притулятися обличчям до окуляра і т.д. або достатньо продемонструвати «електронному» пристрою атрибут, необхідний для ідентифікації, наприклад, вимовити умовну фразу або подивитися в об'єктив відеокамери. Виходячи з цього, розрізняють два способи зчитування – дистанційний і контактний. Технологія дистанційного зчитування дозволяє збільшити пропускну спроможність, уникнути регулярного очищення зчитувача і виключити його знос, збільшити вандало-захищеність і т. д.

Точність автентифікації під час використання біометричних систем дещо відрізняється від точності систем, що використовують паролі. Надання коректного пароля в системі автентифікації за паролем завжди дає коректний результат про підтвердження автентичності. Але якщо в біометричну систему автентифікації представлені законні (справжні) біометричні характеристики, це, тим не менш, не гарантує коректної автентифікації. Таке може статися через «шум» датчика, обмежень методів обробки і, що ще важливіше, мінливості біометричних характеристик. Є також імовірність, що може бути підтверджена справжність людини, що видає себе за законного користувача. Більш того, точність даної біометричної реалізації має важливе значення для користувачів, на яких розрахована система. Для успішного застосування біометричної технології з метою ідентифікації особистості важливо розуміти і реально оцінювати цю технологію в контексті програми, для якого вона призначена, а також враховувати склад користувачів цієї програми.

Продуктивність залежить від таких параметрів, як точність, вартість, інтеграція та зручність використання, інформації в цих системах. Іншими словами, чи не будуть біометричні дані використовуватися для стеження за людьми і порушення їх права на приватне життя. Щоб забезпечити соціально-правовий захист користувача, багато закордонних виробники зчитувачів зобов'язалися зберігати в базі даних не зображення відбитку, а деякий отриманий з нього ключ, по якому відновлення відбитку неможливо.

Розглянемо, як же працює будь-яка біометрична система, що використовує фізіологічні або поведінкові характеристики людини. Основа будь-якої біометричної системи розпізнавання особистості - датчик, який видає сигнал, промодульований в залежності від фізичних особливостей конкретної людини. Далі відбувається перетворення аналогового сигналу в цифровий формат, видаляється вся непотрібна інформація і отримана матриця (шаблон) зберігається в пам'яті. Сучасні системи розпізнавання за відбитками пальців, наприклад, мають матрицю об'ємом менше 100 байт. Замість інформації про відбитки пальців може використовуватися інформація про всю долоню, венозний малюнок зап'ястя, райдужну оболонку очей. Дана інформація може поєднуватися з інформацією про голос, почерк, ходу.

Біометрична система – це система розпізнавання шаблона, яка встановлює автентичність конкретних фізіологічних або поведінкових характеристик користувача. Логічно біометрична система може бути розділена на два модулі:

- модуль реєстрації;
- модуль ідентифікації.

Модуль реєстрації відповідає за «навчання» системи ідентифікувати конкретну людину. На етапі реєстрації біометричні датчики сканують зображення обличчя людини для того, щоб створити його цифрове представлення. Спеціальний модуль обробляє це подання, щоб виділити характерні особливості і згенерувати більш компактне і виразне представлення, що називається шаблоном. Для зображення обличчя такими характерними рисами можуть стати розмір і розташування очей, носа і рота. Шаблон для кожного користувача зберігається в базі даних біометричної системи. Ця база даних може бути централізованою або розподіленою, коли шаблон кожного користувача залишається на смарт-картці і передається користувачеві.

Модуль ідентифікації відповідає за розпізнавання користувача комп'ютера. На етапі ідентифікації біометричний датчик знімає характеристики людини, ідентифікація якого проводиться, і перетворює ці характеристики в той же цифровий формат, в якому зберігається шаблон. Отриманий шаблон порівнюється з тим, що зберігається, щоб визначити, чи відповідають ці шаблони один одному. Ідентифікація може виконуватися у вигляді верифікації, автентифікації (перевірка затвердження типу «Я – Сергій Петров») або розпізнавання, визначаючи особистість людини з бази даних про людей, відомих системі (визначення того, хто я, не знаючи мого імені). У верифікаційній системі, коли отримані характеристики і збережений шаблон користувача, за якого себе видає людина, збігаються, система підтверджує

ідентичність. Коли отримані характеристики і один з збережених шаблонів виявляються однаковими, система розпізнавання ідентифікує людину з відповідним шаблоном.

Наведемо основні характеристики біометричних технологій:

- FTE (failure to enroll) - помилка зняття характеристики (помилка реєстрації в системі);
- час розпізнавання;
- стійкість до навколишнього середовища (експлуатаційні якості можуть втрачати стабільність в залежності від оточуючих умов);
- стійкість до підробки (несанкціонованого доступу);
- соціальна прийнятність - згода людей на збір даних;
- точність - будь-яку біометричну систему можна налаштувати на різну пильність;
- вартість.

Крім того, у кожній з реалізацій технології можна виділити також наступні характеристики:

- FRR (false rejection rate) - частота помилок "першого роду" – помилкова відмова;
- FAR (false acceptance rate) - частота помилок "другого роду" - помилковий допуск.

Для користувачів також важливі такі характеристики:

- можливість ідентифікації і автентифікації;
- складність реалізації систем ідентифікації;
- досягнута точність (рівень FRR і FAR);
- можливість безконтактного зчитування;
- розміри файлу-еталона (чим більше розмір образу, тим повільніше йде розпізнавання).

Переваги біометричних систем безпеки очевидні: унікальні людські якості добрі тим, що їх важко підробити, важко залишити фальшивий відбиток пальця за допомогою свого власного або зробити райдужну оболонку свого ока схожою на чиюсь іншу. На відміну від паперових ідентифікаторів (паспорт, водійські права, посвідчення особи), від пароля або персонального ідентифікаційного номера (ПІН), біометричні характеристики не можуть бути забуті або втрачені, в силу своєї унікальності вони використовуються для запобігання крадіжки або шахрайства. Деякі люди вміють імітувати голоси, а в Голлівуді навчилися гримувати людей так, що вони стають вражаюче схожі на інших, але, погодьтеся, це вимагає особливих навичок, які не часто зустрінеш в повсякденному житті.

Основна ж слабкість біометрії, на думку фахівців, полягає в тому, що біометричні дані можна викрасти після того, як вони отримані. Розглянемо, наприклад, біометричну систему перевірки відбитків пальців для одержання віддаленого доступу до сервера. Ви кладете палець на зчитувач, вбудований в мишу або клавіатуру, комп'ютер надсилає оцифрований відбиток пальця на сервер. Сервер порівнює його з збереженим зразком і при збігу дозволяє вам

доступ. Але ця схема недостатня ефективна просто тому, що "вкрасти" оцифрований відбиток пальця не складе труднощів для досвідченого хакера, і як тільки йому це вдасться, він зможе обманювати сервер знову і знову.

Висновок полягає в тому, що біометричні характеристики добре працюють тільки тоді, коли оператор може перевірити дві речі:

- по-перше, що біометричні дані отримані від конкретної особи саме під час перевірки;
- по-друге, що ці дані збігаються із зразком, що зберігається в картотеці.

Якщо система не в змозі цього зробити, вона не буде працювати.

Біометричні характеристики є унікальними ідентифікаторами, але питання їх надійного зберігання і захисту від перехоплення, як і раніше залишається відкритим.

## 2.2 Основні біометричні параметри

### 2.2.1. Класифікація біометричних методів ідентифікації

Людині властиво розвиватися, міняти свої звички, зовнішність і поведінку, однак у неї є й ознаки, що залишаються незмінними протягом всього життя, наприклад, малюнок відбитка пальця або кровоносних судин очного дна. І ті й інші властивості можуть використовуватися біометричними системами як критерій ідентифікації. І залежно від цього методи біометричної ідентифікації діляться на дві великі групи - статистичні й динамічні, рис. 2.1

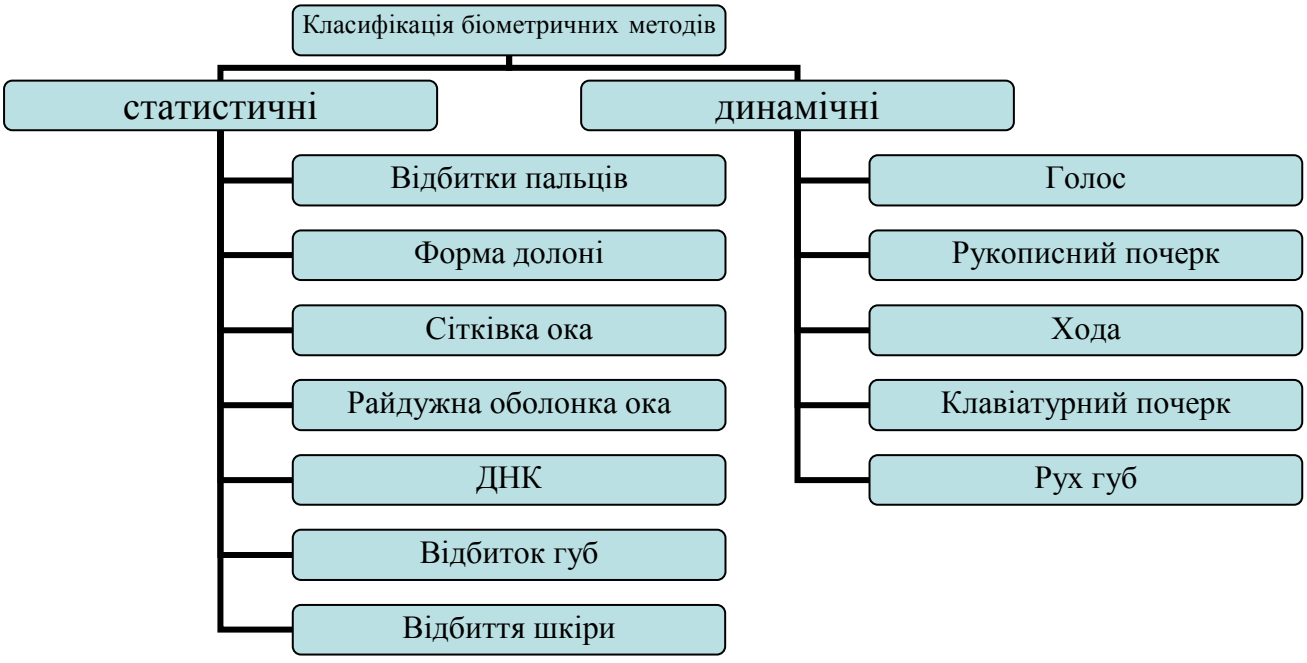



Рис 2.1 Класифікація біометричних методів ідентифікації

Статичні – велика група біометричних продуктів, побудованих на аналізі відкритих статичних (незмінних) образів особистості, даних їй від народження і на які оточуючі звертають свою увагу без особливих зусиль.

Статичні методи ідентифікації засновані на аналізі незмінних фізіологічних характеристик людини. У число цих характеристик входять:

- відбитки пальців (на використанні цих ідентифікаторів будується найпоширеніша, зручна і ефективна біометрична технологія);
- форма і геометрія обличчя (з цими ідентифікаторами працюють технології розпізнавання двовимірних зображень облич);
- форма і будова черепа (для більшої благозвучності компанії, що діють в даній сфері, вважають за краще говорити про технології розпізнавання людини по тривимірній моделі обличчя);
- сітківка ока (практично не використовується в якості ідентифікатора);
- райдужна оболонка ока (розповсюдження технології, в якій застосовується цей ідентифікатор, стримується патентними обмеженнями);
- геометрія долоні, кисті руки або пальця (використовується в декількох вузьких сегментах ринку);
- термографія особи, термографія руки (засновані на використанні цих ідентифікаторів технології не одержали поширення);
- малюнок вен на долоні або пальці руки (відповідна технологія стає популярною, але з огляду на ціну сканерів поки не використовується широко);
- ДНК (в основному в сфері спеціалізованих експертиз);
- запах тіла (автоматичних систем розпізнавання людини, що використовують даний ідентифікатор, ще не створено);
- форма вуха (автоматичних систем розпізнавання людини, що використовують даний ідентифікатор, ще не створено).

Динамічні – пристрої і біометричні програми, побудовані на аналізі динамічних образів особистості. Динамічні образи відображають особливості характерних особистості швидких підсвідомих рухів у процесі відтворення контрольного слова рукописних почерком або при проголошенні контрольного слова голосом. Параметри, що контролюються "динамічною біометрією" можуть бути легко змінені автором шляхом зміни контрольного слова-пароля.

Динамічні методи істотно поступаються статичним в точності та ефективності і, як правило, використовуються як допоміжні.

Застосовувані ідентифікатори:

- динаміка підпису;
- динаміка клавіатурного набору;
- голос;
- рух губ;
- хода;
- особливості накреслення рукописного тексту.

На рис 2.2 наведено сегментацію біометричного ринку за використовуваними ідентифікаторами.

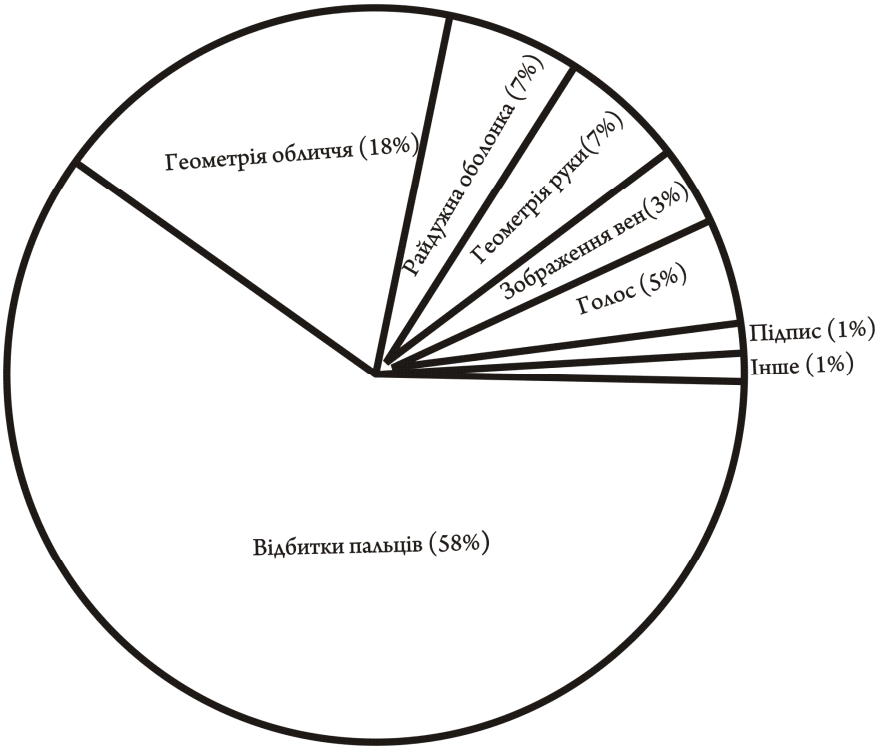



Рисунок 2.2 – Сегментація біометричного ринку по застосовуваним ідентифікаторам (за даними компанії Acuity Market Intelligence)

Статична і динамічна біометрії – це дві взаємно доповнюючи одна одну ланки. Основна перевага статичної біометрії - відносна незалежність від психологічного стану користувачів, малі витрати їхніх зусиль і, отже, можливість організації біометричної ідентифікації великих потоків людей.

### 2.2.2 Ідентифікація людини за допомогою відбитків пальців

Розпізнавання відбитків пальців це одна з найпростіших і добре відомих біометричних технологій. Комерційні ідентифікаційні системи автоматичного розпізнавання відбитків пальців з'явилися ще в 60-х роках XIX століття. Але і до недавнього часу ці системи в основному використовувалися правоохоронними органами при розслідуванні злочинів.

Ідея ідентифікації особистості на основі папілярних малюнків пальців рук була запропонована двома авторами - Г. Фулдсом і В. Гершелем - у статті авторитетного англійського журналу «Nature» в 1880 році. У 1864 році доктор Нейман Гроу опублікував перші роботи з пропозицією ідентифікації особи за відбитками пальців. ФБР наприкінці минулого століття зробив перші кроки в цьому напрямку. У 1895 році дактилоскопія як метод реєстрації злочинців введено в Англії. А вже в 1905 році в Лондонському суді був юридичний прецедент, коли підсудний був засуджений до смертної кари на підставі ідентифікації відбитків його пальців. У Росії дактилоскопія як метод реєстрації злочинців стала використовуватися з 1907 року.

Розпізнавання відбитків пальців – це один з найпростіших і добре відомих біометричних методів ідентифікації особи. Саме він виявився найбільш практичним щодо реалізації та сприйняття його людьми і саме він використовується вже тривалий час. Відбитки пальців у всіх людей абсолютно різні. Всі люди, що населяють в наш час Землю, мають, притаманні тільки їм одним, певні відбитки пальців. І навіть відбитки пальців всіх попередніх поколінь людей також відмінні від всіх наступних. Правоохоронні органи в усьому світі використовують ідентифікацію за відбитками пальців вже більше ста років, причому до сьогодні не виявлено жодного випадку збігу відбитків пальців у різних людей, включаючи навіть однояйцевих близнят. У силу цього саме відбитки пальців руки однієї людини вважаються специфічною, притаманною тільки цій людині «особистою карткою», і саме в такій якості ця властивість застосовується в усьому світі. Але така особливість пальців руки людини була виявлена лише до кінця дев'ятнадцятого століття. До того часу вони представлялися людям просто набором ліній, нічого не позначають і не володіли якимись особливостями.

Шкіра людини складається з двох шарів, при цьому нижній шар утворює безліч виступів - сосочків (від лат. Papillae - сосочок), у вершині яких є отвори вихідних проток потових залоз. На основній частині шкіри сосочки (потові залози) розташовуються хаотично і їх важко побачити.

У кожному відбитку пальця можна визначити два типи ознак:

- глобальні;
- локальні.

Глобальні ознаки - це ті ознаки, які можна побачити неозброєним оком. На окремих ділянках шкіри кінцівок папілляри строго впорядковані в лінії (гребені) і утворюють так звані унікальні папілярні візерунки. Ці візерунки і відображають всю людську індивідуальність.

На рис 2.3 наведено типи папілярних візерунків.


Рисунок 2.3 – Типи папілярних візерунків
(1 - 4 - візерунки типу «петля» (ліва, права, центральна, подвійна), 5 і 6 - візерунки типу «дельта» або «дуга» (проста і гостра), 7 і 8 - візерунки типу «спіраль» (центральна та змішана))

Інший тип ознак - локальні. Їх називають минуціями - унікальні для кожного відбитка ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив і т.д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 минуцій.

Область образу - виділений фрагмент відбитку, в якому локалізовані всі ознаки.

Ядро - пункт, локалізований в середині відбитку або деякої виділеної області.

Пункт "дельта" - початкова точка. Місце, в якому відбувається розділення або підключення борозенок папілярних ліній, або дуже коротка борозенка (може доходити до точки).

Тип лінії - дві найбільші лінії, які починаються як паралельні, а потім розходяться і огинають всю область образу.

Лічильник ліній - число ліній на області образу, або між ядром і пунктом "дельта".

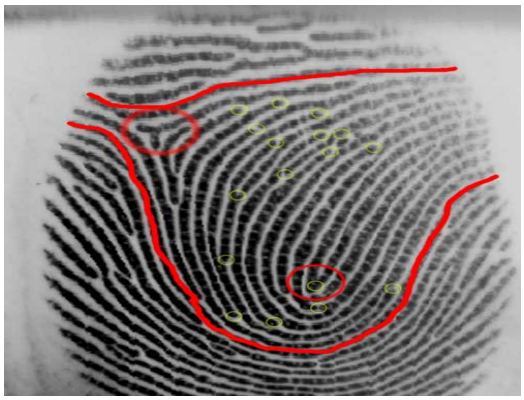


Рисунок 2.4 – Локальні типи ознак - минуції

На рис 2.4 відзначені наступні ознаки:

- дві лінії - "тип лінії";
- те, що між ними - може виступати в якості області образу, але зазвичай береться вся площа відбитка;
- червоне коло ліворуч - пункт "дельта";
- червоне коло нижче - ядро;
- жовті кола показують деякі минуції;
- папілярний візерунок - ліва петля.

Практика показує, що відбитки пальців різних людей можуть мати однакові глобальні ознаки, але зовсім неможливо наявність однакових мікровізерунків минуцій. Тому глобальні ознаки використовують для розділення бази даних на класи і на етапі автентифікації. На другому етапі розпізнавання використовують вже локальні ознаки.

Зараз в основному для розпізнавання відбитків пальців використовуються стандарти ANSI і ФБР США. У них визначено наступні вимоги до образу відбитка:

- кожен образ представляється у форматі не стисненого TIF;
- образ повинен мати розширення не нижче 500 dpi;
- образ повинен бути напів тоновим з 256 рівнями яскравості;
- максимальний кут повороту відбитка від вертикалі не більше 15 градусів;
- основні типи минуцій - закінчення і роздвоєння.

Розглянемо наступні принципи порівняння відбитків за локальними ознаками:

1) Етап 1. Поліпшення якості початкового зображення відбитка. Збільшується різкість кордонів папілярних ліній.

2) Етап 2. Обчислення поля орієнтації папілярних ліній відбитка. Зображення розбивається на квадратні блоки, зі стороною більше 4 пікселів і по градієнтам яскравості обчислюється кут t орієнтації ліній для фрагмента відбитка.

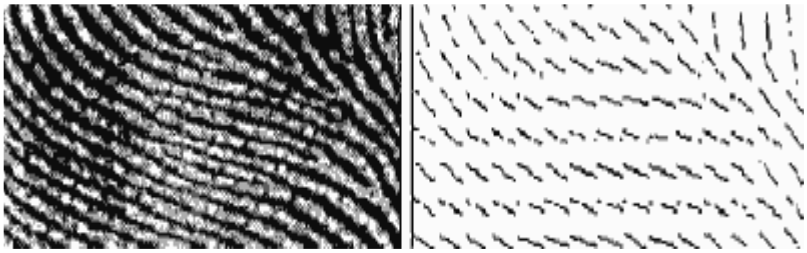


Рисунок 2.5 – Обчислення поля орієнтації папілярних ліній

3) Етап 3. Бінарізація зображення відбитка. Приведення до чорно-білого зображення (1 bit) пороговою обробкою.

4) Етап 4. Стоншення ліній зображення відбитка. Стоншення проводиться до тих пір, поки лінії не будуть шириною 1 піксель.

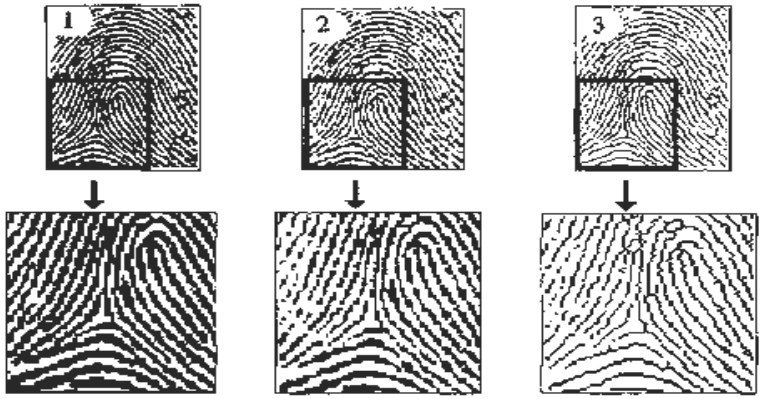



Рисунок 2.6 – Мінімізація ліній зображення відбитка

5) Етап 5. Виділення минуцій. Зображення розбивається на блоки 9x9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центру. Піксель в центрі вважається минуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів один (минуція "закінчення") або два (минуція "роздвоєння").

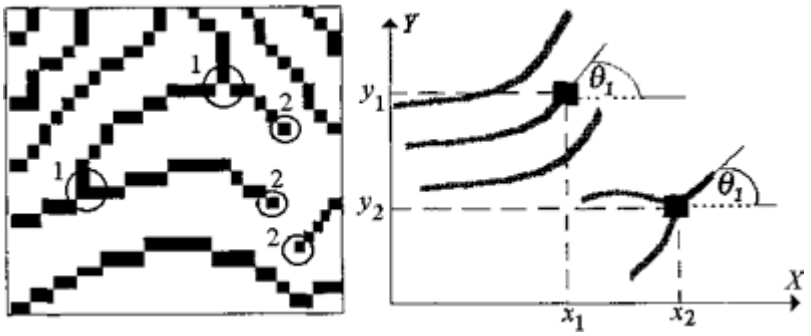


Рисунок 2.7 – Виділення минуцій

Координати виявлених минуцій та їх кути орієнтації записуються у вектор: W (p) = [(x1, y1, t1), (x2, y2, t2 )...( xp, yp, tp)] (p - число минуцій).

При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток (що цілком логічно).

6) Етап 6. Зіставлення минуцій. Два відбитка одного пальця будуть відрізнятися один від одного поворотом, зсувом, зміною масштабу та / або площею дотику в залежності від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток людині чи ні на підставі простого їхнього порівняння (вектори еталона і поточного відбитка можуть відрізнятися по довжині, містити невідповідні минуції і т.д.). Через це процес зіставлення повинен бути реалізований для кожної минуції окремо.

Етапи порівняння:

- реєстрація даних;
- пошук пар відповідних минуцій;
- оцінка відповідності відбитків;
- при реєстрації визначаються параметри афінних перетворень (кут повороту, масштаб і зрушення), за яких деяка минуція з одного вектора є певною минуції з другого.

Під час пошуку для кожної минуції потрібно перебрати до 30 значень повороту (від -15 градусів до +15), 500 значень зсуву (від -250 пкс до 250 пкс - хоча, звісно, межі вибирають і трохи менше ...) і 10 значень масштабу (від 0,5 до 1,5 з кроком 0,1). Разом до 150 000 кроків для кожної з 70 можливих минуцій.

Оцінка відповідності відбитків виконується за такою формулою:

$$K = (D * D * 100\%) / (p * q),$$

де D - кількість збіглися минуцій;

p - кількість минуцій еталона;

q - кількість минуцій ідентифікованої відбитка).

У випадку, якщо результат перевищує 65%, відбитки вважаються ідентичними (поріг може бути знижений виставлянням іншого рівня пильності).

Якщо виконувалася автентифікація, то на цьому все і закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків в базі даних (потім вибирається користувач, у якого найбільший рівень відповідності (зрозуміло, його результат повинен бути вище за поріг 65%)).

Незважаючи на те, що описаний вище принцип порівняння відбитків забезпечує високий рівень надійності, тривають пошуки більш досконалих (і швидкісних) методів порівняння.

Розглянемо метод на основі глобальних ознак. При цьому виконується виявлення глобальних ознак (ядро, дельта). Кількість цих ознак і їх взаємне розташування дозволяє класифікувати тип візерунка. Остаточне розпізнавання виконується на основі локальних ознак (число порівнянь виходить на кілька порядків нижче для великої бази даних).

Вважається, що тип візерунка може визначати характер, темперамент і здібності людини, тому цей метод можна використовувати і в цілях, відмінних від ідентифікації / автентифікації.

Розглянемо метод порівняння відбитків на основі графів (Рисунок 2.8).

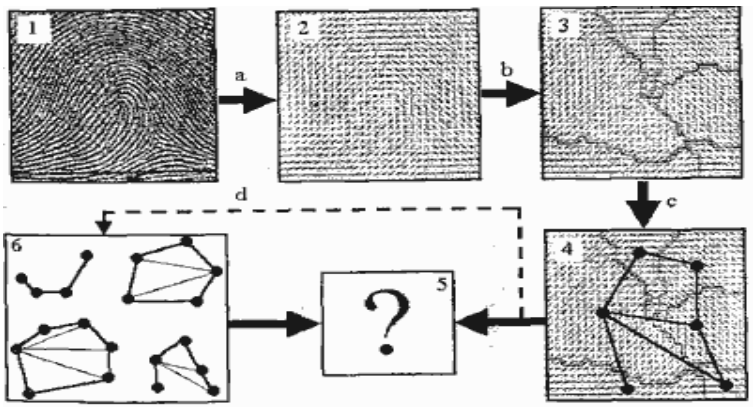



Рисунок 2.8 – Метод на основі графів

Початкове зображення відбитка (1) перетворюється на зображення поля орієнтації папілярних ліній (2). На ньому (2) помітні області з однаковою орієнтацією ліній, тому можна провести межі між цими областями (3). Потім визначаються центри цих областей і виходить граф (4). Стрілкою "d" відзначений запис в базу даних при реєстрації користувача. Визначення подібності відбитків реалізовано в квадраті 5. (Подальші дії аналогічні попереднього методу - порівняння по локальних ознаками).

Розпізнавання відбитків пальців здійснюється за допомогою сучасних сенсорів відбитків пальців. Вони точніше й ефективніше в обробці необхідної інформації, ніж їх більш ранні аналоги. Крім того, ціни на них значно нижчі, ніж на інші біометричні пристрої.

Незважаючи на зовнішні відмінності, всі сканери можна розділити на кілька видів:

1) Оптичні:

- FTIR-сканери;
- оптоволоконні;

- оптичні протяжні;
- роликові;
- безконтактні.

2) Напівпровідникові (напівпровідники змінюють властивості в місцях контакту):

- ємнісні;
- чутливі до тиску;
- термо-сканери;
- радіочастотні;
- протяжні термо-сканери;
- ємнісні протяжні;
- радіочастотні протяжні.

3) Ультразвукові (ультразвук повертається через різні проміжки часу, відбиваючись від борозенок або ліній).

Перевагою ультразвукового сканування є можливість визначити необхідні характеристики на брудних пальцях і навіть через тонкі гумові рукавички.

Крім того, всі прилади зчитування розрізняються по виду, як, наприклад, зовнішні сканери для робочих станцій, ноутбуків і портативних комп'ютерів. Вбудовані сканери відбитків пальців для цих типів систем також починають з'являтися, як і сканери відбитків для стільникових телефонів. Переваги доступу по відбитку пальця - це простота використання, зручність та надійність. Весь процес ідентифікації займає мало часу і не вимагає зусиль від тих, хто використовує дану систему доступу. У будь-якій такій системі клієнтові спочатку пропонують прикласти свій палець (будь-який) до віконця пристрою, який розпізнає. На першому етапі інформація, отримана від зображення пальця, використовується для формування так званого шаблону. Ця операція займає 10-15 с. Потім система пропонує людині пред'явити палець ще кілька разів, щоб перевірити придатність занесеної в пам'ять інформації. Процес реєстрації займає кілька хвилин. Основним елементом пристрою є сканер, що зчитує папілярний візерунок, який потім обробляється за допомогою спеціального алгоритму, і отриманий код порівнюється із шаблоном, що зберігається в пам'яті.

Існує два основних алгоритму порівняння:

- по характерних точках;
- по рельєфу всій поверхні пальця.

Перший алгоритм виявляє характерні ділянки і запам'ятовує їх розташування. У другому випадку аналізується усе «зображення» в цілому. При розпізнаванні по характерних точках виникає шум високого рівня, якщо палець у поганому стані. При розпізнаванні по всій поверхні цього недоліку немає, але є інший: потрібно дуже акуратно розміщувати палець на скануючому елементі.

У сучасних системах використовується також комбінація обох алгоритмів, за рахунок чого підвищується рівень надійності системи. Сформований шаблон заноситься в базу даних системи, в пам'ять головного

комп'ютера або мікропроцесорної картки, або в інший пристрій зберігання цифрових даних і виходить такий собі цифровий індекс. Обсяг збереженої еталонної інформації може бути істотно зменшений, якщо зробити класифікацію за характерними типами папілярних малюнків і виділити на відбитку мікроособливості, що представляють собою початок (закінчення) папілярних ліній або їх злиття (розгалуження). У пропонованих на ринку засобах ідентифікації по відбитку пальця інформація про відбитки, що зберігається в базі даних оператора системи, як правило, недостатня для повної реконструкції відбитка. Це важливо, оскільки виключається використання такої інформації в будь-яких інших цілях, наприклад, при розслідуванні злочину. У деяких системах можна зареєструвати відбитки декількох пальців однієї людини, повторивши процес реєстрації для кожного пальця, який ви захочете використовувати для ідентифікації, але кожен палець можна зареєструвати тільки один раз.

Ще один аспект безпеки розглянутих систем пов'язаний з використанням різних фальшивок. Замовники часто вимагають від постачальників, щоб система розпізнавала випадки представлення зліпків пальців, виконаних, наприклад, із силікону. Жодна з систем ідентифікації по відбитку пальця не забезпечує надійного захисту від підробок. Можна лише розраховувати на те, що зробити гарний зліпок зовсім не так просто, і в більшості випадків для цього необхідно співучасть зареєстрованої людини. Тим не менше, для захисту від пред'явлення фальшивого пальця робляться різні заходи.

Перший захід - аналіз колірного спектра пред'явленого пальця, що дозволяє відмовляти в ідентифікації пред'явникам найпростіших зліпків. Другий захід заснований на оцінці коефіцієнта відбиття речовини, притиснутої до віконця розпізнавального пристрою, що дозволяє відкидати матеріали, з яких зазвичай робляться зліпки. Хоча ні той, ні другий з додаткових тестів не дають 100% надійності, вони все-таки забезпечують високу ймовірність виявлення фальшивок.

Порізи та інші ушкодження пальця, використаного для реєстрації, можуть в деяких випадках виключити можливість ідентифікації. Саме щоб уникнути таких випадків система повинна зареєструвати кілька пальців. Зустрічаються люди, пальці яких практично не мають рельєфу. У більшості таких випадків можна знайти палець, який реєструє система нормально. Інший вихід полягає в зниженні порога ідентифікації для даної конкретної людини. При цьому загальний рівень безпеки системи знижуватися не повинен.

Є ще ряд вимог до стану руки. Наприклад, вологість. Окремі пристрої при сухому або мокрому пальці часто видають «помилкові відмови».

Ще один недолік дактилоскопічної системи ідентифікації - рука повинна бути чистою. Окремі моделі зчитувачів примхливі до відносної температури кисті.

## 2.3 Ідентифікація людини за допомогою її очей

Існує багато систем ідентифікації, де як ключ використовуються очі людини. Ці системи можна розділити на два різновиди, що використовують різні ідентифікатори:

- У першому випадку як «носій» ідентифікаційного коду застосовується малюнок капілярів (кровоносних судин) на сітківці (дні) ока.
- У другому - візерунок райдужної оболонки ока (Рисунок 2.9).

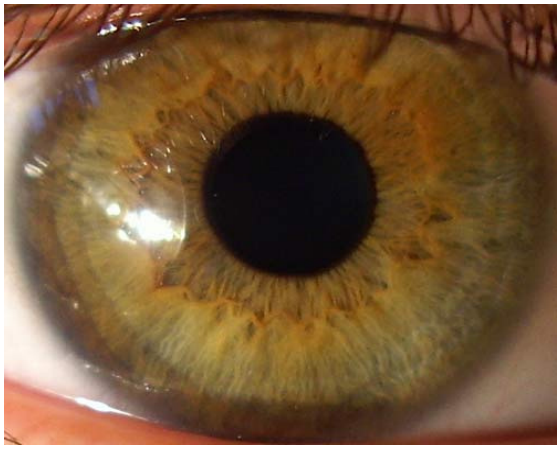


Рисунок 2.9 – Райдужна оболонка ока

### 2.3.1 Ідентифікація за допомогою сітківки ока

Розглянемо спосіб ідентифікації по візерунку кровоносних судин, розташованих на поверхні очного дна (сітківці). Сітківка розташована глибоко всередині ока, але це не зупиняє сучасні технології. Більше того, саме завдяки цій властивості, сітківка - одна з найбільш стабільних фізіологічних ознак організму. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судинах на задній стінці ока. Для цих цілей використовується лазерний промінь м'якого випромінювання. Вени і артерії, що постачають кров'ю очі, добре видно при підсвічуванні очного дна зовнішнім джерелом світла. Ще в 1935 році Саймон і Голдштейн довели унікальність дерева кровоносних судин очного дна для кожного конкретного індивідуума.

Сканери для сітківки ока отримали велике поширення в надсекретних системах контролю доступу, оскільки у них один з найнижчих відсотків відмови доступу зареєстрованих користувачів. Крім того, у системах передбачений захист від муляжу.

В даний час широкому поширенню цього методу перешкоджає ряд причин:

- висока вартість зчитувача;
- невисока пропускна здатність;
- психологічний фактор.

Невисока пропускна здатність пов'язана з тим, що користувач повинен протягом декількох секунд дивитися в окуляр на зелену крапку. І тим не менше, ці системи удосконалюються і знаходять своє застосування. У США, наприклад, розроблено нову систему перевірки пасажирів, яка заснована на скануванні сітківки ока. Фахівці стверджують, що тепер для перевірки не треба діставати з кишені гаманець з документами, що достатньо лише пройти перед камерою. Дослідження сітківки ґрунтуються на аналізі більш як 500 характеристик. Після сканування код буде зберігатися в базі даних разом з іншою інформацією про пасажира, і в подальшому ідентифікація особи займатиме лише кілька секунд. Використання подібної системи буде абсолютно добровільною процедурою для пасажирів. Англійська Національна фізична лабораторія (National Physical Laboratory, NPL), за замовленням організації Communications Electronics Security Group, що спеціалізується на електронних засобах захисту систем зв'язку, провела дослідження різних біометричних технологій ідентифікації користувачів. В ході випробувань система розпізнавання користувачів по сітківці ока не дозволила допуск жодному з більш ніж 2,7 млн «сторонніх», а серед тих, хто мав права доступу, лише 1,8% були помилково відкинуті системою (проводилися три спроби доступу). Як повідомляється, це був наднизький коефіцієнт помилкових рішень серед перевіряючих систем біометричної ідентифікації. А найбільший відсоток помилок був у системи розпізнавання обличчя - в різних серіях випробувань вона відкинула від 10до 25% законних користувачів.

### 2.3.2 Ідентифікація на основі параметрів райдужної оболонки ока

Унікальним для кожної особистості статичним ідентифікатором також є райдужна оболонка ока. Унікальність малюнка райдужної оболонки обумовлена генотипом особистості, і суттєві відмінності райдужної оболонки спостерігаються навіть у близнюків. Лікарі використовують малюнок і колір райдужної оболонки для діагностики захворювань та виявлення генетичної схильності до деяких захворювань. Виявлено, що при ряді захворювань на райдужній оболонці з'являються характерні пігментні плями і зміни кольору. Для ослаблення впливу стану здоров'я на результати ідентифікації людини в технічних системах розпізнавання використовуються тільки чорно-білі зображення високої роздільної здатності.

Ідея розпізнавання на основі параметрів райдужної оболонки ока з'явилася ще в 1950-х роках. Джон Даугман, професор Кембриджського університету, винайшов технологію, до складу якої входила система розпізнавання по райдужній оболонці, що використовується зараз в Nationwide ATM. У той час вчені довели, що не існує двох людей з однаковою райдужною оболонкою ока (більше того, навіть у однієї людини райдужні оболонки очей відрізняються), але програмного забезпечення, здатного виконувати пошук і встановлювати відповідність зразків відсканованого зображення, тоді ще не було. У 1991 році Даугман почав роботу над алгоритмом розпізнавання параметрів райдужної оболонки ока і в 1994 році отримав патент на цю

технологію. З цього моменту її ліцензували вже 22 компанії, в тому числі Sensar, British Telecom і японська OKI. Отримане при скануванні райдужної оболонки ока зображення зазвичай виявляється більш інформативним, ніж оцифроване у випадку сканування відбитків пальців. Унікальність малюнка райдужної оболонки ока дозволяє випускати фірмам цілий клас досить надійних систем для біометричної ідентифікації особи. Для зчитування візерунка райдужної оболонки ока застосовується дистанційний спосіб зняття біометричної характеристики.

Зараз використовуються два основні підходи розпізнавання райдужної оболонки ока, що відрізняються способами представлення образів. У першому підході райдужна оболонка ока виділяється з зображення очей, у другому - образом є матриця штрих-кодів, відповідна радужці.

У першому підході є два своїх способи подання:

- у вигляді кілець, що відносяться до області райдужної оболонки;
- у вигляді прямокутника, отриманого шляхом перетворення декартової системи координат в полярну.

Спочатку визначається центр зіниці і два радіусу щодо нього - радіус зіниці і радіус зовнішнього краю райдужної оболонки (межі визначаються пороговою обробкою). Межі зіниці та райдужної оболонки не є при цьому круглими. Вони стають такими після додаткової обробки. Після чого виконується збільшення чіткості образу.

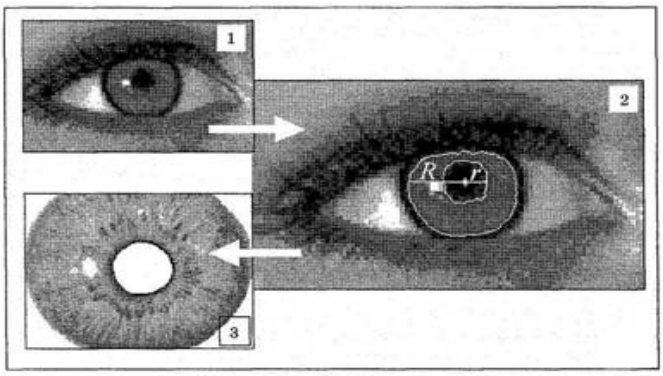



Рисунок 2.10 – Перший спосіб представлення райдужної оболонки ока

Другий спосіб представимо на наступному Рисунку 2.11:

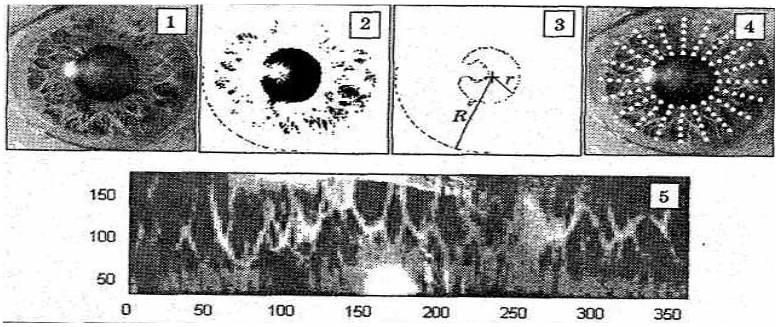



Рисунок 2.11 – Другий спосіб представлення райдужної оболонки ока

Другий спосіб можна представити у вигляді наступного алгоритму:

- Визначення місця розташування, центру і контурів зіниці.
- Визначення радіусів зіниці і зовнішнього краю райдужної оболонки.
- Формування полярної системи координат.
- Перетворення кожного пікселя з декартової системи в полярну.

На останньому етапі може знадобитися інтерполяція зображення, тому що цілочисельні декартові координати не завжди відповідають цілочисельним полярним.

В результаті по осі X відкладені кути полярної системи координат, а по осі Y - значення радіуса (радіус зовнішнього кола радужки мінус радіус внутрішнього). Другий підхід, хоч і вимагає великих обчислень на етапі реєстрації, але зручніше через те, що поворот зображення, перетвореного з декартової системи координат в полярну, замінюється циклічним зсувом.

Другий підхід розпізнавання райдужної оболонки ока (одержання матриці штрих-кодів) можна представити так (рис 2.12):

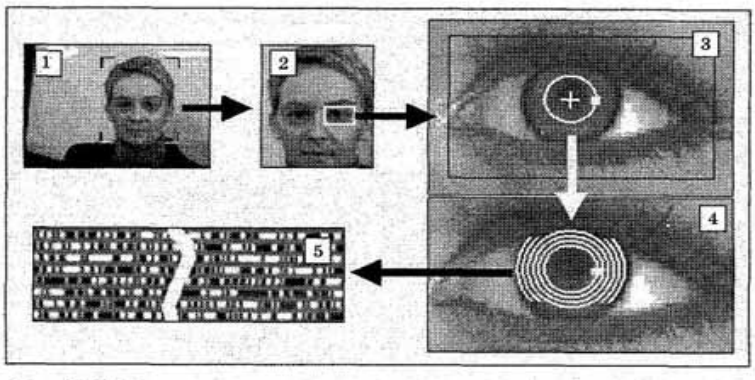



Рисунок 2.12 – Отримання матриці штрих-кодів

Зображення ока виділяється з зображення обличчя, потім на райдужну оболонку накладається спеціальна маска штрих-кодів. У результаті виходить матриця, отримана шляхом логічного множення маски на райдужну оболонку. Образ-еталон виходить розміром 512 байт.

Системи цього класу, використовуючи звичайні відеокамери, захоплюють відео зображення очі на відстані до одного метра від відеокамери, здійснюють автоматичне виділення зіниці та райдужної оболонки. Пропускна здатність таких систем дуже висока. Імовірність же помилкових спрацьовувань невелика. Крім цього, передбачений захист від муляжу. Вони сприймають лише око живої людини.

Ще одна перевага цього методу ідентифікації - висока стійкість. На працездатність системи не впливають окуляри, контактні лінзи і сонячні відблиски. Перевага сканерів для райдужної оболонки полягає в тому, що вони не вимагають, щоб користувач зосередився на цілі, тому що зразок плям на райдужній оболонці знаходиться на поверхні ока. Навіть у людей з ослабленим зором, але з неушкодженою райдужною оболонкою, все одно можуть скануватися і кодуватися ідентифікуючи параметри. Навіть якщо є катаракта

(ушкодження кришталика ока, яке знаходиться позаду райдужної оболонки), то і вона ніяк не впливає на процес сканування райдужної оболонки. Однак погане фокусування камери, сонячний відблиск і інші труднощі при розпізнаванні приводять до помилок в 1% випадків.

Перспективи поширення цього способу біометричної ідентифікації для організації доступу в комп'ютерних системах дуже великі. Тим більше, що зараз вже існують мультимедійні монітори з вбудованими в корпус відеокамерами. Тому на такий комп'ютер досить встановити необхідне програмне забезпечення, і система контролю доступу готова до роботи. Зрозуміло, що і її вартість при цьому буде не дуже високою.

## 2.4. Голосова ідентифікація особи людини

У сучасному світі все більше проявляється інтерес до мовних технологій, зокрема, до ідентифікації людини по голосу. Це пояснюється, з одного боку, появою високопродуктивних обчислювальних систем на базі персональних комп'ютерів і апаратних засобів, що дозволяють виробляти введення сигналу в комп'ютер, а, з іншого боку, високою потребою систем автентифікації в різних галузях життєдіяльності людини.

Метод ідентифікації людини по голосу існує з тих пір, як людина навчилася говорити. Тому переваги і недоліки цього методу відомі всім. Не завжди з відповіді на питання «Хто там?» Ми можемо визначити, що за дверима стоїть знайома людина, і доводиться розвіювати свої сумніви, заглянувши у дверне вічко, так і технічна система ідентифікації може помилятися в силу зміни голосу окремої людини. Привабливість даного методу - зручність у застосуванні.

Метод перевірки голосу має дві позитивні відмінності від інших біометричних методів:

- по-перше, це ідеальний спосіб для телекомунікаційних програм;
- по-друге, більшість сучасних комп'ютерів вже мають необхідне апаратне забезпечення.

Основна проблема, пов'язана з цим біометричних підходом, - точність ідентифікації. Однак це не є серйозною проблемою з того моменту, як пристрої ідентифікації людини по голосу розрізняють характеристики людської мови. Голос формується з комбінації фізіологічних і поведінкових чинників. В даний час ідентифікація по голосу використовується для керування доступом до приміщення середнього ступеня безпеки, наприклад, лабораторії та комп'ютерні класи. Ідентифікація по голосу зручний, але в той же час не такий надійний, як інші біометричні методи. Наприклад, людина з застудою або ларингітом може відчувати труднощі при використанні даних систем. Існує також можливість відтворення звукозапису з магнітофона. Технологія розпізнавання голосу - ймовірно, найбільш практичне рішення для більшості мережевих додатків, у всякому разі, на даний момент. Системи розпізнавання голосу аналізують характеристики оцифрованої мови, в тому числі її тон, висоту і ритм. Незважаючи на те, що залишаються технічні питання, зокрема,

на зниження надійності розпізнавання за наявності шумів, це досить економічне рішення, так як мікрофони і звукові карти вже давно отримали прописку в мережі.

Як відомо, джерелом мовного сигналу служить мовоутворюючий тракт, який збуджує звукові хвилі в пружному повітряному середовищі. Сформований мовний сигнал і передається у просторі у вигляді звукових хвиль. Приймач сигналу - це датчик звукових коливань. Зазвичай для цих цілей використовують мікрофон - пристрій для перетворення звукових коливань в електричні. Існує велика кількість типів мікрофонів (вугільні, електродинамічні, електростатичні, п'єзоелектричні та ін.). Але в мікрофонах будь-якого типу чутливим елементом є пружна мембрана, за допомогою якої передається коливальний процес під впливом звукових хвиль. Мембрана пов'язана з елементом, який перетворює коливання мембрани в електричний сигнал. З виходу мікрофона сигнал подається на вхід звукової карти персонального комп'ютера. Під час запису звукова карта є аналого-цифровим перетворювачем з широкими можливостями настройки параметрів оцифрування. Основними параметрами є частота дискретизації та розрядність кодування. Ці параметри визначають якість і розмір вибірки, що отримується в результаті запису. Причому розмір запису і її якість прямо пропорційні, тобто чим вище якість запису, тим більше її розмір. Щоб забезпечити компроміс між якістю і розміром, скористаємося знаннями про властивості людського голосу при виборі параметрів аналого-цифрового перетворення. На цей момент у нас і за кордоном реалізовані системи автоматичної ідентифікації по голосу, більшість з яких будуються за єдиною концептуальною схемою:

- здійснюється реєстрація користувача та обчислюється шаблон;
- вибираються ділянки мовного потоку для подальшого аналізу;
- здійснюється первинна обробка сигналу;
- обчислюються первинні параметри;
- будується «відбиток» (шаблон) голосу;
- проводиться порівняння «відбитків» голосів і формується рішення щодо ідентичності голосів або «близькості» голосу до групи голосів.

Розглянемо більш детально кожен з етапів. На етапі реєстрації новий користувач вводить свій ідентифікатор, наприклад, ім'я та прізвище, а потім вимовляє кілька разів ключове слово або фразу (створюються еталони). Кількість повторів ключової фрази може варіюватися для кожного користувача, а може бути постійним для всіх. Після попередньої обробки фрагменти попарно порівнюються, і на основі їх ступеня подібності обчислюється значення «відбитка» (шаблону). Для вибору фрагментів фонограми, з метою отримання необхідних параметрів, існує кілька підходів. Наприклад, часто застосовують метод, в якому використовується весь мовний сигнал за винятком пауз. Також існує метод вибору опорних сегментів - найбільш інформативних ділянок мовного сигналу. При цьому вибирають найбільш енергетично потужні звуки, оскільки вони менш залежні від шумів і спотворень. В основному це голосні і дзвінкі приголосні, вимова яких добре відображає роботу голосових зв'язок і

мовного тракту. Ці звуки обов'язково мають яскраво виражену нерівномірність спектральної характеристики і саме в них виражена індивідуальна особливість м'язової активності мовного тракту людини.

У процесі первинної обробки сигналу проводиться оцінка спектральних параметрів мови. Перші системи ідентифікації особи за особливостями голосу будувалися виходячи з частотних уявлень і можливостей засобів аналогової фільтрації. В основу їх роботи покладено різне тембральне забарвлення голосів і індивідуальна нерівномірність розподілу потужності виголошуваної фрази по частотному спектру. Первинні параметри мовного сигналу повинні мати наступні властивості:

- відображати індивідуальність диктора;
- повинні легко і надійно виділятися з сигналу;
- мало залежати від заважаючих факторів;
- бути інваріантними до емоційного та фізичного стану диктора;
- слабо піддаватися імітації.

В якості первинних параметрів зазвичай використовуються такі характеристики мовного сигналу, як АЧХ, основний тон, формант, відстань між обертонами, форми імпульсів збудження, тривалість окремих звуків і т. п.

За отриманими на попередньому етапі параметрами, виходячи з обраної математичної моделі, будується «відбиток» голосу. Далі виробляється порівняльний аналіз відбитків голосів. Аналізувати можна різними способами, починаючи від простих статистичних методів і закінчуючи тим, що рішення приймається нейро-мережею або складною системою штучного інтелекту. Задача ідентифікації виникає тоді, коли необхідно знайти найближчий голос (або кілька голосів) з фонотеки до розглянутої фонограми. Необхідність автоматизації цього завдання безпосередньо залежить від кількості голосів у фонотеці, рівня експерта і необхідної оперативності прийняття рішення.

Зазвичай після задачі ідентифікації доводиться вирішувати друге завдання, в якому підтверджується або спростовується приналежність фонограми конкретному голосу, тобто завдання верифікації. Рішення задачі ідентифікації дозволяє вирішувати задачу верифікації не на всій фонотеці, а тільки на групі найближчих голосів, що значно скорочує час обробки фонограми. Описаний вище частотний підхід до ідентифікації людини міг бути реалізований засобами аналогової фільтрації вже 30-40 років тому і саме з цієї причини в той час відбувся сплеск інтересу до цього класу систем голосової ідентифікації. У міру розвитку засобів обчислювальної техніки та методів цифрової фільтрації, інтерес до частотних методів ідентифікації заміщається на інтерес до систем, що застосовують лінійне передбачення мовного сигналу.

Системи ідентифікації з лінійним передбаченням мови використовують опис сигналу у часовій області. В основу кодування мови методом лінійного передбачення покладена хвильова структура мовного сигналу, особливо добре спостерігається при вимові голосних. Метод лінійного передбачення побудований на апроксимації сусідніх хвиль у звуковий пачці перехідним процесом деякого лінійного цифрового фільтра. При описі звукового сигналу

методом лінійного передбачення вихідний сигнал розбиває на окремі інтервали аналізу фіксованої довжини (зазвичай довжина інтервалу аналізу становить 20 мс). Далі визначають тип звуку всередині інтервалу.

Даний метод ідентифікації має наступні переваги та недоліки.

Переваги:

- звичний для людини спосіб ідентифікації;
- низька вартість (найнижча серед всіх біометричних методів);
- безконтактність.

Недоліки:

- високий рівень помилок 1 і 2 роду;
- необхідність у спеціальному шумоізолюючому приміщенні для проходження ідентифікації;
- можливість перехоплення фрази "магнітофоном";
- якість розпізнавання залежить від багатьох факторів (інтонація, швидкість виголошення, психологічний стан, хвороби горла);
- необхідність підбору спеціальних фраз.

## 2.5 Система розпізнавання облич

### 2.5.1 Ідентифікація людини за допомогою геометрії обличчя

Система розпізнавання облич - найбільш давній і розповсюджений спосіб ідентифікації. Саме такій процедурі піддається кожен, хто перетинає кордон. При цьому прикордонник звіряє фото на паспорті з особою власника паспорта і приймає рішення, його це паспорт чи ні. Приблизно таку ж процедуру виконує комп'ютер, але з тією лише різницею, що фото вже знаходиться в його пам'яті. Привабливість даного методу заснована на тому, що він найбільш близький до того, як ми ідентифікуємо одне одного. Розвиток даного напряму обумовлено швидким зростанням мультимедійних відеотехнологій, завдяки яким можна побачити все більше відеокамер, встановлених вдома і на робочих місцях. Істотний імпульс цей напрямок одержав з великим розповсюдженням технології відеоконференцій Internet / Intranet. Орієнтація на стандартні відеокамери персональних комп'ютерів робить цей клас біометричних систем порівняно дешевим. Тим не менш, ідентифікація людини по геометрії обличчя являє собою досить складне (з математичної точки зору) завдання. Хоча обличчя людини - унікальний параметр, але досить динамічний; людина може посміхатися, відпускати бороду і вуса, надягати окуляри - все це додає труднощів у процедуру ідентифікації і вимагає досить потужної й дорогої апаратури, що відповідно впливає на ступінь поширення даного методу.

Алгоритм функціонування системи розпізнавання досить простий. Зображення особи зчитується звичайною відеокамерою та аналізується. Програмне забезпечення порівнює введений портрет з тим, що зберігається в пам'яті в якості еталона. Деякі системи додатково архівують зображення які вводяться для можливого в майбутньому вирішення конфліктних ситуацій.

Вельми важливо також те, що біометричні системи цього класу потенційно здатні виконувати безперервну ідентифікацію (автентифікацію) користувача комп'ютера протягом всього сеансу його роботи. Більшість алгоритмів дозволяє компенсувати наявність окулярів, капелюха і бороди у піддослідного. Було б наївно припускати, що за допомогою подібних систем можна отримати дуже точний результат. Незважаючи на це, в деяких країнах вони досить успішно використовуються для верифікації касирів і користувачів депозитних сейфів.

Основними проблемами, з якими стикаються розробники даного класу біометричних систем, є зміна освітленості, варіації положення голови користувача, виділення інформативної частини портрета (гасіння фону). З цими проблемами вдається впоратися, автоматично виділяючи на обличчі особливі точки і потім вимірюючи відстані між ними. На обличчі виділяють контури очей, брів, носа, підборіддя. Відстані між характерними точками цих контурів утворюють вельми компактний еталон конкретного обличчя, що легко піддається масштабуванню. Завдання оконтурювання характерних деталей обличчя легко може бути вирішена для плоских двомірних зображень з фронтальним підсвічуванням, але такі біометричні системи можна обдурити плоскими зображеннями обличчя оригіналу.

Для двомірних систем виготовлення муляжу фотографії - це не складна технічна задача. Істотні технічні труднощі при виготовленні муляжу виникають при використанні тривимірних біометричних систем, здатних по перепадах яскравості відбитого світла відновлювати тривимірне зображення обличчя. Такі системи здатні компенсувати невизначеність розташування джерела освітлення по відношенню до ідентифікуючого обличчя, а також невизначеність положення обличчя по відношенню до відеокамери. Обманути системи цього класу можна тільки об'ємною маскою, яка точно відтворює оригінал.

Даний метод має суттєву перевагу: для зберігання даних одного зразку ідентифікаційного коду потрібно зовсім небагато пам'яті. А все тому, що, як з'ясувалося, людське обличчя можна поділити на відносно невелику кількість «блоків», незмінних у всіх людей. Цих блоків більше, ніж відомих нам частин обличчя, але сучасна техніка навчилася виділяти їх і будувати на їх основі моделі, керуючись взаємним розташуванням блоків.

### 2.5.2 Ідентифікація за «тепловим портретом» обличчя

Більш надійним різновидом систем розпізнавання облич є ідентифікація за «тепловим портретом» особи або тіла людини в інфрачервоному діапазоні. Цей метод, на відміну від звичайного, оптичного, не залежить від змін обличчя людини (наприклад, появи бороди), так як теплова картина обличчя змінюється вкрай рідко. Дана технологія заснована на тому, що термограми обличчя людини (теплова картинка, створена випромінюванням тепла кровоносними судинами обличчя) унікальна для кожної людини і, отже, може бути використана в якості біокода для систем контролю допуску. Дана термограма є більш стабільним кодом, ніж геометрія обличчя, оскільки не залежить від часу і змін зовнішності людини.

У процесі термографічної ідентифікації обличчя індивідуальний малюнок розподілу теплових областей на обличчі людини вводиться в комп'ютер за допомогою інфрачервоної камери та плати захоплення зображення. Монохромне зображення, що надходить від інфрачервоної відеокамери, вводиться в комп'ютер за допомогою спеціального кабелю. В цей же час до зображення додається спеціально створена переглядова таблиця (look up table). Зображення піддається обробці спеціальною утилітою, розробленою на C + +. У цей час і відбувається ідентифікація за індивідуальним малюнком теплових областей на обличчі.

Проблеми ідентифікації людини за допомогою обличчя істотно спрощуються при переході спостережень у дальній інфрачервоний діапазон світлових хвиль. Запропоновано здійснювати термографію ідентифікуючого обличчя, яка виявляє унікальність розподілу артерій на обличчі, що забезпечують шкіру теплою кров'ю. Проблема підсвічування для цього класу біометричних пристроїв не існує, так як вони сприймають лише температурні перепади обличчя і можуть працювати в повній темноті. На результати ідентифікації не впливають перегрів особи, його переохолодження, природне старіння обличчя, пластичні операції, тому що вони не змінюють внутрішнє розташування судин. Методом лицьової термографії можливо розрізнити однояйцевих близнят, кровоносні судини на їхніх обличчях мають досить істотні відмінності. Дистанційне зчитування з будь-якої відстані незалежно від освітленості забезпечує високу пропускну здатність. Метод розрахований на використання спеціалізованої відеокамери далекого інфрачервоного діапазону, що й визначає його високу вартість.

## 2.6 Ідентифікація людини за допомогою кисті руки

Практично все про людину можливо прочитати за його рукою. Проте, в біометриці з метою ідентифікації (або автентифікації) використовується зараз тільки проста геометрія руки - розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин).

### 2.6.1 Метод розпізнавання геометрії кисті руки

Взагалі з руки можна зібрати до 90 інформаційних знаків, частина з яких не використовується в біометриці. Наприклад, унікальний візерунок на долоні.

Існує два підходи до використання геометрії руки:

- перший (існує з 1976 року) заснований на геометричних характеристиках кисті;
- другий (сучасний) використовує крім геометричних ще й образові характеристики руки (образи на згинах між фалангами пальців і візерунки кровоносних судин).

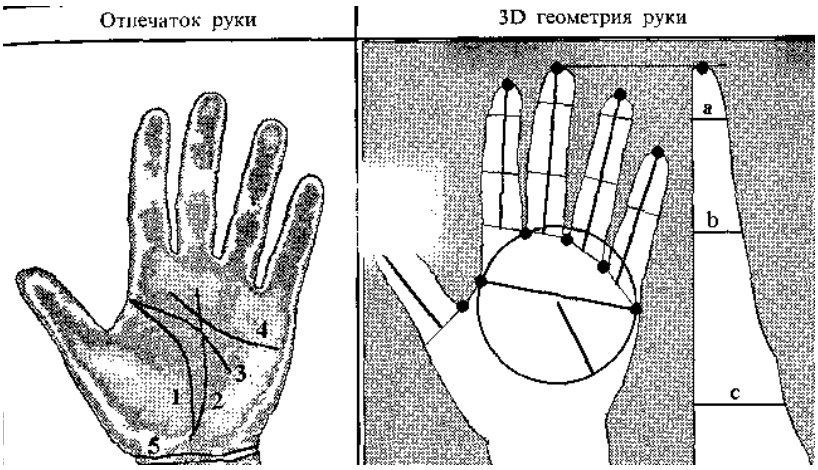



Рисунок 2.13 – Інформаційні знаки руки

Візерунок на долоні, що складається з п'яти основних ліній (ліворуч), контрольної точки і 17 геометричних ознак руки (праворуч). Як видно з рис 2.13, вихідними біометричними ознаками руки є ширина долоні, радіус вписаного в долоню кола, довжина пальців, ширина пальців, висота кисті руки в трьох місцях (a, b, c). Також можна використовувати й інші ознаки, наприклад, кути між контрольними точками, середні значення і дисперсія значень вихідних ознак.

Метод розпізнавання геометрії кисті руки заснований на аналізі тривимірного зображення кисті руки і отримав розвиток у зв'язку з тим, що математична модель ідентифікації за даним параметром вимагає досить малого обсягу інформації - всього 9 байт, що дозволяє зберігати великий обсяг записів, і отже, швидко здійснювати пошук . Однак форма кисті руки також є параметром, який досить сильно зазнає змін у часі, а крім того, вимагає сканерів великого розміру, що веде до подорожчання системи.

В даний час, метод ідентифікації користувачів по геометрії руки використовується багатьма організаціями і компаніями. У деяких випадках працювати з відбитком руки набагато зручніше, ніж з відбитком пальця.

Перший комерційний біометричний пристрій, що визначає геометрію пальців, з'явився більше 30 років тому. Перші моделі зчитувачів, у яких в якості ідентифікатора використовувалося об'ємне зображення долоні, з'явилися в 1972 році в США. Долоня підсвічувалась безліччю лампочок, розташованих у вигляді матриці, і аналізувалася тінь - двомірне зображення кисті руки. У сучасних моделях зчитувачів враховується і товщина долоні.

Більш складними є системи, які додатково вимірюють профіль руки (обсяг пальців, обсяг кисті, нерівності долоні, розташування складок шкіри на згинах). Дані про тривимірну геометрію руки отримують шляхом використання однієї телевізійної камери та інфрачервоної підсвітки руки під різними кутами. Послідовне включення декількох підсвічуючих світлодіодів дають тіньові варіанти проекцій тривимірної геометрії кисті руки, що містять інформацію про її об'єм. Пристрої, в яких реалізовано подібне технічне рішення, не будуть

малогабаритними, так як потрібно виносити джерела підсвічування на відстань 10-15 см. Широкому поширенню таких систем перешкоджає кілька факторів:

- висока ціна самого зчитувача;
- невисока пропускна здатність - долоню потрібно правильно розташувати у зчитувальному пристрої;
- відсутність технологій захисту від фальсифікації;
- замість кисті руки в зчитувач можна засунути її муляж.

Також у цієї системи біометричної ідентифікації є і свої переваги. На відміну від дактилоскопічних зчитувачів, вони не пред'являють підвищених вимог до вологості, температури, кольору, забрудненості та інших параметрів. Системи такого типу доцільно застосовувати в студентських містечках, на складах і т. п., тобто там, де неможливо забезпечити чистоту рук і відносно невисокі вимоги до безпеки.

### 2.6.2 Ідентифікація по зображенню кровоносних судин на зворотному боці долоні

Ще один варіант застосування кисті руки в якості ідентифікатора - це використання малюнка кровоносних судин на зворотному боці долоні. Такий візерунок унікальний, його можна зчитувати на відстані і складно відтворити штучно.

Ця новітня технологія розпізнавання лежить в основі багатьох пристроїв ідентифікації. Особливість приладів полягає в тому, що вони сканують не поверхню пальця, а склад внутрішніх органів людини (структуру мережі кровоносних судин руки) за допомогою спеціального інфрачервоного датчика. У цьому випадку деформація поверхні, сухість, вологість або забрудненість рук ніяк не впливають на результати розпізнавання. Після сканування система розпізнавання обробляє отримане зображення. Такі пристрої можуть працювати як самостійно, так і в мережі під управлінням сервера.

Крім розглянутих пристроїв, існують такі, які використовують для ідентифікації людини малюнок вен, розташованих на тильній стороні кисті руки, стиснутої в кулак. Спостереження малюнка вен здійснюється телевізійною камерою за інфрачервоного підсвічування, після чого обчислюється шаблон.

## 2.7 Розпізнавання за голосом

Ідентифікація людини за голосом – один із традиційних способів розпізнавання, застосовуваний повсюдно. Можна легко довідатися співрозмовника по телефону, не бачачи його. Також можна визначити психологічний стан по емоційному фарбуванню голосу. Тому що голосова ідентифікація безконтактна й не жадає від людини особливих зусиль, ведуться роботи зі створення голосових замків і систем обмеження доступу до інформації. Інтерес у цій області зв'язаний ще й із прогнозами повсюдного впровадження голосових інтерфейсів.

На сьогоднішній день існує два підходи до ідентифікації людини по голосі, побудовані на обліку структури мовного сигналу, рис 2.14.

Кожний сплеск голосового сигналу відповідає деякому фрагменту мови. Це може бути одна буква, сполучення букв (фонема) або коротке слово (те саме слово із трьох букв сюди не ставиться). Усього в російської мови є 42 фонеми, але підходять для ідентифікації людини не все. Частина фонем огласовані. Саме їм властивий індивідуальний характер. Це звуки "э", "об", "л", "а", "і" та інші. Інша частина фонем - шиплячі (шумоподібні). Це "ц", "ч", "ш", "щ" і т.д. Вони не є індивідуальними і їхнє використання при ідентифікації може привести до зниження якості розпізнавання. На малюнку вище синім цвітом відзначена огласована фонема, а червоним - шумоподібна.

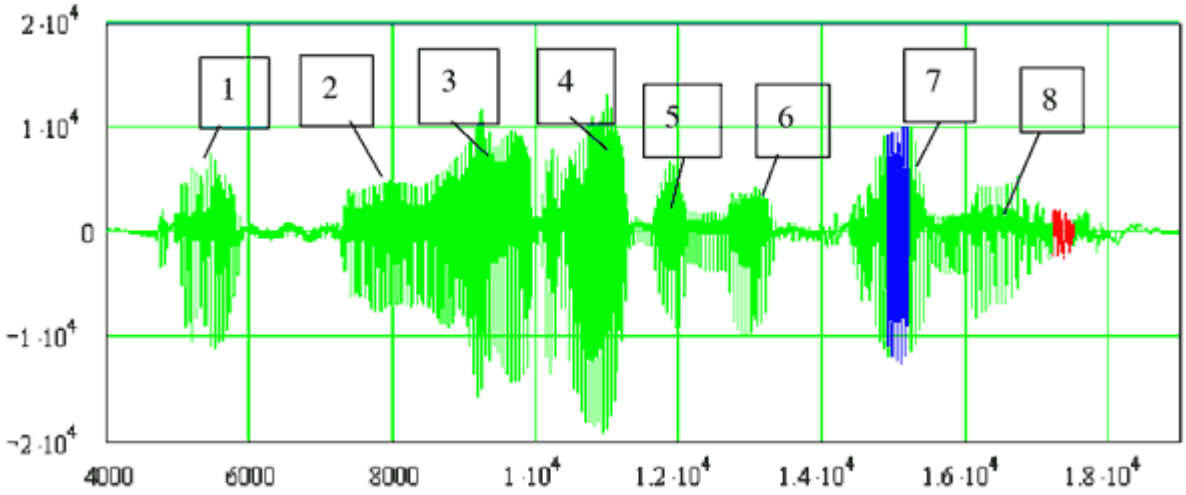



Рисунок 2.14 – Приклад голосової фрази й виділення з її 8 фрагментів

Огласовані фрагменти мови мають явно виражений періодичний характер, представлені на рис. 2.15. Період і характер коливань індивідуальні. Це добре видно на графіку:

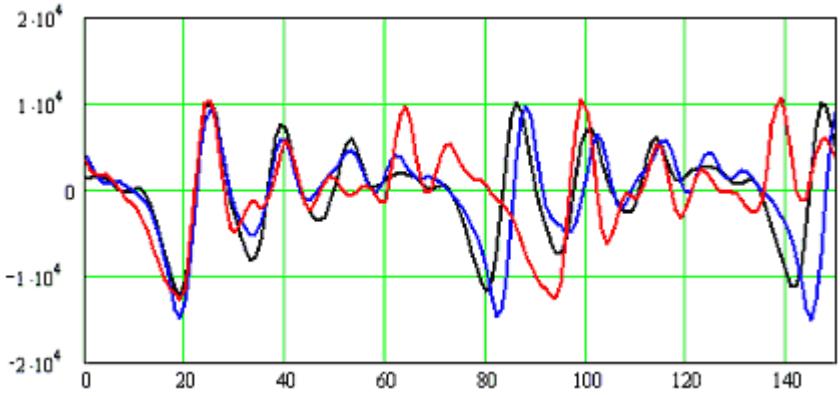



Рисунок 2.15 - Графік коливання фонем

Чорною й синьою лініями позначені коливання однієї фонеми для однієї людини. Червоний цвітом позначена фонема від іншої людини. Для однієї

людини графіки дуже схожі. В іншої людини й період тону й форма внутрішніх коливань значно відрізняються.

Перший підхід. Індивідуальні розходження розподілу потужності сигналу по спектрі покладені в основу першої категорії систем біометричної ідентифікації по голосі. Вони будуються на базі гребінки вузькополосних фільтрів, що виділяють із голосу коливання різних частот. На підставі вихідних даних можна побудувати графік (амплітудно-частотну характеристику).Смуги пропущення фільтрів вибираються при проектуванні системи, але вони не повинні бути занадто вузькими, щоб не залежати від варіацій частотного спектра голосу. У той же час, вони не повинні бути й дуже широкими. Потрібно підбирати оптимальну ширину, достатню для впевненої ідентифікації. Звичайно використовують 16 фільтрів, які розширюються в міру росту значень виділюваних частот. Це пов'язане з нестабільністю високих частот по енергії (у порівнянні з низькими частотами). Системи спектрального аналізу голосу навчаються, запам'ятовуючи розподіл енергій із частотою порядку 35 мілісекунд. У підсумку виходить великий масив даних, що відповідає фразі. Дані знімаються із частотою 16кГц і в 16 розрядів (це пов'язане з особливостями фільтрів). Після чого вони пропускаються через фільтри. Підсумковий масив даних виходить дуже маленького розміру (потрібно записати тільки 16 координат вершин по одній осі). Для ідентифікації можна використовувати як статистичні методи, так і нейронну мережу, що не повинне впливати на результат розпізнавання.

Другий підхід – використання апарата лінійного пророкування. Огласовані коливання звуку імітують періодичними ударами по деякій коливальній ланці (дзвону). Період ударів повинен точно відповідати періоду основного тону голосу. Динамічні характеристики дзвона повинні мінятися, щоб одержати форму, близьку до голосової фрази. Зрозуміло, що як дзвін використовується цифровий коливальний фільтра, а не реальний аналог. Число коефіцієнтів фільтра коливається від 10 до 12 (a1,..., a12). Цього досить для якісного відтворення мови зі збереженням індивідуальних особливостей. Коефіцієнти лінійного провісника обчислюються на вибірці з 180-220 відліків ("ударів"). Обчислення параметрів провісника (цифрового фільтра) знаходять рішенням системи з 10...12 лінійних рівнянь. Для того, щоб понизити обчислювальне навантаження частоту дискретизації знижують до 8 кГц. При імітації огласованих звуків на вхід цифрового фільтра подають періодичну послідовність імпульсів, змодульовану по амплітуді. У такому випадку на виході фільтра з'являються періодичні перехідні процеси, що повторюють звук, який моделюється. При моделюванні шиплячих на вхід фільтра подають випадковий шум потрібної амплітуди. При навчанні системи, на її вхід подають кілька зразків голосу користувача. Вони перетворяться в послідовність імпульсів основного тону й відповідну послідовність коефіцієнтів лінійного провісника. Виходить масив даних, що описує індивідуальні особливості голосу людини для даної фрази. Цей масив з коефіцієнтів і є тим біометричним еталоном, що записується в базу даних.

Характеристика обох методів. Помилки першого роду (недопуск свого) складають 1-5% (хоча, залежно від реалізації програмного забезпечення, можуть доходити до 40% - перевірено досвідченим шляхом). Кількість помилок другого роду (пропуск чужого) залежить від того, чи знає зловмисник ключову фразу (до 1%, якщо голоси близькі) чи ні (0,00000001%). Голосовий захист просто пройти, якщо перехоплено або записана ключова фраза. Тому розроблювачі зараз намагаються створити систему, захищену від перехоплення. Зараз можна використовувати голосову идентифікацію разом з іншими видами захисту. Наприклад, по геометрії особи. Тоді можна відслідковувати рух губ і синхронізацію їх зі звуком. Або якось інакше.

Наведемо наступні переваги та недоліки цих систем:

Переваги:

- Звичний для людини спосіб ідентифікації.
- Низька вартість (найнижча серед всіх біометричних методів).
- Безконтактність.

Недоліки:

- Високий рівень помилок 1 і 2 роди.
- Необхідність у спеціальному шумоізольованому приміщенні для проходження ідентифікації.
- Можливість перехоплення фрази "магнітофоном".
- Якість розпізнавання залежить від багатьох факторів (інтонація, швидкість проголошення, психологічний стан, хвороби горла).
- Необхідність підбора спеціальних фраз

## 2.8 Ідентифікація людини за її підписом

Підпис – один з класичних способів ідентифікації, що застосовується вже кілька століть в юридичній практиці, банківській справі і торгівлі

Існує два незалежних способи ідентифікації за підписом:

- ідентифікація по зображенні підпису на документі;
- ідентифікація за динамікою підпису, що вводиться в комп'ютер.

У першому способі потрібно порівняти два зображення. З цим краще впорається людина.

У другому способі є дані про коливання пера при відтворенні підпису в тривимірному просторі (X, Y - координати і Z - тиск на планшет). З цим може впоратися тільки комп'ютер.

Системи, що використовують одну з функцій часу X (t), Y (t) або Z (t) забезпечують вірогідність помилок 0,1. Якщо використовувати дві функції, то 0,01. Для трьох функцій - 0,003.

Деякі системи використовують не самі функції, а їх першу або другу похідну, що незначно впливає на якість розпізнавання. Імовірність помилки 1 роду (не допуск свого) 0,01 - цілком прийнятно. Однак для помилок другого роду (допуск чужого) це дуже багато. Для зниження вірогідності використовують ключове слово (імовірність помилки знижується в 10 000 ... 1 000 000 разів).

Якщо система аналізу підпису враховує тільки глобальні параметри (деяка функція від коливань пера для всього підпису), то біометричний еталон формується досить просто. Якщо ж враховуються локальні ознаки (та ж функція, але для окремих елементів підпису), то можуть з'являтися і зникати фрагменти підпису (зливатися). У результаті підпис складно розділити на фрагменти. Доводиться враховувати всі варіанти, або приводити образи до середнього варіанту.

Однією з основних проблем даних біометричних систем є залежність від психологічного стану людей і стабільності їх почерку.

Наведемо наступні переваги та недоліки цих систем:

Переваги:

- невисока вартість;
- відносна звичність для людини.

Недоліки:

- високий рівень помилок 1 і 2 роду;
- необхідність навчання роботи з планшетом перед реєстрацією;
- тривалий час реєстрації користувача (більше 2 хвилин);
- користувачі можуть зображати нестабільний почерк, якщо опираються системі;
- бездротове перо можна вкрасти або розбити.

## 2.9 Додаткові біометричні параметри

Раніше були розглянуті основні біометричні параметри, які в цей час широко використовуються для аутентифікації людини. Ріст ринку біометричних систем стимулює розвиток нових технологій ідентифікації, у кожної з яких є свої достоїнства й недоліки й своя область застосування. До таких біометричних параметрів ставляться:

1.ДНК – часто називають майже самим ідеальним параметром, тому що код ДНК є ідентифікаційною інформацією в цифровій формі, що є в будь-якій клітині людини . Недолік цього параметра в тім, що із практичної точки зору порівняння людей на основі двох зразків ДНК - повільний, дорогий й складний процес;

2. сітківка ока – ідентифікація людини по сітківці ока відбувається шляхом порівняння зображень кровоносних судин очного дна. У цей час сенсори, використовувані для ідентифікації по сітківці, усе ще занадто дорогі в порівнянні із сенсорами для зчитування інших біометричних параметрів. Більшою перевагою ідентифікації по сітківці є сталість параметра: на сітківку не впливає нічого, крім сильних травм, її не можливо підробити;

3. термограмми – це зображення, отримані в різних областях інфрачервоного спектра, іноді з додатковим використанням видимого спектра. Термограмми в біометрії – це зображення частин тіла в короткохвильовому, середньому й довгохвильовому діапазонах інфрачервоного спектра. Велика перевага термограмм перед звичайними зображеннями - це їхня незалежність

від зміни висвітлення. На термограмми також не впливає зміна зовнішності, принаймні, вони не чутливі до деяких видів маскування. Одним з недоліків цього методу аутентифікації є висока вартість сенсорів;

4. хода – ставиться до поведінкових біометричних параметрів . Достоїнство цього методу - можливість розпізнавання людей на відстані, використовуючи відеозапис. Недолік - процедура розпізнавання дуже сильно залежить від умов, у яких перебуває об'єкт.

5. клавіатурний почерк – ідентифікація по клавіатурному почерку - це ідентифікація людини по власному стилю друкування. Система ідентифікації по клавіатурному почерку заснована на фіксованому паролі, але приблизно можуть бути й незалежними від тексту, що набирається, як системи розпізнавання голосу ;

6. відбиття шкіри – один з нових біометричних параметрів, що з'явилися завдяки розробці сенсорів. Перевагою даної технології є те, що для зразка маленького розміру потрібно й маленький чип - зо розміром й обсягу пам'яті й продуктивності. Також потрібно відзначити відсутність проблем з реєстрацією, які характерні для методу ідентифікації по відбитках пальців; 7 рух губ - ставиться до поведінкових біометричних параметрів, він може використовуватися як візуальне доповнення до системи розпізнавання мовця; технологія аутентифікації по русі губ має такого ж різновиду, що й методика розпізнавання мовця: з фіксованим текстом, залежна від тексту й незалежна від тексту. Одне із самих більших достоїнств цього методу - можливість легко сполучити його з ідентифікацією мовця й розпізнаванням по геометрії особи. У такий спосіб можна створити дуже точну систему, що буде складно обдурити.

## 2.10 Мультибіометричні технології

Розробка та застосування мультибіометричних рішень - перспективний напрямок розвитку галузевого ринку. У мультибіометричних системах розпізнавання здійснюється не по одному, а по кількох ідентифікаторах.

Мультибіометричні рішення стають все більш популярними: так, наприклад, в електронні паспорти та ідентифікаційні картки, що випускаються різними державами, вносяться не тільки цифрові фотографії власників цих документів, але і відомості про відбитки їхніх пальців.

Основні переваги мультибіометричних технологій:

- підвищення надійності та якості розпізнавання і одночасно - зниження рівня помилок, коли дозволяється доступ незареєстрованного користувача або відмову в доступі отримує зареєстрований користувач;
- більша різноманітність ідентифікаторів з можливістю їх альтернативного застосування (наприклад, розпізнавання за відбитками пальців у разі, якщо особа або голос користувача істотно змінені);
- прискорення процесу ідентифікації.

Крім мультибіометричних технологій, в один клас з ними прийнято об'єднувати мультимодальні та багатофакторні системи.

У мультимодальних системах ідентифікатори одного і того ж типу (наприклад, відбитки пальців) обробляються за допомогою різних алгоритмів. Головна мета - підвищення надійності ідентифікації.

У багатофакторних системах поряд з біометричними використовуються також і інші ідентифікатори (PIN-код, пароль, смарт-карта і т.д.). У цьому випадку для підтвердження своєї особи та / або повноважень, користувачеві необхідно пройти біометричну ідентифікацію і пред'явити (ввести) додаткові ідентифікатори з числа згаданих вище. Основні цілі застосування багатофакторних систем - прискорення процесу ідентифікації та / або надання можливості розпізнавання без звернення до централізованої бази даних ідентифікаторів (наприклад, коли відомості про відбитки пальців заносяться в пам'ять смарт-картки, яка пред'являється при ідентифікації, і модель відбитка, внесена в пам'ять карти, порівнюється з моделлю знову пред'явленого ідентифікатора).

## 2.11 Методичні вказівки до виконання лабораторних робіт

### Лабораторна робота № 1
### Одержання біометричного еталону клавіатурного почерку

### 1 Мета роботи

Навчитися визначати вектор біометричних параметрів за пред'явленими зразками клавіатурного почерку, а також будувати біометричний еталон користувача.

### 2 Ключові положення

#### 2.1 Загальні принципи побудови біометричних систем динамічної ідентифікації / аутентифікації

Динамічні системи біометричної ідентифікації / аутентифікації особи засновані на використанні в якості ознак деяких динамічних параметрів і характеристик особи (хода, рукописний і клавіатурний почерки, мова).

Біометричні системи, побудовані на аналізі індивідуальних особливостей динаміки рухів, мають багато загального. Це дозволяє використовувати одну узагальнену схему для опису всіх біометричних систем цього класу, яка наведена на рис. 2.16 і відбиває основні етапи обробки інформації [1].

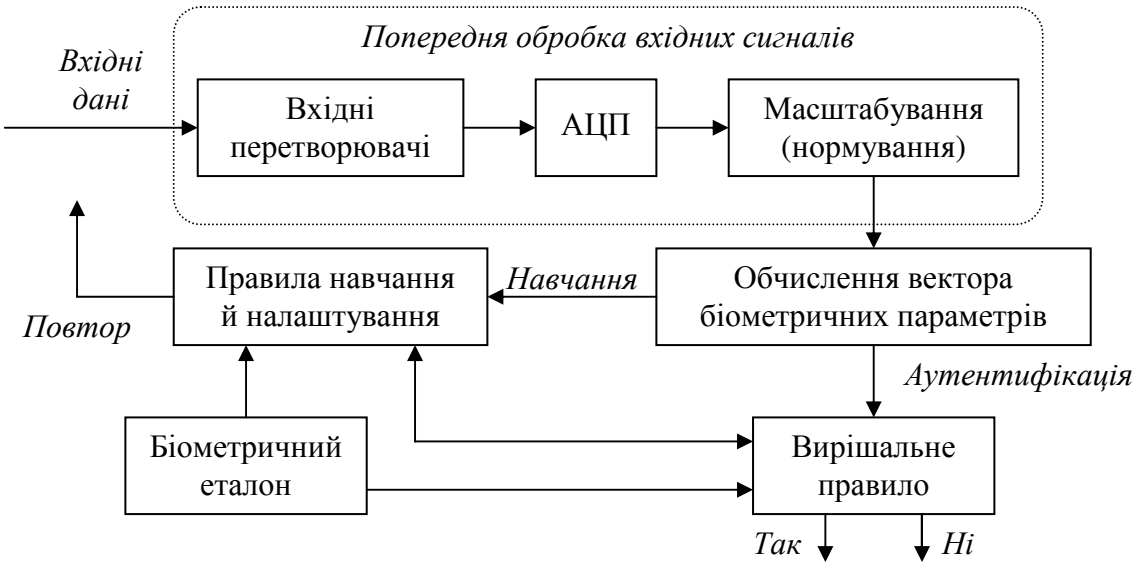



Рисунок 2.16 – Узагальнена структурна схема системи ідентифікації особи по особливостях динаміки рухів

Першим етапом обробки є перетворення неелектричних величин (координат кінця пера, звукового тиску, положення рук) в електричні сигнали. Далі ці сигнали оцифровуються й уводяться в процесор, що здійснює програмну обробку даних. При програмній обробці виконується масштабування амплітуд вхідних сигналів, що приводить їх до єдиного

масштабу часу, дроблення сигналів на окремі фрагменти з наступним зсувом фрагментів сигналу до оптимального суміщення з еталонним розташуванням.

Після приведення до еталонного значення масштабів і зсуву фрагментів сигналів здійснюється обчислення вектора функціоналів (вектора контрольованих біометричних параметрів – $\mathbf{V} = (v_1, v_2, \ldots, v_k)$.

Перераховані вище п'ять перших блоків обробки інформації працюють по тих самих алгоритмах, незалежно від режиму роботи самої біометричної системи. Саме із цієї причини вони утворюють послідовне з'єднання блоків без розгалужень. Режим роботи системи (навчання або аутентифікація) визначає сукупність операцій, здійснюваних із уже сформованим вектором параметрів $\mathbf{V} = (v_1, v_2, \ldots, v_k)$.

У випадку якщо біометрична система перебуває в режимі навчання, вектори біометричних параметрів **V** надходять у блок правил навчання, який формує біометричний еталон особи. Тому що динамічні образи особи мають істотну мінливість, для формування біометричного еталона потрібно кілька прикладів реалізацій того самого образа. У найпростішому випадку біометричний еталон може формуватися у вигляді двох векторів: вектора математичних очікувань контрольованих параметрів $m(v)$ і вектора дисперсій цих параметрів $\sigma(v)$.

У режимі аутентифікації вектор контрольованих біометричних параметрів **V**, отриманий із пред'явленого образа порівнюється вирішальним правилом з біометричним еталоном. Якщо пред'явлений вектор виявляється близький до біометричного еталона, приймається позитивне аутентифікаційне рішення. При значних відмінностях пред'явленого вектора від його біометричного еталона здійснюється відмова в допуску. Якщо протокол аутентифікації не занадто жорсткий, то користувачеві надаються додаткові спроби повторної аутентифікації.

Вигляд використовуваного системою вирішального правила й вигляд біометричного еталона нерозривно пов'язані. При розробці системи, виходячи з обраного вирішального правила, визначається вигляд біометричного еталона.

Застосування принципів біометричної ідентифікації особи в системах інформаційної безпеки призвело до створення біометричних систем ідентифікації / аутентифікації (БСІ) при доступі до об'єктів інформатизації (зокрема, до персональних комп'ютерів). Користувачі таких об'єктів для одержання доступу до них повинні пройти процедуру біометричної ідентифікації / аутентифікації.

Якість роботи БСІ характеризується відсотком помилок при проходженні процедури допуску. У БСІ розрізняють помилки трьох видів:

- FRR (False Reject Rate) або помилка першого роду – імовірність помилкових відмов авторизованому користувачеві (помилкова відмова «своєму»);
- FAR (False Accept Rate) або помилка другого роду – це ймовірність допуску незареєстрованного користувача (помилковий пропуск «чужого»);

- EER (Equal Error Rates) – рівна ймовірність (норма) помилок першого й другого роду.

Залежно від вимог, пропонованих до БСІ, формування біометричного еталона користувача також виконується із заданим ступенем строгості. Зразки, пропоновані даним користувачем, повинні відповідати деякій середньостатистичній характеристиці для даного користувача. Тобто після набору деякої початкової статистики пред'явлення поганих зразків (зразків з великими відхиленнями від середньостатистичних) системою повинне відкидатися. Відношення прийнятих системою зразків до загального числа пред'явлених зразків характеризує ступінь стійкості біометричних параметрів даного користувача.

Для експериментальної перевірки характеристики FRR системі послідовно $n$ раз пред'являються біометричні характеристики користувачів, що успішно пройшли реєстрацію. Далі підраховується відношення числа $n_1$ невдалих спроб (відмова системи в допуску) до загального числа спроб $n$. Зазначене відношення дає оцінку ймовірності помилки FRR. Оцінка вважається достовірною при значеннях $n \geq 1/\text{FRR}$.

Для експериментальної перевірки характеристики FAR системі послідовно $m$ раз пред'являються біометричні характеристики користувачів, що не проходили реєстрацію. Далі підраховується відношення числа $n_2$ удалих спроб (позитивне аутентифікаційне рішення) до загального числа спроб $m$. Зазначене відношення дає оцінку ймовірності помилки FAR. Оцінка вважається достовірною при значеннях $m \geq 1/\text{FAR}$.

## 2.2 Одержання вектора біометричних параметрів при аналізі клавіатурного почерку

В БСІ по клавіатурному почерку претендентом на допуск із клавіатури комп'ютера вводиться певна парольна фраза. Контрольованими параметрами уведення є час $t_1, t_2, t_3, ..., t_n$ натискання кожної клавіші з послідовності клавіш, що відповідає парольній фразі, а також інтервали часу між натисканням сусідніх клавіш $\tau_1, \tau_2, \tau_3, ..., \tau_{n-1}$, (рис. 2.17) [8].

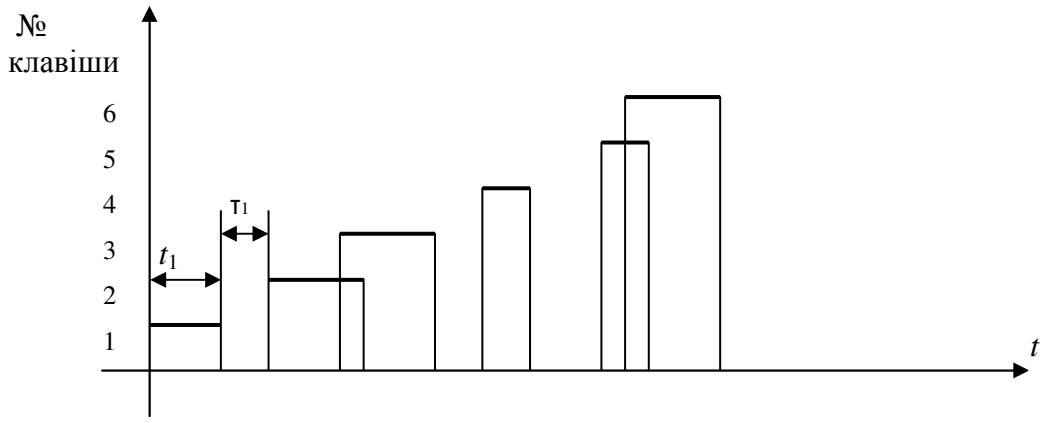



Рисунок 2.17 – Часова діаграма набору парольної фрази

Можливе перекриття часу при натисканні користувачем сусідніх клавіш. У цьому випадку параметр $\tau_k$ стає негативним. Контрольовані параметри $t_k$ й $\tau_k$ істотно залежать від того, скільки пальців використовується при наборі, а також від характерних для користувача сполучень рухів руки пальців рук при наборі певних символів на стандартній клавіатурі.

Один з методів одержання вектора біометричних параметрів користувача при аналізі його клавіатурного почерку полягає в наступному. При введенні парольної фрази в якості інформативних параметрів, що відбивають індивідуальні особливості клавіатурного почерку користувача, використовуються тільки час натискань клавіш $t_1$, $t_2$, $t_3$, ..., $t_n$ й інтервали часу між натисканням сусідніх клавіш $\tau_1,\tau_2,\tau_3$, ...,$\tau_{n-1}$, тобто винятково параметри часу. Послідовність натискання клавіш при введенні фіксованої парольної фрази для даного користувача однакова, тому цю послідовність можна виключити з розгляду (рис. 2.17). З урахуванням цих обставин штучно конструюється спеціальна часова функція, що відбиває весь процес набору парольної фрази в часі за період уведення фрази й несе в собі всю необхідну інформацію про особливості клавіатурного почерку користувача. Як така функція обрана кусочно-постійна періодична функція $f(t)$, що формується за наступними правилами:

Період $T$ функції $f(t)$ відповідає часу набору на клавіатурі парольної фрази. Функція $f(t)$ формується в процесі набору парольної фрази як апостеріорне сполучення трьох характерних ділянок. Перша ділянка має постійну амплітуду $A$ и довжину, що відповідає часу натискання чергової клавіші. Друга ділянка має нульову амплітуду ($A$=0) і довжину, що відповідає часу паузи між натисканнями чергових клавіш. Третя ділянка має постійну амплітуду $k{\cdot}A$ та довжину, що відповідає часу перекриття при одночасному натисканні двох послідовних клавіш.

Коефіцієнт $k$ ураховує ступінь впливу перекриттів у загальній сукупності інформативних параметрів й у лабораторних експериментах прийнятий $k$ = 2.

З урахуванням уведених правил, часову діаграму початку парольної фрази (рис. 2.17) можна представити функцією $f(t)$, що буде мати вигляд, показаний на рис. 2.18.

Безпосереднє використання функції $f(t)$ для одержання вектора інформативних біометричних параметрів конкретного користувача незручно, оскільки вона залежить від часу. Як і при аналізі рукописного почерку перехід від функції часу $f(t)$ до вектора **V** реалізується за допомогою розкладання $f(t)$ у який-небудь ряд, члени якого будуть компонентами вектора **V**.

Враховуючи особливості виду функції $f(t)$, одним з найбільш ефективних методів її розкладання є розкладання по ортогональному базису несинусоїдальних функцій Хаара.

Функції Хаара утворюють періодичну, ортонормовану, повну систему непарних функцій. Кожна функція Хаара {$har$ ($r$, $m$, $t$)}, за винятком першої, являє собою прямокутний двополярний імпульс різної амплітуди, що займає строго певне положення на напіввідчиненому інтервалі [0, 1). Перша функція Хаара $har$ (0, 0, $t$), на відміну від всіх інших, являє собою прямокутний імпульс позитивної полярності й одиничної амплітуди на всьому інтервалі [0, 1).

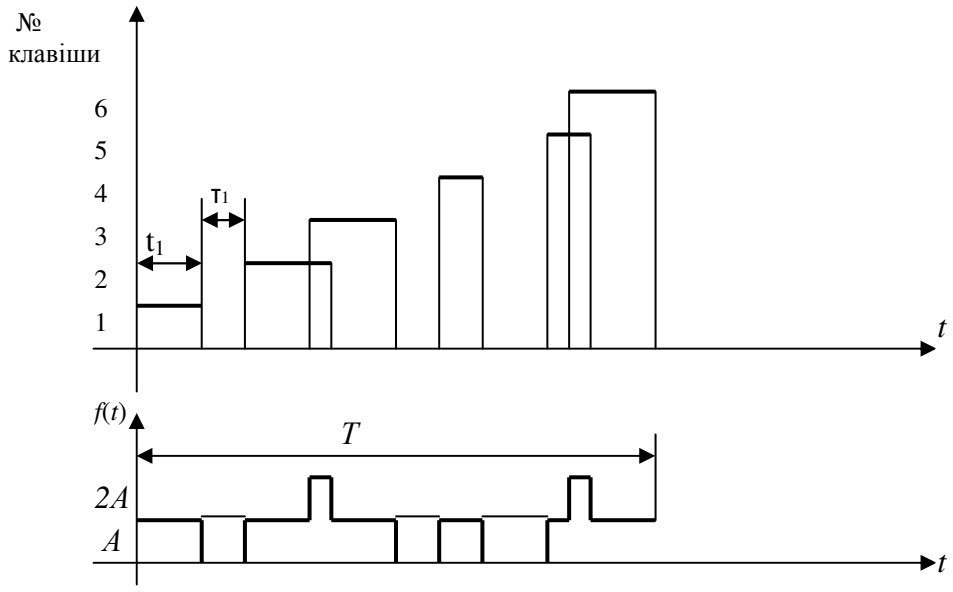



Рисунок 2.18 – Принцип конструювання функції $f(t)$
з часової діаграми набору парольної фрази

Функції Хаара $har\ (r,\ m,\ t)$ можна отримати з рекуррентного співвідношення: $har(0,0,t) = 1, t \in [0,1)$;

$$har(r,m,t) = \begin{cases} 2^{\frac{r}{2}}, \text{якщо } \dfrac{m-1}{2^r} \le t < \dfrac{m-\frac{1}{2}}{2^r} \\ 0, \text{при інших } t \in [0,1), \\ -2^{\frac{r}{2}}, \text{якщо } \dfrac{m-1}{2^r} \le t < \dfrac{m}{2^r} \end{cases} \qquad (2.1)$$

де $0 \le r < \log_2 N$ і $1 \le m \le 2^r$.

Дискретизація системи функцій Хаара приводить до матриці Хаара $\mathbf{H}^*(n)$, де $n=\log_2 N$. Так, для $N = 8$, матриця Хаара $\mathbf{H}^*(3)$ буде мати вигляд:

$$\mathbf{H}^*(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \end{bmatrix} \qquad (2.2)$$

Кожен рядок матриці є дискретною функцією Хаара *Har*(*r,m, t*).

Для перетворення вихідної біометричної функції $f(t)$ у вектор біометричних параметрів **V** на основі розкладання Хаара, функцію $f(t)$ необхідно попередньо дискретизувати за часом відповідно до параметрів дискретизації функцій Хаара. Дискретний вигляд $F(t_k)$ функції $f(t)$ буде мати вигляд:

$$F(t_k) = \{f(t_0), f(t_1), \ldots, f(t_{N-1})\}, k = 0, 1, \ldots, N-1... \quad (2.3)$$

Тоді шуканий вектор біометричних параметрів **V** можна представити у вигляді коефіцієнтів перетворення Хаара:

$$\mathbf{V}_f(n) = \frac{1}{N}\mathbf{H}^*(n)F(t_k), \quad (2.4)$$

де $n = \log_2 N$.

За правилом перемножування матриць компоненти вектора $\mathbf{V}_f(n) = \{v_{f0}(n), v_{f1}(n), \ldots, v_{f(N-1)}(n)\}$ визначаються в такий спосіб:

$$\begin{aligned}
\mathbf{V}_{f0}(n) &= \frac{1}{N}\sum_{k=0}^{N-1} f(t_k)h_{k0}; \\
\mathbf{V}_{f1}(n) &= \frac{1}{N}\sum_{k=0}^{N-1} f(t_k)h_{k1}; \\
&\ldots \\
\mathbf{V}_{f(N-1)}(n) &= \frac{1}{N}\sum_{k=0}^{N-1} f(t_k)h_{k(N-1)},
\end{aligned} \quad (2.5)$$

де функції $h_{kr}$ обчислюються згідно (3.1).

На практиці, для збереження інформативної високочастотної складової функції $f(t)$, уводиться додаткова дискретизація функції $F(t_k)$ з більш дрібним кроком, при цьому крок дискретизації базисних функцій Хаара залишається колишнім. Щоб уникнути пропорційного збільшення часу обчислень, вони виконуються не безпосередньо по формулах (3.5), а за спеціальний алгоритмом. Цей алгоритм аналізує логічні умови взаємного сполучення відліків функцій $f(t_k)$ і $h_k$, а обчислення здійснює за допомогою формули прямокутників.

### 2.2 Обчислення біометричного еталону

Вектор біометричних параметрів **V** є вихідним для наступної процедури аутентифікації, що може будуватися різними способами.

У даному циклі лабораторних робіт використовується, зокрема, спосіб аутентифікації, заснований на вимірі близькості пред'явленого для аутентифікації вектора **V** до еталона за допомогою міри близькості Хеммінга.

Завдання в біометричному еталоні інтервалів припустимих значень вимірюваних параметрів може здійснюватися двома способами. На малих

навчальних вибірках доцільно здійснювати пряме обчислення мінімуму й максимуму обмірюваних значень контрольованих параметрів. При обсязі навчальної вибірки в 5 і більше прикладів стає доцільним обчислення математичного очікування значень параметрів $m(v_i)$ і їхніх дисперсій $\sigma(v_i)$. У цьому випадку значення мінімальної й максимальної границь прийнято обчислювати в такий спосіб:

$$\min(v_i) = m(v_i) - C[L,(1-P_1)]\sigma(v_i) \tag{2.6}$$

$$\max(v_i) = m(v_i) + C[L,(1-P_1)]\sigma(v_i), \tag{2.7}$$

де $L$ – число використаних при навчанні прикладів;

$P_1$ – задане значення ймовірності помилок першого роду (у цих операціях $P_1$ приймають звичайно рівним 0,1);

$C[L,(1-P_1)]$– коефіцієнт Стьюдента, наведений у табл. 2.2.

Таблиця 2.2 - Коефіцієнти Стьюдента $C[L,(1-P_1)]$

| **Кіль-кість зразків $L$** | **Ймовірність помилки першого роду – $P_1$ (ймовірність відмови в допуску справжньому користувачеві)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **0,1** | **0,05** | **0,03** | **0,025** | **0,02** | **0,015** | **0,01** | **0,005** | **0,0025** |
| **2** | 3,07 | 6,31 | 10,56 | 12,5 | 15,9 | 21,21 | 31,82 | 63,7 | 127,3 |
| **3** | 1,88 | 2,92 | 3,89 | 4,3 | 4,85 | 5,64 | 6,97 | 9,92 | 14,1 |
| **4** | 1,63 | 2,35 | 2,95 | 3,18 | 3,48 | 3,82 | 4,54 | 5,84 | 7,54 |
| **5** | 1,53 | 2,13 | 2,60 | 2,78 | 2,99 | 3,25 | 3,75 | 4,60 | 5,60 |
| **6** | 1,47 | 2,01 | 2,44 | 2,57 | 2,75 | 3,01 | 3,37 | 4,03 | 4,77 |
| **7** | 1,43 | 1,94 | 2,31 | 2,45 | 2,61 | 2,83 | 3,14 | 3,71 | 4,32 |
| **8** | 1,41 | 1,89 | 2,24 | 2,36 | 2,51 | 2,72 | 3,00 | 3,50 | 4,03 |
| **9** | 1,39 | 1,86 | 2,19 | 2,37 | 2,45 | 2,63 | 2,90 | 3,36 | 3,83 |
| **10** | 1,38 | 1,83 | 2,15 | 2,26 | 2,40 | 2,57 | 2,82 | 3,25 | 3,69 |
| **12** | 1,36 | 1,80 | 2,09 | 2,16 | 2,33 | 2,49 | 2,72 | 3,11 | 3,49 |
| **14** | 1,35 | 1,77 | 2,06 | 2,14 | 2,28 | 2,43 | 2,65 | 3,01 | 3,37 |
| **16** | 1,34 | 1,75 | 2,03 | 2,12 | 2,24 | 2,39 | 2,60 | 2,95 | 3,28 |
| **18** | 1,33 | 1,74 | 2,01 | 2,10 | 2,22 | 2,36 | 2,57 | 2,9 | 3,22 |
| **21** | 1,33 | 1,73 | 1,99 | 2,09 | 2,19 | 2,33 | 2,53 | 2,85 | 3,15 |
| **26** | 1,32 | 1,71 | 1,97 | 2,06 | 2,16 | 2,30 | 2,49 | 2,79 | 3,07 |
| **31** | 1,31 | 1,70 | 1,95 | 2,04 | 2,14 | 2,27 | 2,46 | 2,75 | 3,03 |
| **41** | 1,30 | 1,68 | 1,93 | 2,02 | 2,12 | 2,25 | 2,42 | 2,7 | 2,97 |
| **∞** | 1,28 | 1,65 | 1,89 | 1,96 | 2,06 | 2,18 | 2,33 | 2,58 | 2,81 |

При обчисленні математичного очікування контрольованого параметра може використатися звичайна формула

$$m(v_i) \approx \frac{1}{L}\sum_{j=1}^{L} v_{ij} \tag{2.8}$$

Якщо зберігаються всі значення обмірюваних параметрів при обчисленні дисперсії, то може бути використана звичайна формула обчислення

$$\sigma^2(v_i) \approx \frac{1}{L-1}\sum_{j=1}^{L}[x_{ij} - m(v_i)]^2 \tag{2.9}$$

## 3 Лабораторне устаткування

Для отримання клавограми користувача використовується утиліта Typing statistics, головне вікно якої показано на рис. 2.19. Для запуска утиліти необхідно скористатися ярликом Ts на робочому столі комп'ютера.

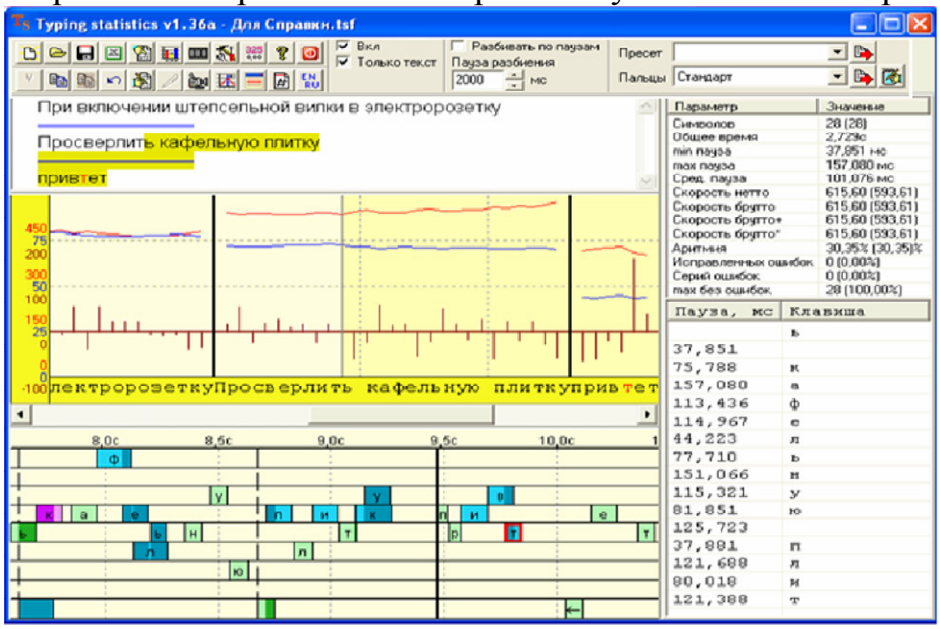



Рисунок 2.19 - Головне вікно програми Typing statistics

Після того, як Ви запустили Ts, можете згорнути його й переключитися в який-небудь текстовий редактор або натиснути кнопку на панелі інструментів для того, щоб вводити текст в програмі.

У секції тексту відображається перехоплений текст. Символи, які під час набору були вилучені клавішею BackSpace, відображаються червоними кольорами.

Під секцією графіків відображається клавограма.

Клавограма - це часова діаграма клавіатурних подій. Складається з дев'яти лінійок, перші вісім з яких відповідають восьми робочим пальцям, починаючи з лівого мізинця й закінчуючи правим. На дев'ятій відображається пробіл і всі службові клавіші. Над лінійками - вісь часу.

Натискання клавіш відображаються кольоровими прямокутниками, на яких написані назви натиснутих клавіш. Довжини прямокутників пропорційні часам утримання клавіш. Кольори прямокутників залежить від ступеня перекриття, з яким натиснута клавіша. Ступінь перекриття – це кількість клавіш, що втримувалося в момент натискання даної клавіші. Наприклад, на рис. 2.19 клавіша «к» у слові «кафельную» була натиснута в той момент, коли клавіші «ь» і пробіл утримувалися. Таким чином, це дворазове перекриття. Клавіші, що натискають із нульовим перекриттям відображаються зеленим, з однократним - блакитним, із дворазовим - фіолетовим, із трикратним - червоним, із чотириразовим і більше - жовтогарячим. Зона перекриття виділяється темним відтінком тих же кольорів. Вилучені символи виділяються червоною рамкою.

Справа у секції статистики відображаються основні статистичні дані тексту, що набирався, а також паузи та натискання кожної окремої клавіші. Для того, щоб скопіювати дані в Excel, необхідно натиснути кнопку  на панелі інструментів і перейти на лист Дані.

Для отримання вектору біометричних ознак використовується програма Handwriting, яка при введенні пауз та натискань тексту розраховує функцію $f(t)$ та вектор ознак **V**, а також будує графік функції $f(t)$.

## 4 Порядок підготовки й виконання роботи

***Підготовка до проведення роботи***

1. Ознайомитись з ключовими положеннями та відповісти на ключові запитання.

2. Вибрати (придумати, скласти) пароль (парольну фразу) з не більш ніж 20 символів, що вводяться із клавіатури комп'ютера й прорепетувати його введення шляхом багаторазового повторення набору до появи автоматизму (клавіатурного почерку). При введенні бажане використовувати як можна більше число пальців обох рук. Для пароля припустиме використання всіх клавіш клавіатури. Функціональні й керуючі клавіші при введенні на екрані не відображаються, але використовуються в процесі розпізнавання. Пароль повинен бути однаковим для всієї академічної групи.

3. Підготувати бланк звіту про виконання лабораторної роботи, який повинен містити:

- назву та мету роботи;
- зразок парольного слова, що вводиться;
- заготовки таблиці експериментальних даних;
- висновки по роботі.

***Виконання роботи***

4. Запустити програму Typing statistics, скориставшись ярликом  на робочому столі комп’ютера.

5. Відкрити вікно текстового набору (або запустивши будь-який текстовий редактор, або натиснувши кнопку  на панелі інструментів).

6. Ввести підготовлену парольну фразу. Проаналізувати отриману клавограму, повернувшись до програми Ts.

7. Передати інформацію про паузи і натискання у Excel, натиснувши кнопку  на панелі інструментів. Перейти на лист Дані і скопіювати інформацію у буфер обміну. При цьому необхідно зауважити, що пусті комірки недопустимі. В них треба проставити значення «0».

8. Запустити MATLAB. У вікні команд набрати текст Handwriting – запуститься програма Handwriting.

9. Натиснути кнопку Пуск у програмі та вставити інформацію з буферу обміну у форму, що відкрилася. Отримані результати (функцію $f(t)$, вектор **V** та графік) записати у протокол лабораторної роботи.

10. Повернутись до програми Ts та створити новий запис, натиснувши кнопку  .

11. Пункти 5-10 повторити за завданням викладача $L$ разів ($L \geq 5$) для здійснення етапу навчання.

12. За результатами проведення лабораторної роботи заповнити табл. 2.3.

Таблиця 2.3 – Біометричний еталон користувача

| | $v_1$ | $v_2$ | $v_3$ | $v_4$ | $v_5$ | $v_6$ | $v_7$ | $v_8$ |
|---|---|---|---|---|---|---|---|---|
| $\mathbf{V}_1$ | | | | | | | | |
| $\mathbf{V}_2$ | | | | | | | | |
| … | | | | | | | | |
| $\mathbf{V}_L$ | | | | | | | | |
| $m(v_i)$ | | | | | | | | |
| $\sigma(v_i)$. | | | | | | | | |
| $\min(v_i)$ | | | | | | | | |
| $\max(v_i)$ | | | | | | | | |

13. Заповнити таблицю векторів ознак для всієї групи (одну на групу), вибравши один з векторів біометричних параметрів кожного студента.

Таблиця 2.4 – Вектори біометричних ознак групи

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Група _____ | |
| № за списком | $v_1$ | $v_2$ | $v_3$ | $v_4$ | $v_5$ | $v_6$ | $v_7$ | $v_8$ |
| **1** | | | | | | | | |
| **2** | | | | | | | | |
| **…** | | | | | | | | |
| **30** | | | | | | | | |

14. Зробити висновки.

## 5 Ключові запитання

1. У чому відмінність статичних і динамічних систем біометричної ідентифікації/аутентифікації? Які переваги й недоліки тих і інших?

2. У чому полягають загальні принципи побудови біометричних систем динамічної ідентифікації/аутентифікації?

3. На чому засновані методи біометричної аутентифікації користувача за клавіатурним почерком?

4. Що лежить в основі біометричних параметрів клавіатурного почерку?

5. Якими способами можна одержати вектор параметрів почерку користувача?

6. Чим характеризується якість роботи БСІ?

7. Для чого в біометричних системах аутентифікації використовують коефіцієнт Стьюдента?

## Лабораторна робота № 2

## Біометрична аутентифікація користувача ПК за клавіатурним почерком на основі вимірювання близькості образу до біометричного еталону мірою Хемінга

### 1 Мета роботи

Дослідження системи біометричної аутентифікації користувача ПК за клавіатурним почерком, що використовує в якості міри близькості зразка підпису до біометричного еталону – міру Хемінга.

### 2 Ключові положення

Нехай на етапі реєстрації (навчання) авторизований користувач пред'явив $L$ своїх підписів, що відповідає $L$ реалізаціям вектора біометричних параметрів $\mathbf{V} = \{\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_L\}$...

Шляхом аналізу наявні $L$ реалізацій вектора $\mathbf{V}$ можна визначити характерний для даного користувача інтервал зміни кожного конкретного параметра $[\min(v_i), \max(v_i)]$, $i = 1, N$ , що запам'ятовується в системі як біометричний еталон даного користувача.

Нехай на етапі аутентифікації користувач що ідентифікувався пред'явив підпис, який буде відповідати деякий вектор інформативних біометричних параметрів $\mathbf{V} = \{v_1, v_2, \ldots, v_N\}$... Система аутентифікації робить аналіз пред'явлених параметрів $v_i$, $i = 1, N$ на влучення у встановлені біометричним еталоном зареєстрованого під заявленим ім'ям користувача інтервали, формуючи вектор $\mathbf{E} = \{e_1, e_2, \ldots, e_N\}$... Якщо параметр $v_i$ попадає в інтервал, то $e_i = 0$, у противному випадку $e_i = 1$. У результаті аналізу буде сформований вектор Хеммінга $\mathbf{E}$ претендента на доступ. Для «свого» користувача цей вектор повинен складатися практично з одних нулів. Для «чужого», що предъявив інші біометричні параметри, вектор $\mathbf{E}$ буде мати багато розбіжностей з біометричним еталоном (багато одиниць). Абсолютне значення відстані Хеммінга $\mathbf{E}_\mathbf{V}$ до біометричного еталона визначається як загальне число розбіжностей з біометричним еталоном. Відстань Хеммінга $\mathbf{E}_\mathbf{V}$ завжди позитивна й може змінюватися від 0 до $N$.

Після того як сформований біометричний еталон, можлива реалізація процедур аутентифікації зареєстрованого користувача. При здійсненні процедур аутентифікації «свій» користувач досить рідко помиляється й, відповідно, міра Хеммінга виявляється малою. При спробах аутентифікації «чужих» користувачів помилки виявляються набагато більш часто.

При використанні досить великого числа контрольованих біометричних параметрів розподіл значень міри Хеммінга близький до нормального. У цьому випадку граничне значення міри Хеммінга $\mathbf{E}_\text{п}$ можна визначити через математичне очікування й дисперсію значень міри Хеммінга для «свого» користувача

$$\mathbf{E}_{\text{п}} = m(\mathbf{E}_C) + C[L, (1- P_1)]\ \sigma(\mathbf{E}_C), \qquad (2.10)$$

де $C[L, (1-P_1)]$ – коефіцієнт Стьюдента, що задається, виходячи із числа використаних прикладів $L$ і величини помилки першого роду (імовірності $P_1$ помилкової відмови «своєму» користувачеві, див. табл. 2.2).

## 3 Лабораторне устаткування

Лабораторне устаткування таке саме, як і в лабораторній роботі № 1.

## 4 Порядок підготовки й виконання роботи

***Підготовка до проведення роботи***

1. Ознайомитись з ключовими положеннями та відповісти на ключові запитання.

2. На основі табл. 2.3 сформувати вектор $\mathbf{E}_C$ $\{\mathbf{E}_{C1}, \mathbf{E}_{C2, \ldots,} \mathbf{E}_{CL}\}$ і розрахувати його математичне очікування та дисперсію. Розрахунки представити в вигляді таблиці 2.5.

Таблиця 2.5 – Вектори біометричного еталону за мірою Хемінга

| | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $e_6$ | $e_7$ | $e_8$ | $\sum = \mathbf{E}_C$ |
|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{E}_{C1}$ | | | | | | | | | |
| $\mathbf{E}_{C2}$ | | | | | | | | | |
| … | | | | | | | | | |
| $\mathbf{E}_{CL}$ | | | | | | | | | |

3. Розрахувати граничне значення міри Хеммінга $\mathbf{E}_{\text{п}}$.

4. Підготувати бланк звіту про виконання лабораторної роботи, який повинен містити:

- назву та мету роботи;
- таблицю векторів біометричного еталону за мірою Хемінга;
- розраховані значення $m(\mathbf{E}_C)$, $\sigma(\mathbf{E}_C)$, $\mathbf{E}_{\text{п}}$;
- заготовки таблиці експериментальних даних;
- висновки по роботі.

***Виконання роботи***

5. Пройти процедуру аутентифікації «свого» користувача. Для цього запустити програму Typing statistics, набрати парольну фразу і отримати вектор біометричних ознак за допомогою програми Handwriting. Перевірку провести 10 разів, щоразу формуючи вектор Хемінга і оцінюючи, чи пройшла аутентифікація успішно. Результати занести в табл. 2.3 (без розрахунків математичного очікування, дисперсії та мінімального та максимального значень) та табл. 2.6.

Таблиця 2.6 – Результати аутентифікації користувача

| | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $e_6$ | $e_7$ | $e_8$ | $\sum$ | Так/ні |
|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{E}_1$ | | | | | | | | | | |
| $\mathbf{E}_2$ | | | | | | | | | | |
| … | | | | | | | | | | |
| $\mathbf{E}_{10}$ | | | | | | | | | | |

6. Зробити оцінку помилки першого роду

7. Пройти процедуру аутентифікації «чужого» користувача. Для цього скористатися табл. 2.4. Сформувати вектори Хемінга для кожного «чужого» користувача, щоразу оцінюючи, чи пройшла аутентифікація успішно. Результати занести у табл. 2.6.

8. Зробити оцінку помилки другого роду.

9. Зробити висновки по роботі.

## 5 Ключові запитання

1. Які існують засоби вимірювання близькості між біометричними параметрами клавіатурного почерку «свого» та «чужого» користувача?

2. У чому полягає сутність методу вимірювання близькості між біометричними параметрами клавіатурного почерку «свого» та «чужого» користувача мірою Хемінга?

3. Які види помилок використовуються для характеристики біометричних систем ідентифікації / аутентифікації?

4. Які переваги та недоліки є у методі біометричної аутентифікації користувача по клавіатурному почерку, заснованому на вимірюванні близькості між біометричними параметрами клавіатурного почерку «свого» та «чужого» користувача мірою Хемінга?

## Лабораторна робота № 3

## Аутентифікація користувача на основі контролю влучення в область розподілу еталонних зразків

### 1 Мета роботи

Дослідження системи біометричної аутентифікації користувача ПК за клавіатурним почерком, що використовує в якості міри близькості зразка підпису до біометричного еталону – контроль влучення в область розподілу еталонних зразків.

### 2 Ключові положення

Нехай на етапі реєстрації (навчання) авторизований користувач пред'явив $L$ своїх підписів, що відповідає $L$ реалізаціям вектора біометричних параметрів $\mathbf{V} = \{\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_L\}$.

Для завдань динамічної біометрії в більшості випадків можна вважати, що розподіл вектора $\mathbf{V}$ в $N$-мірному просторі близький до нормального й, отже, вектори $\mathbf{V}_i$, $i = 1, L$ лежать усередині $N$-мірної області, що при $L \to \infty$ в ортогональній системі координат описується гіпереліпсоїдом розсіювання. Причому, у загальному випадку компоненти біометричних векторів $\mathbf{V}_i$, $i = 1, L$ корельовані між собою, тобто головні осі гіпереліпсоїда розсіювання не паралельні осям координат. Отже, одержавши формулу такого гіпереліпсоїда, аутентифікацію користувача можна здійснювати шляхом контролю влучення вектора його біометричних параметрів $\mathbf{V}$ усередину $N$-мірної області, описуваної гіпереліпсоїдом розсіювання.

Для нормального закону розподілу $N$-мірних випадкових корельованих величин функція щільності розподілу має вигляд:

$$f(v_1, v_2, \cdots v_N) = \frac{1}{\sqrt{(2\pi)^N \det_j(\lambda_{jk})}} \exp\left[-\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N}\Lambda_{jk}(v_j - m(v_j))(v_k - m(v_k))\right], \quad (2.11)$$

де

$$\lambda_{jk} = \lambda_{kj} = M(v_j - m(v_j))(v_k - m(v_k)) = \begin{cases} \sigma_j^2 \text{ при } j = k, \\ \operatorname{cov}\{v_j, v_k\} \text{ при } j \neq k, \end{cases} \quad (2.12)$$

$j, k = 1,2,\cdots,N$

Коефіцієнти $\lambda_{jk}$ становлять кореляційну матрицю $[\lambda]$, а коефіцієнти $\Lambda_{jk}$ становлять матрицю $[\Lambda]$, зворотну кореляційній матриці. Для обчислення коефіцієнтів матриці $[\Lambda]$ використовується формула:

$$\Lambda_{jk} = (-1)^{j+k}\frac{M_{jk}}{|\lambda|}, \quad (2.13)$$

де $\lambda$ – визначник кореляційної матриці, а $M_{jk}$ – мінор цього визначника, одержуваний з нього викреслюванням $j$ -й рядка й $k$ -го стовпця. Помітимо, що

$$|\Lambda| = \frac{1}{|\lambda|}. \tag{2.14}$$

Гіпереліпсоїд розсіювання має рівну щільність розподілу $N$-мірних випадкових величин, тому вираз для нього можна одержати з умови

$$f(v_1, v_2, \cdots, v_N) = \text{const}. \tag{2.15}$$

З виразу (2.11) видно, що умова (2.15) буде виконуватися, якщо

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N}\Lambda_{jk}(v_j - m(v_j))\big(v_k - m(v_k)\big) = \text{const}. \tag{2.16}$$

Причому із всіх можливих реалізацій рівняння (2.16) для різних констант у правій частині вибирається єдине, відповідне так називаному одиничному гіпереліпсоїду, у якого головні півосі відповідають середньоквадратичним відхиленням $\sigma_1, \sigma_2, \ldots, \sigma_N$:

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N}\Lambda_{jk}(v_j - m(v_j))\big(v_k - m(v_k)\big) = 1. \tag{2.17}$$

Через обмежену статистику біометричних зразків, пропонованих на стадії реєстрації «своїм» користувачем завжди залишається ймовірність того, що зразок, пред'явлений цим же користувачем при аутентифікації, вийде за межі зафіксованого в еталоні діапазону. Для зменшення цієї ймовірності додатково задається величина допуску між областями «свій» й «чужий» у вигляді коефіцієнта Стьюдента $C[L,(1-P_1)]$, виходячи з заданої помилки першого роду (імовірність $P_1$ помилкового недопуску «свого» і числа $L$ пред'явлених на стадії реєстрації зразків. Введення зазначеного допуску в рівняння (2.17) приводить його до виду:

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N}\Lambda_{jk}(v_j - m(v_j))\big(v_k - m(v_k)\big) = C\big[L,(1-P_1)\big]^2. \tag{2.18}$$

Процедура аутентифікації зводиться до перевірки: чи попадає пред'явлений користувачем вектор біометричних параметрів **V** в область, описувану виразом (2.18). Для цього вирішується нерівність

$$\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{n}\Lambda_{jk}(v_j - \xi_j)\big(v_k - \xi_k\big) \le C\big[L,(1-P_1)\big]^2. \tag{2.19}$$

Якщо нерівність для пред'явленого користувачем вектора біометричних параметрів **V** задовольняється, то вважається, що цей вектор належить «своєму» користувачеві й доступ дозволяється, у противному випадку вважається, що пред'явлений вектор належить «чужому» й у доступі відмовляється.

## 3 Порядок підготовки й виконання роботи

***Підготовка до проведення роботи***

1. Ознайомитись з ключовими положеннями та відповісти на ключові запитання.

2. Підготувати бланк звіту про виконання лабораторної роботи, який повинен містити:

- назву та мету роботи;
- зразок парольного слова, що вводиться;
- заготовки таблиці експериментальних даних;
- висновки по роботі.

***Виконання роботи***

3. Пройти процедуру реєстрації користувача. Для цього запустити програму MATLAB та у вікні команд набрати текст Handwriting_hiper. У вікні, що з'явилося, натиснути кнопку Реєстрація та ввести через пробіл значення всіх векторів **V**, що занесені в таблицю 2.3 при виконанні першої роботи циклу.

4. Пройти процедуру аутентифікації «свого» користувача. Для цього натиснути кнопку Аутентифікація та ввести вектор (тільки один) з таблиці 2.3, що отримана при виконанні другої роботи циклу.

5. П. 4 повторити 10 разів, фіксуючи, чи була авторизація успішною. Розрахувати коефіцієнт помилки першого роду.

6. Пройти процедуру аутентифікації «чужого» користувача. Для цього натиснути кнопку Аутентифікація та ввести вектор (тільки один) з таблиці 2.4, що отримана при виконанні другої роботи циклу.

7. П. 6 повторити для всіх «чужих» користувачів, фіксуючи, чи була авторизація успішною. Розрахувати коефіцієнт помилки другого роду.

8. Зробити порівняльний аналіз двох методів аутентифікації користувачів за допомогою клавіатурного почерку.

## 4 Ключові запитання

1. Що таке гіпереліпсоїд розсіювання біометричних параметрів користувача?

2. У чому полягає сутність методу аутентифікації користувача по клавіатурному почерку, заснованому на контролі влучення в область розподілу еталонних зразків?

3. Які види помилок використовуються для характеристики біометричних систем ідентифікації / аутентифікації?

4. Які переваги та недоліки є у методі біометричної аутентифікації користувача по клавіатурному почерку, заснованому на контролі влучення в область розподілу еталонних зразків?

5. Як можливо реалізувати метод контроля влучення в область розподілу еталонних зразків при наявності в системі багатьох зареєстрованих користувачів?

**Додаток А**
**Міністерство транспорту та зв'язку України**
**Державний департамент з питань зв'язку**

**Одеська національна академія зв'язку ім. О.С. Попова**

Кафедра інформаційної безпеки та передачі даних

ЗАТВЕРДЖУЮ
Ректор ОНАЗ ім. О.С. Попова
_____ П.П. Воробієнко
«___»_____2009 р.

# НАВЧАЛЬНА ПРОГРАММА

## Методи та засоби технічного захисту інформації (Інженерно-технічний захист інформації)

Нормативна професійно-орієнтована дисципліна

освітньо-професійної програми
підготовки бакалаврів у галузі: **1701 Інформаційна безпека** І
за напрямом вищої освіти:
**6.170102 Системи технічного захисту інформації**

Кваліфікація бакалавра: **фахівець з систем технічного захисту інформації**

**Одеса-2009**

Навчальна програма дисципліни: **Методи та засоби технічного захисту інформації (Інженерно-технічний захист інформації)**

Програму розроблено на кафедрі **Інформаційної безпеки та передачі даних**

Автор: доц. Кононович В.Г.

Програму розглянуто і схвалено на засіданні кафедри

Протокол № ___ від «____» _____ 2009 р.

Зав. каф._____ М.В. Захарченко

**Програму погоджено з кафедрами:**

Безпеки виробничих процесів та електроживлення систем зв'язку

_____ Зав. каф. проф. А.Ф. Кадацький

Комутаційних систем

_____ Зав. каф. доц. А.Г. Ложковський

**Програму розглянуто і схвалено методичною радою ННІ Радіо, телебачення, електроніки**

Протокол № __ від «____» _____ 2009 р.

Директор ННІ РТЕ _____ /проф. С.А. Михайлов/

**Програму розглянуто і схвалено методичною радою Одеської національної академії зв'язку ім. О.С. Попова**

Протокол № __ від «____» _____ 2009 р.

Голова ради, проф. М.В. Захарченко

## І. Передмова

Загальна характеристика дисципліни:
кількість кредитів ECTS 10
модулів 3;
загальна кількість годин 360;
у тому числі:
лекції 59 год.; лабораторних занять 42 год.; практичні заняття 42 год.; самостійна робота 217 год.; аудиторної роботи 143 годин;
семестри: 4.1, 4.2, 4.3
вид контролю: екзамен

## ІІ. Мета навчання з дисципліни

Формування базових знань механізмів функціонування сучасних систем технічного захисту інформації, придбання умінь користуватися концептуальними принципами побудови систем технічного захисту інформації, отримання навичок для розв'язування реальних задач, які виникають під час експлуатації та модернізації існуючих систем технічного захисту інформації. Розглядаються загальні принципи побудови систем технічного захисту інформації, принципи функціонування систем технічного захисту інформації, характеристики існуючих систем технічного захисту інформації. Надбані знання забезпечують уміння для практичної роботи в напрямі систем технічного захисту інформації.

## ІІІ. Зміст дисципліни

**Модуль 1:** *Види, джерела та носії інформації, що підлягає захисту* (кредитів ECTS – 3,0)

**Вхідні вимоги до вивчення модуля**

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Основи теорії кіл, сигнали та процеси | ЗН.1 |
| 2 | Метрологію та вимірювання, цифрову обробку сигналів | ЗН.2 |
| 3 | Електроніку та спеціальні мікропроцесори | ЗН.3 |
| | Зміст умінь | |
| 1 | Визначати інформацію, що підлягає захисту | УМ.1 |
| 2 | Програмувати мікропроцесорні системи | УМ.2 |
| | Проводити вимірювання фізичних величин кіл, сигналів та процесів | УМ.3 |

**Структура залікового модуля 1**

| Змістовий модуль | лекції (годин) | Заняття | | самостійна робота | індивідуальна робота |
|---|---|---|---|---|---|
| | | практичні | лабораторні | | |
| **Модуль 1: Види, джерела та носії інформації, що підлягає захисту (3,0 кредити; 86 год.)** | | | | | |
| 1. *Основні властивості інформації з позицій її технічного захисту* | 2 | 2 | | 6 | |
| 2. *Характеристики та способи запису сигналів на носії* | 2 | | 2 | 6 | |
| 3. *Демаскуючі прикмети об'єктів інформаційної діяльності* | 2 | 2 | | 6 | |
| 4. *Джерела та носії конфіденційної інформації* | 2 | | 2 | 6 | |
| 5. *Джерела небезпечних сигналів* | 2 | 2 | | 6 | |
| 6. *Загрози безпеці інформації* | 2 | | 2 | 6 | |
| 7. *Органи та технології розвідки* | 2 | 2 | | 6 | |
| 8. *Способи несанкціонованого доступу до джерел інформації* | 2 | | 2 | 6 | |
| **Разом 1 модуль, год.** | **16** | **8** | **8** | **54** | |

**Зміст змістових модулів (лекційних годин):**

1.1. *Основні властивості інформації з позицій її технічного захисту* (2 год.)

Види інформації, що захищаються технічними засобами. Властивості інформації, які впливають на можливості її захисту. Демаскуючі прикмети об'єктів інформаційної діяльності. Характеристики інформації, особливості семантичної інформації, інформацію щодо демаскуючих прикметах об'єкта.

1.2. *Характеристики та способи запису сигналів на носії* (2 год.)

Оцінка кількості інформації. Старіння інформації. Вартість інформації. Характеристики аналогових та дискретних сигналів. Способи запису інформації на різні види носіїв. Види модуляції сигналів. Методи забезпечення безпеки інформації в умовах завад.

1.3. *Демаскуючі прикмети об'єктів інформаційної діяльності* (2 год.)

Класифікація демаскуючих прикмет. Ідентифікаційні прикмети та прикмети діяльності об'єктів. Видові, сигнальні та речовинні демаскуючі

прикмети. Інформативність прикмет. Основні видові демаскуючі прикмети об’єктів спостереження. Особливості видових прикмет у оптичному та радіо діапазоні.

1.4. *Джерела та носії конфіденційної інформації* (2 год.)

Поняття щодо джерел, носіях та приймачах інформації. Класифікації джерел інформації. Джерела технічної та економічної інформації при наукових дослідженнях, розробках, виробництві та експлуатації продукції, на різних етапах і видах комерційної діяльності. Види носіїв інформації (люди, фізичні поля, електричні сигнали і матеріальні тіла).

1.5. *Джерела небезпечних сигналів* (2 год.)

Поняття про небезпечні сигнали та їх джерелах. Основні та допоміжні технічні засоби і системи. Побічні електромагнітні випромінювання та наводки. Акустоелектричні перетворювачі, їх види та принципи роботи. Принципи високочастотного нав’язування. Високочастотні та низькочастотні побічні випромінювання технічних засобів і систем. Паразитна генерація підсилювачів. Види паразитних зв’язків між ланцюгами технічних засобів і систем. Паразитні наводки у ланцюгах електроживлення, заземлення, у конструкціях приміщень і будівель, що проводять струм.

1.6. *Загрози безпеці інформації* (2 год.)

Види потенційних загроз безпеці інформації. Навмисні і випадкові впливи на джерела інформації. Витік інформації та його особливості. Методи оцінки рівня загроз. Фактори, що впливають на можливість реалізації загроз.

1.7. *Органи та технології розвідки* (2 год.)

Роль розвідки у діяльності держав та комерційних структур. Види зарубіжної розвідки і розвідки комерційних структур. Класифікація технічної розвідки за фізичною природою носія. Носії технічної розвідки. Принципи ведення розвідки. Основні принципи та етапи добування інформації. Видова та комплексна обробка даних і відомостей.

1.8. *Способи несанкціонованого доступу до джерел інформації* (2 год.)

Поняття щодо розвідувального контакту та його умовах. Види доступу до джерел інформації (фізичний контакт і дистанційний доступ). Принципи доступу до джерел інформації без фізичного проникнення до контрольованої зони. Класифікація та основні характеристики наземних засобів дистанційного з’йому інформації з носіїв. Принципи доступу до джерел інформації без порушення державних кордонів. Можливості закордонної космічної, повітряної та морської розвідки у мирний час.

## Теми практичних занять модуля 1

| № | Тема | годин |
|---|---|---|
| 1 | Принципи та критерії категоріювання об’єктів інформаційної діяльності. Вивчення нормативного документа ТПКО-95 | 2 |
| 2 | Вивчення державних стандартів ДСТУ 3396 0-96 та ДСТУ 3396 1-96 | 2 |
| 3 | Вивчення державних будівельних норм з ТЗІ | 2 |
| 4 | Організація технічного захисту інформації на підприємстві (організації, установі) | 2 |
| | **Усього:** | **8** |

## Теми лабораторних занять модуля 1

| № | Тема | годин |
|---|---|---|
| 1 | Дослідження методів прослуховування телефонних ліній | 2 |
| 2 | Способи підключення до телефонної лінії та запис переговорів | 2 |
| 3 | Системи прослуховування повідомлень, переданих мобільним зв’язком | 2 |
| 4 | Направлені та лазерні мікрофони. Стетоскопи | 2 |
| | **Усього:** | **8** |

**Вихідні знання та уміння з модуля 1**

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Види, джерела та носії інформації, що підлягає захисту | ЗН.1 |
| 2 | Технічні канали витоку інформації | ЗН.2 |
| | Зміст умінь | |
| 1 | Кваліфіковано аналізувати інформацію, надану технічними системами, з метою виявлення типових ознак можливого несанкціонованого доступу | УМ.1 |
| 2 | Уміти зафіксувати інформацію з додержання чи порушення заходів об’єктового контролю у відповідних реєстраційних документах | УМ.2 |
| 3 | Розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу | УМ.3 |

**Модуль 2:** *Технічні канали витоку інформації* (кредитів ECTS – 3,0)

**Вхідні вимоги до вивчення модуля**

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Види, джерела та носії інформації, що підлягає захисту | ЗН.1 |
| 2 | Технічні канали витоку інформації | ЗН.2 |
| | Зміст умінь | |
| 1 | Кваліфіковано аналізувати інформацію, надану технічними системами, з метою виявлення типових ознак можливого несанкціонованого доступу | УМ.1 |
| 2 | Уміти зафіксувати інформацію з додержання чи порушення заходів об'єктового контролю у відповідних реєстраційних документах | УМ.2 |
| 3 | Розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу | УМ.3 |

## Структура залікового модуля 2

| Змістовий модуль | лекції (годин) | Заняття | | самостійна робота | індивідуальна робота |
|---|---|---|---|---|---|
| | | практичні | лабораторні | | |
| **Модуль 2: Технічні канали витоку інформації (3,0 кредити; 86 год.)** | | | | | |
| 1. *Способи і засоби добування інформації технічними засобами* | 2 | 2 | | 6 | |
| 2. *Способи і засоби перехоплення сигналів* | 2 | | 2 | 6 | |
| 3. *Способи і засоби підслуховування акустичних сигналів* | 2 | 2 | | 6 | |
| 4. *Характеристики каналів витоку інформації* | 2 | | 2 | 6 | |
| 5. *Оптичні канали витоку інформації* | 2 | 2 | | 6 | |
| 6. *Радіоелектронні канали витоку інформації* | 2 | | 2 | 6 | |
| 7. *Акустичні канали витоку інформації* | 2 | 2 | | 6 | |
| 8. *Матеріально – речовинні канали витоку інформації* | 2 | 2 | | 6 | |
| **Разом 2 модуль, год.** | **16** | **8** | **8** | **54** | |

**Зміст змістових модулів (лекційних годин):**

2.1. *Способи і засоби добування інформації технічними засобами* (2 год.)

Способи і засоби спостереження. Фактори, що впливають на ефективність виявлення та розпізнавання об'єктів спостереження. Структура та основні характеристики засобів спостереження. Параметри зорової системи людини. Класифікація та основні характеристики об'єктивів. Види і технічні характеристики візуально-оптичних приладів. Способи і засоби добування інформації щодо демаскуючих прикметах речовин та способи й можливості їх визначення.

2.2. *Способи і засоби перехоплення сигналів* (2 год.)

Задачі, що вирішуються при перехопленні сигналів. Структура засобів перехоплення та їх функції. Класифікація і характеристики антен. Структура радіоприймача та його характеристики. Особливості та основні характеристики скануючи радіоприймачів. Принципи визначення координат джерел радіо випромінювання та аналізу сигналів.

2.3. *Способи і засоби підслуховування акустичних сигналів* (2 год.)

Параметри слухової системи людини. Структура і характеристики технічних засобів підслуховування. Класифікація і характеристики мікрофонів. Види і принципи одно направлених мікрофонів. Стетоскопи. Принципи роботи і характеристики диктофонів для прихованого запису. Класифікація і характеристики закладних пристроїв. Способи і засоби лазерного підслуховування та ВЧ-нав'язування.

2.4. *Характеристики каналів витоку інформації* (2 год.)

Структура технічних каналів витоку інформації. Відмінності технічного каналу витоку від каналу зв'язку. Види технічних каналів витоку інформації. Основні характеристики технічних каналів витоку інформації. Способи комплексного використання зловмисних технічних каналів витоку інформації.

2.5. *Оптичні канали витоку інформації* (2 год.)

Структура оптичного каналу витоку інформації. Умови освітленості об'єктів спостереження у видимому та інфра - червоному діапазонах у різні періоди часу. Характеристики середовища розповсюдження оптичних променів. Основні показники опто - електронних ліній зв'язку та способи зняття з них інформації. Варіанти оптичних каналів витоку інформації для типових контрольованих зон організації.

2.6. *Радіоелектронні канали витоку інформації* (2 год.)

Особливості радіоелектронних каналів витоку інформації. Види і структура радіоелектронних каналів витоку інформації. Вторинні антени.

2.7. *Акустичні канали витоку інформації* (2 год.)

Структура акустичного каналу витоку інформації. Відбиття та поглинання акустичних хвиль у середовищі розповсюдження. Поняття реверберації та вплив часу реверберації на розбірливість мови. Способи збільшення протяжності акустичного каналу витоку інформації.

2.8. *Матеріально – речовинні канали витоку інформації* (2 год.)

Структура матеріально – речовинного каналу витоку інформації та характеристики його елементів.

## Теми практичних занять модуля 2

| № | Тема | годин |
|---|---|---|
| 1 | Вивчення нормативних документів ПЕМВН-95 | 2 |
| 2 | Вимоги до системи технічного захисту серверних | 2 |
| 3 | Вимоги до системи технічного захисту центрів сертифікації ключів | 2 |
| 4 | Планування комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності | 2 |
| | **Усього:** | **8** |

## Теми лабораторних занять модуля 2

| № | Тема | годин |
|---|---|---|
| 1 | СВЧ та ІЧ-передавачі | 2 |
| 2 | Пристрої дистанційного управління та відео детектори руху | 2 |
| 3 | Відео та мікро відеокамери, системи передачі та приймання відеоінформації | 2 |
| 4 | Системи віброакустичного зашумлення | 2 |
| | **Усього:** | **8** |

**Вихідні знання та уміння з модуля 2**

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Можливі види технічної розвідки | ЗН.1 |
| 2 | Моделі технічних каналів витоку інформації та статистику фактів витоку інформації обмеженого доступу | ЗН.2 |
| 3 | Класифікацію і основні характеристики засобів технічного захисту від витоку по технічним каналам | ЗН.3 |
| 4 | Облік та обстеження режимних територій (зон) приміщень | ЗН.4 |
| | Зміст умінь | |
| 1 | Розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу | УМ.1 |

| | | |
|---|---|---|
| 2 | Проводити атестацію режимних територій в умовах додержання режиму секретності із за фіксуванням результатів у відповідних документах | УМ.2 |
| 3 | Розробляти узагальнений перелік потрібних технічних засобів | УМ.3 |
| 4 | Підбирати такі методи, моделі і алгоритми, що забезпечують оптимальне розв'язання задач захисту інформації | УМ.4 |

**Модуль 3:** *Методологія інженерно-технічного захисту інформації* (кредитів ECTS – 4,0)

**Вхідні вимоги до вивчення модуля**

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Можливі види технічної розвідки | ЗН.1 |
| 2 | Моделі технічних каналів витоку інформації та статистику фактів витоку інформації обмеженого доступу | ЗН.2 |
| 3 | Класифікацію і основні характеристики засобів технічного захисту від витоку по технічним каналам | ЗН.3 |
| 4 | Облік та обстеження режимних територій (зон) приміщень | ЗН.4 |
| | Зміст умінь | |
| 1 | Розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу | УМ.1 |
| 2 | Проводити атестацію режимних територій в умовах додержання режиму секретності із за фіксуванням результатів у відповідних документах | УМ.2 |
| 3 | Розробляти узагальнений перелік потрібних технічних засобів | УМ.3 |
| 4 | Підбирати такі методи, моделі і алгоритми, що забезпечують оптимальне розв'язання задач захисту інформації | УМ.4 |

**Структура залікового модуля 3**

| Змістовий модуль | лекції (годин) | Заняття | | самостійна робота | індивідуальна робота |
|---|---|---|---|---|---|
| | | практичні | лабораторні | | |
| **Модуль 3: Методологія інженерно-технічного захисту інформації (4,0 кредити; 188 год.)** | | | | | |
| 1. *Концепції інженерно-технічного захисту інформації* | 2 | 2 | 2 | 8 | |
| 2. *Способи та засоби інженерного захисту і технічної охорони* | 2 | 2 | 2 | 8 | |
| 3. *Способи, засоби та структура системи відео контролю* | 2 | 2 | 2 | 8 | |

| | | | | | |
|---|---|---|---|---|---|
| 4. *Способи і засоби захисту інформації від спостереження* | 2 | 2 | 2 | 8 | |
| 5. *Способи і засоби захисту інформації від підслуховування* | 2 | 2 | 2 | 8 | |
| 6. *Способи і засоби попередження витоку інформації за допомогою закладних пристроїв* | 2 | 2 | 2 | 8 | |
| 7. *Способи і засоби попередження витоку інформації через побічні електромагнітні випромінювання та наводки* | 2 | 2 | 2 | 8 | |
| 8. *Способи попередження витоку інформації матеріально-речовинному каналу* | 2 | 2 | 2 | 9 | |
| 9. *Організація інженерно-технічного захисту інформації* | 2 | 2 | 2 | 9 | |
| 10. *Системний підхід до захисту інформації* | 2 | 2 | 2 | 9 | |
| 11. *Моделювання об'єкта захисту* | 2 | 2 | 2 | 9 | |
| 12. *Моделювання загроз інформації* | 2 | 2 | 2 | 9 | |
| 13. *Оцінка ефективності технічного захисту інформації* | 2 | 2 | 2 | 9 | |
| **Разом 3 модуль, год.** | **26** | **26** | **26** | **110** | |

**Зміст змістових модулів (лекційних годин):**

2.1. *Концепції інженерно-технічного захисту інформації* (2 год.)

Мета та задачі інженерно-технічного захисту інформації. Принципи інженерно-технічного захисту інформації. Рівні безпеки інформації. Методи захисту інформації. Сутність інженерного захисту та технічної охорони джерел інформації. Поняття про інформаційний портрет об'єкта захисту. Способи змінювання інформаційного портрета за маскування та дезінформації. Залежність якості інформації від відношення потужності носія інформації та завади. Сутність енергетичного закриття. Показники ефективності інженерно-технічного захисту інформації.

2.2. *Способи та засоби інженерного захисту і технічної охорони* (2 год.)

Концепція охорони об'єктів. Категоріювання об'єктів охорони. Демаскуючі прикмети зловмисника та стихійних сил (пожежа, повінь). Моделі зловмисників. Рівні фізичної безпеки об'єктів охорони. Типова структура охорони. Способи і засоби інженерного захисту об'єктів. Двері та ворота,

захист вікон, замки. Контрольно-пропускні пункти. Способи ідентифікації людей. Металічні шкафи, сейфи та сховища. Способи і засоби виявлення зловмисників та пожежі. Контактні, акустичні, оптико-електронні, радіохвильові, вібраційні, емностні, теплові, іонізаційні сповіщувачі. Рекомендації з встановлення сповіщувачів. Пульти централізованого спостереження.

2.3. *Способи, засоби та структура системи відеоконтролю* (2 год.)

Способи та засоби нейтралізації загроз. Підрозділ охорони. Засоби тривожної сигналізації. Засоби управління системою охорони. Способи і засоби передавання сповіщень. Автоматизовані інтегральні системи охорони об'єктів їх структура та тенденції розвитку (розумний дім).

2.4. *Способи і засоби захисту інформації від спостереження* (2 год.)

Способи та засоби протидії спостереженню у оптичному діапазоні хвиль. Види та особливості маскування у видимому та інфра - червоному діапазонах. Способи і засоби протидії радіолокаційному та гідроакустичному спостереженню. Способи дезінформування та зашумлення зображення на екрані радіолокатора. Радіо поглинаючі покриття. Способи активного подавлення сигналів радіолокаторів.

2.5. *Способи і засоби захисту інформації від підслуховування* (2 год.)

Способи, засоби, види, класифікація інформаційного закриття акустичних сигналів та мовної інформації. Сутність способів технічного закриття. Типи і параметри скремблерів. Способи, засоби і методи енергетичного приховання акустичних сигналів. Звукоізоляція та звукопоглинання. Звукоізоляція, Огороджень, кабін, акустичних екранів, вікон та дверей. Типи та способи застосування генераторів акустичного та вібраційного зашумлення. Способи оцінки енергетичних та інформаційних показників безпеки мовної інформації.

2.6. *Способи і засоби попередження витоку інформації за допомогою закладних пристроїв* (2 год.)

Основні демаскуючі прикмети дротових і радіо закладних пристроїв, якісна оцінка їх інформативності. Класифікація засобів виявлення, локалізації та придушення закладних пристроїв. Принципи роботи та основні характеристики, переваги та недоліки виявлювачів електромагнітного поля. Можливості побутових приймачів та селективних вольтметрів. Типи і параметри скануючи приймачів. Склад, принципи роботи, можливості і параметри автоматизованих комплексів радіоконтролю приміщень. Способи контролю ліній та ланцюгів живлення. Способи придушення сигналів закладних пристроїв. Типи генераторів радіо завад.

2.7. *Способи і засоби попередження витоку інформації через побічні електромагнітні випромінювання та наводки* (2 год.)

Вимоги до засобів придушення сигналів побічних електромагнітних випромінювань та наводок. Методи та засоби пасивного придушення небезпечних сигналів акустоелектричних перетворень. Екранування електричних, магнітних та електромагнітних полів. Екранування проводів та кабелів. Матеріали для екранування. Вимоги до заземлення та конструкції заземлювачів. Розв'язка та фільтрація ланцюгів електроживлення. Засоби активного лінійного та просторового зашумлення.

2.8. *Способи попередження витоку інформації матеріально-речовинному каналу* (2 год.)

Класифікація способів попередження витоку інформації по матеріально-речовинному каналу. Способи і засоби знищення інформації, яка міститься у відходах діловодства та промислового виробництва. Способи та засоби стирання інформації на магнітних носіях. Способи захисту демаскуючих речовин.

2.9. *Організація інженерно-технічного захисту інформації* (2 год.)

Загальні положення щодо інженерно-технічного захисту в організації. Коротка характеристика державної системи захисту інформації. Організаційні та інженерно-технічні заходи з інженерно-технічного захисту. Основні напрями інженерно-технічного захисту інформації в організації. Задачі і види контролю ефективності системи захисту інформації.

2.10. *Системний підхід до захисту інформації* (2 год.)

Сутність системного підходу та системного аналізу. Характеристики системи захисту інформації Часткові та глобальні критерії ефективності системи захисту. Порядок проектування системи.

2.11. *Моделювання об'єкта захисту* (2 год.)

Сутність та методичні рекомендації із структурування інформації, що захищається. Виявлення та опис джерел інформації. Форми представлення моделей об'єктів інформаційної безпеки.

2.12. *Моделювання загроз інформації* (2 год.)

Види моделей загроз інформації: шляхів проникнення зловмисника до джерела і каналів витоку. Типові індикатори каналів витоку. Рекомендації з оцінки загроз безпеці інформації. Комплексування заходів захисту.

2.13. *Оцінка ефективності технічного захисту інформації* (2 год.)

Способи, заходи і засоби контролю ефективності системи захисту інформації. Оцінка ефективності системи захисту інформації.

## Теми практичних занять модуля 3

| № | Тема | годин |
|---|---|---|
| 1 | Загальні принципи захисту інформації у приміщеннях та мережах зв'язку | 2 |
| 2 | Пристрої захисту телефонних апаратів | 2 |
| 3 | Виявлення підключення до енергонесучих ліній та вимірювачі неоднорідностей ліній | 2 |
| 4 | Аналізатори телефонних ліній | 2 |
| 5 | Аналізатори та перевірочні пристрої дротових ліній та комунікацій | 2 |
| 6 | Детектори поля | 2 |
| 7 | Індикатори поля, зокрема індикатор поля електричної мережі | 2 |
| 8 | Принципи виявлення відеокамер та шукачі відеокамер | 2 |
| 9 | Скануючи приймачі | 2 |
| 10 | Автоматизований комплекс виявлення радіовипромінювання АКОР-1 | 2 |
| 11 | Широкодіапазонний спектральний корелятор OSCOR-500 | 2 |
| 12 | Випалювачі телефонних закладних пристроїв та подавлювачі диктофонів | 2 |
| 13 | Системи віброакустичного зашумлення | 2 |
| | **Усього:** | 26 |

## Теми лабораторних занять модуля 3

| № | Тема | годин |
|---|---|---|
| 1 | Вивчення і використання вимірювальних приладів SMV-11, SMV-8 та UNIPAN | 2 |
| 2 | Методика дослідження та вимірювання каналів витоку інформації в ефір з ЕОТ (з моніторів, клавіатури тощо) | 2 |
| 3 | Методика дослідження та вимірювання каналів витоку інформації ланцюгами електроживлення | 2 |
| 4 | Методика дослідження та вимірювання каналів витоку інформації ланцюгами заземлення | 2 |
| 5 | Методика оцінки та вимірювання затухання системи екранування приміщень (серверних) | 2 |
| 6 | Вивчення та використання багатофункціонального пошукового приладу ST– 031 Піранья | 2 |
| 7 | Виявлення витоку інформації з обмеженим доступом технічними каналами за допомогою багатофункціонального пошукового приладу ST– 031 Піранья | 2 |

| | | |
|---|---|---|
| 8 | Вивчення функціональних можливостей та використання комплексу „Бумеранг - 2Г” | 2 |
| 9 | Вимірювання витоку інформації акусто-електричним каналом за допомогою комплексу „Бумеранг - 2Г” | 2 |
| 10 | Вивчення функціональних можливостей та використання нелінійного локатора MS-888 | 2 |
| 11 | Пошук закладних пристроїв несанкціонованого знімання інформації за допомогою нелінійного локатора MS-888 | 2 |
| 12 | Вивчення функціональних можливостей та використання комплексу “Ореол-А” | 2 |
| 13 | Вимірювання витоку інформації акустичним та віброакустичним каналами за допомогою комплексу “Ореол-А” | 2 |

**Вихідні знання та уміння з модуля** 3

| № | Зміст знань | Шифр |
|---|---|---|
| 1 | Основні положення методології інженерно-технічного захисту інформації | ЗН.1 |
| 2 | Інженерно-технічного захисту інформації та класифікацію технічної розвідки | ЗН.2 |
| 3 | Методи і засоби технічного захисту інформації | ЗН.3 |
| 4 | Способи і принципи роботи засобів захисту від спостереження, підслуховування і перехоплення | ЗН.4 |
| 5 | Розуміти системний підхід до інженерно-технічного захисту інформації | ЗН.5 |
| | Зміст умінь | |
| 1 | Використовувати технічні засоби захисту інформації в умовах забезпечення режиму секретності на підприємствах, в організаціях та установах різних форм власності, уміти провести дії щодо організації технічного захисту інформації, зокрема приймати рішення про додержання чи наявність факту порушення конфіденційності інформації обмеженого доступу | УМ.1 |
| 2 | Розробляти (оформляти) схему розташування (підключення) технічних засобів внутрішньо-об’єктового контролю, захисту інформації обмеженого доступу в каналах зв’язку, закриття можливих каналів витоку інформації обмеженого доступу, протидіяти спробам цільового теленагляду за територією режимних підрозділів, приміщень, будинків, тощо. | УМ.2 |
| 3 | Уміти проводити атестацію режимних територій (зон), приміщень тощо із за фіксуванням результатів у відповідних документах. | УМ.3 |
| 4 | Розробляти номенклатурний перелік технічних засобів захисту інформації від витоку технічними каналами та реалізовувати технічні заходи закриття можливих каналів витоку інформації (за переліком каналів витоку) | УМ.4 |

| | | |
|---|---|---|
| 5 | Оцінювати ефективність систем захисту | УМ.5 |
| 6 | Здійснювати розробку і проектування об’єктів і присроїв систем технічного захисту інформації та оцінку їх ефективності | УМ.6 |

**Методи навчання**

Лекції, практичні заняття з використанням опитування, обговорення проблем і дискусій, лабораторні роботи з використанням ЕОМ, самостійна робота.

**Методи оцінювання**

Поточний контроль знань: *icnum*.

Оцінювання проводиться за шкалою , національною та за шкалою ОНАЗ (100 бал.)

**Література**


1. Конахович Г.Ф. и др. Защита информации в телекомуникационных системах. – К.: «МК-Прес», 2005. – 288 с.
2. Тардаскін М.Ф., Савицький Л.Ю., Кононович В.Г., Технічна експлуатація систем захисту інформації. Частина 1. Захист мовної інформації в каналах зв’язку та на об’єктах інформаційної діяльності: Навч. посібник / за ред. М.В. Захарченка. – Одеса: ОНАЗ, 2004. – С 188.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998, – 320 с.
4. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ. ООО "Д.В.К.", 2004 . – 508 с.
5. Герасименко В.А., Малюк А.А. Основи защиты информации. – М.: МОПО РФ. МИФИ, 1997. – 537 с.
6. Петраков А.В. Основи практической защиты информации. М.: Радио и свіязь, 1999, – 368 с.
7. Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонних каналах. – М.: Энергоатомиздат, 1997. – 304 с.
8. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: ученое пособие. – М.: Издательский центр «Академія», 2006. – 336 с.

## Тримовний тезаурус навчальної дисципліни

| № з/п | Терміни, категорії, поняття українською, російською та англійською мовами | Умовні позначення | Визначення терміна (категорії, поняття) | Джерело визначення |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1 | Автентифікація<br>Аутентификация<br>Authentication | | Перевірка належності суб'єктові доступу пред'явленого ним ідентифікатора. | Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – КиївіООО "Д.В.К.", 2004 . – 16 с. |
| 2 | Адміністратор<br>Администратор<br>Administrator, manager | | Користувач, роль якого включає функції керування системою комп'ютерною і (або) комплексом засобів захисту. | [4] – 24 с. |
| 3 | Аналіз<br>Анализ<br>Analysis | | Метод дослідження, що полягас в мисленому або практичному розчленуванні питого на складові частини. | [4] –33 с. |
| 4 | Антивірус<br>Антивирус<br>Antivirus | | В обчислювальній техніці – програма, що виявляє або виявляє та знищує віруси комп'ютерні. | [4] – 38 с. |
| 5 | Атака<br>Атака<br>Attack | | Дії порушника, спрямовані на порушення однієї з функцій захисту інформації (причетності, автентифікації, цілісності, доступності, конфіденційності); зловмисна дія. | [4] – 44 с. |

| | | | | |
|---|---|---|---|---|
| 6 | Безпека комп’ютерних систем Безопасность компьютерных систем Computer security | | Такий стан комп'ютерних систем, при якому забезпечується без пека даних, які обробляються ними. | [4] – 60 с. |
| 7 | Витік інформації Утечка информации Information leakage | | Несанкціонований процес перенесения інформації від джерела до зловмисника. | [4] – 76 с. |
| 8 | Вірус комп'ютерний Вирус компьютерный Computer virus | | Специальна програма, що здатна самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приеднання до них для наступного одержання управління та відтворення нових копій. | [4] – 94 с. |
| 9 | Дискета ключова Дискета ключевая Key diskette | | Дискета, що містить ключі системи захисту інформації. | [4] – 130 с. |
| 10 | Доступ несанкціонований до інформації Доступ несанкционированный к информации Unauthorized access to information | НСД НСД | Доступ до інформації під час якого порушуютвся встановлені правові норми і порядок його здійснення (правила розмежування доступу). | [4] – 149 с. |
| 11 | ЕОМ ЭВМ Computer | ЕОМ ЭВМ | Комплекс технічних засобів, призначений для автоматичного оброблення інформації в процесі вирішення задач обчислювальних і завдань інформаційних. | [4] – 158 с. |

| | | | | |
|---|---|---|---|---|
| 12 | Журнал контрольний<br>Журнал контрольный<br>Audit journal | | Журнал, в якому реєструються події, що мають відношення до забезпечення безпеки обчислювальної системи, зокрема, звернення до захищених даних. | [4] – 163 с. |
| 13 | Загроза безпеці обчислювальної системи<br>Угроза безопасности вычислительной системы<br>Threat | | Впливи на систему обчислювальну, які прямо або побічно можуть нанести шкоду її безпеці. | [4] – 178 с. |
| 14 | Зашифровування<br>Зашифровывание<br>Encryption | | Процес перетворення тексту відкритого до виду, незрозумілого несанкціонованому користувачеві (в шифротекст). | [4] – 222 с. |
| 15 | Ідентифікатор<br>Идентификатор<br>Identification | | Лексична одиниця, що використо-вується як ім'я для елементів мови; ім'я, що присвоюється даним і являє собою послідовність латинських літер і цифр, яка починається з літери. | [4] – 233 с. |
| 16 | Ідентифікація<br>Идентификация<br>Identification | | Надання суб'єктам і об'єктам доступу ідентифікатора і (або) порівняння пред'явленого ідентифікатора з переліком наданих ідентифікаторів. | [4] – 234 с. |
| 17 | Конфіденціиність інформації<br>Конфиденциальность информации<br>Information confidentiality | | Властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. | [4] – 304 с. |

| | | | | |
|---|---|---|---|---|
| 18 | Розмежування доступу до інформації<br>Разграничение доступа к информации<br>Differentiation | | Сукупність заходів, які здійснюють розділення інформації на частини і організацію доступу до неї посадових осіб у відповідності до їхніх функціональних обов'язків і повноважень. | [4] – 574 с. |
| 19 | Розшифровування<br>Расшифрование<br>Decryption | | Процес перетворення ши-фротексту у текст відкритий при відомому ключі; процес, зворотний процесу зашифровування. | [4] – 576 с. |
| 20 | Шифрування<br>Шифрование<br>Encryption | | Процес зашифровування або розшифровування. Процес перетворення криптографічного даних, за допомогою якого текст відкритий перетворюється в шифртекст з метою захисту від несанкціонованого доступу. | [4] – 744 с. |

## Перелік використаних скорочень та позначень

У цьому навчальному посібнику використовуються такі позначення й скорочення:

АРМ – автоматизоване робоче місце
АС – автоматизована система
БД – база даних
В/В – введення/виведення
ЖФ – журнальний файл
ЕОД – електронне опрацьовування даних
ЕОМ – електронна обчислювальна машина, комп'ютер
ІБ – інформаційна безпека
ІзОД – інформація з обмеженим доступом
ІК – ідентифікаційний код
ІТ-безпека – безпека інформаційної технології
ІТ-система – системи інформаційної технології
ІТ-продукт – продукт інформаційної технології
КЗЗ – комплекс засобів захисту
КСЗІ – комплексна система захисту інформації
ЛОМ – локальна обчислювальна мережа
НГМД – нагромаджувач на гнучких магнітних дисках
НД ТЗІ – нормативний документ системи технічного захисту інформації
НСД – несанкціонований доступ
НСЗ – несанкціоноване завантаження
ОС – операційна система
ПБ – політика безпеки
ПЗУ (ПЗП) – постійний запам'ятовувальний пристрій
ПЗ – програмне забезпечення
ПЕОМ – персональна електронна обчислювальна машина, персональний комп'ютер
ПЕМВН – побічні електромагнітні випромінювання і наведення
ПК – персональний комп'ютер
СЗІ – система захисту інформації
СУБД – система управління базами даних
ТЗІ – технічний захист інформації
OSI (ВВС) – взаємодія відкритих систем
SDU – блок сервісних даних
SMIB – бази керування безпекою інформації
MIB – інформаційна база керування
ISO/SEC – міжнародні організації стандартів

Позначення послуг безпеки згідно з НД ТЗІ 2.5-004:
ДВ-1 – ручне відновлювання
ДЗ-1 – модернізація
ДР-1 – квоти

ДС-1 – стійкість за обмежених відмовлянь
КА-2 – базова адміністративна конфіденційність
КВ-1 – мінімальна конфіденційність при обміні
КД-2 – базова довірча конфіденційність
КО-1 – повторне використання об’єктів
НВ-1 – автентифікування вузла
НИ-2 – поодиночна ідентифікування та автентифікування
НК-1 – однонаправлений вірогідний канал
НО-1 – розподіл обов’язків
НО-2 – розподіл обов’язків адміністраторів
НТ-1 – самотестування за запитом
НТ-2 – самотестування при старті
НР-2 – захищений журнал
НЦ-1 – КЗЗ з контролем цілісності
НЦ-2 – КЗЗ з гарантованою цілісністю
ЦА-1 – мінімальна адміністративна цілісність
ЦА-2 – базова адміністративна цілісність
ЦВ-1 – мінімальна цілісність при обміні
ЦД-1 – мінімальна довірча цілісність
ЦО-1 – обмежений відкот

## Тезаурус

**Автентифікування** (authentification) – процедура перевіряння відповідності пред’явленого ідентифікатора об’єкта комп’ютерної системи на предмет приналежності його до цього об’єкта; встановлення чи потвердження автентичності.

**Автентифікаційна інформація** – інформація, використовувана для встановлення законності потрібної особи.

**Автентифікування однорівневих об’єктів** – потвердження, що однорівневий у спілкуванні об’єкт є саме той, який потрібен.

**Обмін автентифікаційною інформацією** – механізм, призначений для завірення особистості об’єкта шляхом обміну інформацією.

**Пароль** (password) – конфіденційна автентифікаційна інформація, яка складається здебільшого з послідовності символів і яку слід ввести для отримання доступу.

**Ідентифікування** (identification) – процедура надавання ідентифікатора об’єктові комп’ютерної системи чи встановлення відповідності поміж об’єктом та його ідентифікатором; розпізнавання.

**Ідентифікування походження даних** – потвердження, що джерело даних визначено у належний спосіб.

**Персональний ідентифікаційний номер; ПІН** (personal identification number, PIN) – вид паролю, який здебільшого складається лише з цифр, і який, як правило, має бути пред’явлено нарівні з носимим ідентифікатором.

**Авторизація** – надавання прав, які включають надавання доступу на підставі права доступу.

**Аудит захисту** – незалежний огляд й експертиза системних записів та дій, щоби випробувати на адекватність системний контроль, гарантувати відповідність встановленої політики й операційних процедур, аби виявляти порушування у захисті й рекомендувати відповідні змінення в керуванні, політиці й процедурах.

**Журнал аудиту захисту** – зібрані й потенційно корисні дані для полегшування аудиту захисту.

**Аналізування трафіка –** виведення інформації від спостерігання потоків трафіка (наявність, відсутність, кількість, напрямок та частота).

**Виявлення маніпуляції** – механізм, використовуваний для виявлення того, чи було блок даних змінено випадково чи зумисно.

**Відповідальність** – властивість, яка гарантує, що дії об'єкта може бути відстежено винятково щодо об'єкта.

**Вибірковий польовий захист** – захист певних полів у межах повідомлення, яке має бути передане.

**Довірче функціонування** – функціональні можливості, сприймані, як правильні стосовно певних критеріїв, наприклад, як встановлено політикою захисту.

**Загроза** – потенційне порушування захисту.

**Активная загроза** – загроза зумисного неправочинного змінення стану системи. За прикладом активних загроз, які порушують безпеку, можуть слугувати: модифікування повідомлень, повторне використання повідомлень, вставлення фальшивих повідомлень, маскарад під авторизований об'єкт та відмова в обслуговуванні.

**Пасивна загроза** – загроза протиправного розкривання інформації без змінення стану системи.

**Відмова** – спростування одним із об'єктів, включених у зв'язок, того, що взято участь у всьому чи в частині сеансу зв'язку.

**Маскарад** – намагання певного об'єкта подати себе за інший об'єкт.

**Відмовлення в обслуговуванні** – перешкодження авторизованого доступу до ресурсів чи затримування операцій, які критичні у часі.

**Заповнення трафіка зайвою інформацією** – генерація фальшивих випадків зв'язку, фальшивих блоків даних та/чи фальшивих даних у межах блоків даних.

**Контроль доступу** – попередження неавторизованого використання ресурсу, включаючи попередження використання ресурсу в неавторизований спосіб.

**Список контролю доступу** – список об'єктів разом з їхніми правами доступу, уповноважених мати доступ до ресурсу.

**Повноваження** – дані, передані, аби встановити потрібну особистість об'єкта.

**Можливості** – символ, використовуваний як ідентифікатор ресурсу у таий спосіб, що володіння символом надає права доступу до ресурсу.

**Позначка (мітка) захисту** – має позначати ресурс (котрий може бути й блоком даних), який називає чи визначає атрибути захисту цього ресурсу. Маркування та/чи зв'язки можуть бути явні чи неявні.

**Ступінь важливості** – характеристика ресурсу, яка схарактеризовує його значення чи важливість, і може включати його вразливість.

**Канал** – шлях для передавання інформації.

**Конфіденційність** – властивість, завдяки якій інформація не стає доступною чи відкритою неправочинним особам, об'єктам чи процесам.

**Цілісність інформації** – властивість, що дані не було змінено чи знищено у противочинний спосіб.

**Доступність** – властивість доступності й придатності до використання після запиту авторизованим об'єктом.

**Таємність** – право особистостей управляти чи впливати на те, яку інформацію, пов'язану з ними, може бути зібрано й збережено; а також на те, кому й ким цю інформацію може бути розкрито.

**Політика захисту** – набір критеріїв для забезпечування сервісів безпеки. Завершена політика захисту неодмінно включає функції та механізми поза можливостямс відкритої системи, котрі визначаються організаційними, організаційно-технічними заходами тощо.

**Політика захисту на підставі ідентифікаційної інформації** – політика захисту, яка грунтується на ідентифікаційній інформації та/чи атрибутах окремих користувачів, груп користувачів, чи об'єктів, котрі діють від імені користувачів і отримують доступ до ресурсів/об'єктів.

**Політика захисту на підставі правил** – політика захисту, яка грунтується на глобальних правилах, наданих для всіх користувачів. Ці правила здебільшого базуються на порівнянні ступеня важливості ресурсів, які отримують доступ й право володіння відповідними атрибутами окремих користувачів, груп користувачів, чи об'єктів, котрі діють від імені користувачів.

**Сервіс безпеки** – сервіс, забезпечуваний рівнем зв'язку відкритих систем, котрий гарантує адекватний захист систем чи передаваних даних.

**Конфіденційність трафіка** – сервіс конфіденційності для захисту проти аналізування трафіка.

**Шифрування** – галузь техніки, яка зреалізовує принципи, засоби й методи перетворення даних для приховування змісту інформації, аби попереджувати її невиявлене модифікування та/чи попереджувати її неправочинне використання. Ці методи використовуються у шифруванні й дешифруванні. Внаслідок криптографічного перетворення даних здобувається шифротекст. Вплив на криптографічні принципи, засоби чи методи називається криптоаналізом.

**Криптоаналіз** – аналізування криптографічної системи та/чи її вводів та виводів, що використовується, аби здобути конфіденційні змінні та/чи таємні дані, включаючи чистий текст.

**Чистий текст** – зрозумілі дані, семантичний зміст яких є доступний.

**Шифротекст** – дані, випродуковані за допомогою шифрування. Внаслідок шифрування семантичний зміст даних стає не доступний.

**Дешифрування** – перетворення, протилежне до шифрування.

**Ключ** – послідовність символів, яка управляє операціями шифрування й дешифрування.

**Керування ключами** – генерування, зберігання, розподіл, знищування, архівування й застосовування ключів у відповідності з політикою безпеки.

**Криптографічна контрольна величина** – інформація, здобута при виконанні криптографічного перетворення блока даних.

**Цифровий підпис** – дані, які додано наприкінці, чи криптографічне перетворення блока даних, яке дозволяє довести джерело і цілісність блока даних отримувачеві повідомлення й захищає блок даних від підробляння, приміром отримувачем повідомлення.

**Нотаризація** – реєстрування даних довіреною третьою особою, яка дозволяє з часом потвердити точність його характеристик: змісту, походження, часу й доставляння.

**Фізична безпека** – заходи, які забезпечують фізичний захист ресурсів проти зувмисних та випадкових загроз.

**Керування маршрутизацією** – застосовування правил протягом процесу маршрутизації, щоби обрати чи відхилити певні мережі, канали зв’язку чи передавання.

# СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1 Закон України "Про інформацію" від 02.10.92 р.

2 Закон України "Про державну таємницю" від 21.12.94 р.

3 Закон України "Про науково-технічну інформацію".

4 Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.

5 Закон України “Про зв’язок”. Від 16.11.2003 р.

6 Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. № 1229.

7 Концепція технічного захисту інформації в Україні. – 1997.

8 Концепція технічного захисту інформації в галузі зв’язку України. – 1999.

9 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

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

11 ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

12 НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

13 НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

14 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (Критерії базуються на аналізі Федеральних критеріїв США і критеріїв оцінки безпеки Канади).

15 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

16 НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

17 НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

18 НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

19 НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

20 НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супровадження і модернізації засобів технічного захисту інформації від несанкціонованого доступу.

21 НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

22 НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.

23 НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

24 НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

25 НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

26 НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

27 НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова).

28 Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС.

29 Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications. Geneva.1991; Стандарт ISO 7498-1:1984. Базова модель ВВС.

30 ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.

31 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model.

32 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements.

33 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements.

34 Домарев В. В. Защита информации и безопасность компьютерных систем. К.: Диасофт, 1999. – 480 с.

35 Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

36 Герасименко В.А. Размахин М. К. Защита информации в вычислительных информационных и управляющих системах и сетях // Зарубежная радиоэлектроника. –1984. –№ 8.

37 Тардаскін М.Ф., Кононович В.Г. Технічний захист комерційної таємниці підприємства зв'язку: Навч. посібник/ За ред. М.В. Захарченка. – Одеса: ОНАЗ, 2002. – 76 с.

38 Банкет В. Л., Захарченко Н. В., Дырда А. В., Гулак Г. Н., Владишевский Б. С. Защита информации в системах телекоммуникации. Одесса-1997.

**ЗМІСТ**

С.

Навчальне видання

**Голев Денис Володимирович,**
**Русляченко Ольга Юріївна,**
**Бєлова Юлія Володимірівна,**
**Гончарук Дмитрій Сергійович**

# ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ
## Лабораторний практикум
## Частина 2 – Комплекси техничного захисту інформації

Навчальний посібник

Редактор *Л.А. Кодрул*
Комп'ютерне верстання *Ж.А. Гардиман*

Здано до набору
Підписано до друку Обсяг ум. -друк. арк.
Формат Зам. № Наклад прим.
Видруковано на видавничому устаткуванні фірми RISO
в друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
Одеса, 65021, вул. Старопортофранківська, 61
Тел. (0482) 207-894

---