



**Нормативний документ  
системи технічного захисту інформації**

---

**Тимчасові рекомендації  
з технічного захисту інформації від  
витоку каналами побічних  
електромагнітних випромінювань і наводок**

**Державна служба України  
з питань технічного захисту інформації**

**Київ 1995**

**Нормативний документ  
системи технічного захисту інформації**

---

Затверджено  
наказом Державної служби  
України з питань технічного  
захисту інформації  
від 09 червня 1995 р. N 25

**Тимчасові рекомендації  
з технічного захисту інформації  
від витоку каналами побічних  
електромагнітних випромінювань та наводок**

**ТР ТЗІ - ПЕМВН-95**

**ДСТЗІ**

**Київ**

## **Передмова**

1 Розроблено

Державною службою України з питань технічного захисту інформації

2 Введено вперше

Цей документ не може бути повністю або частково відтворений, тиражований і розповсюджений без дозволу Державної служби України з питань технічного захисту інформації

## Зміст

Галузь застосування .....	5
Нормативні посилання.....	5
1 Терміни і визначення .....	5
2 Основні положення .....	5
3 Короткий опис можливого витоку інформації каналами ПЕМВН .....	7
4 Загальні рекомендації з технічного захисту інформації з обмеженим доступом від витоку каналами ПЕМВН.....	10
4.1 Організаційні заходи .....	10
4.2 Підготовчі технічні заходи .....	10
4.3 Технічні заходи .....	12
5 Порядок контролю за станом технічного захисту інформації.....	14
Додаток 1 Таблиця вихідних даних для здійснення ТЗІ .....	16
Додаток 2 Методи і зміст контролю за підготовчими технічними заходами.....	18

**ТР ТЗІ - ПЕМВН-95**  
**Тимчасові рекомендації**  
**з технічного захисту інформації**  
**від витоку каналами**  
**побічних електромагнітних випромінювань та наводок**

---

Чинний від 01 липня 1995 р.

## **Галузь застосування**

Цей нормативний документ призначено для організації захисту інформації з обмеженим доступом (далі - інформація, ІЗОД) від витоку каналами побічних електромагнітних випромінювань та наводок (ПЕМВН).

Положення цього документа тимчасові і поширюються на центральні та місцеві органи державної виконавчої влади, органи виконавчої влади Республіки Крим, місцеві Ради народних депутатів та їх органи, на військові частини всіх військових формувань, на підприємства, установи й організації всіх форм власності, представництва України за кордоном і громадян, які володіють, користуються та розпоряджаються інформацією з обмеженим доступом.

Власники (користувачі) конфіденційної інформації, що не є власністю держави, положення цього документа застосовують на свій розсуд.

Зміни заходів, виконаних раніше відповідно до вимог керівних документів Держтехкомісії СРСР, не потрібно.

## **Нормативні посилання**

Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 09.09.94 р. N 632.

## **1 Терміни і визначення**

1.1 У цьому документі використовуються визначення, що відповідають наведеним у Положенні про технічний захист інформації в Україні.

## **2 Основні положення**

2.1 Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних

засобів пересилання, оброблення, зберігання, відображення інформації (ТЗП), а також допоміжних технічних засобів і систем (ДТЗС).

## 2.2 До ТЗП відносяться:

- засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв'язку;

- засоби і системи звукопідсилення, звукозапису та звуковідтворення;

- пристрої, що утворюють дискретні канали зв'язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна тощо;

- апаратура перетворення, оброблення, пересилання і приймання відеоканалів, що містять факсимільну інформацію.

ТЗП можуть бути захищеними і незахищеними.

## 2.3 До допоміжних технічних засобів і систем відносяться:

- засоби і системи спеціальної охоронної сигналізації (на відкриття дверей, вікон та проникнення до приміщення сторонніх осіб), пожежної сигналізації (з датчиками, що реагують на дим, світло, тепло, звук);

- система дзвінкової сигналізації (виклик секретаря, вхідна сигналізація);

- контрольно-вимірювальна апаратура (КВА);

- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);

- засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення (абонентські гучномовці системи радіомовлення та оповіщення, радіоприймачі та телевізори);

- засоби і системи годинофікації (електронні годинники, вторинні електрогодинники);

- засоби і системи електроосвітлення та побутового електрообладнання (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, провідна мережа електроосвітлення);

- електронна та електрична оргтехніка.

ДТЗС можуть бути захищеними і незахищеними.

## 2.4 Елементи ТЗП та ДТЗС можуть являти собою зосереджені випадкові антени (апаратура та її блоки) або розподілені випадкові антени (кабельні лінії та проводи).

Зазначеними елементами можуть бути:

- кінцеві технічні засоби і прилади;

- кабельні мережі та розводки, що з'єднують пристрої та обладнання;

- комутаційні пристрої (комутатори, кроси, бокси тощо);

- елементи заземлення та електроживлення.

## 2.5 ТЗП, застосовувані для оброблення інформації з обмеженим доступом, називаються основними технічними засобами (ОТЗ).

## 2.6 Роботи із захисту інформації з обмеженим доступом від витоку каналами ПЕМВН складаються з організаційних, підготовчих технічних, технічних заходів і контролю за виконанням заходів технічного захисту інформації (ТЗІ) та за ефективністю цього захисту.

2.7 Організаційні і підготовчі заходи щодо технічного захисту інформації проводяться одночасно і є першим етапом робіт, технічні заходи - наступним етапом робіт.

2.8 Заходи щодо ТЗІ і контролю за його ефективністю можуть виконуватись організаціями, що мають ліцензію Державної служби України з питань технічного захисту інформації (ДСТЗІ) на право надання послуг у галузі ТЗІ

### **3 Короткий опис можливого витоку інформації каналами ПЕМВН**

3.1 Можливі канали витоку інформації утворюються:

- низькочастотними електромагнітними полями, які виникають під час роботи ТЗП та ДТЗС;
- під час впливу на ТЗП та ДТЗС електричних, магнітних та акустичних полів;
- під час виникнення паразитної високочастотної (ВЧ) генерації;
- під час проходження інформативних (небезпечних) сигналів у колі електроживлення;
- під час взаємного впливу кіл;
- під час проходження інформативних (небезпечних) сигналів у колі заземлення;
- під час паразитної модуляції високочастотного сигналу;
- внаслідок хибних комутацій і несанкціонованих дій.

3.2 Під час пересилання інформації з обмеженим доступом в елементах схем, конструкцій, підвідних і з'єднувальних проводах технічних засобів протікають струми інформативних (небезпечних) сигналів. Електромагнітні поля, що виникають при цьому, можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації.

Джерелами виникнення електромагнітних полів у ТЗП та ДТЗС можуть бути неекрановані проводи, розімкнуті контури, елементи контрольно-вимірювальних приладів, контрольні гнізда на підсилювальних блоках і пультах, неекрановані кінцеві пристрої, підсилювачі потужності та лінійні підсилювачі, трансформатори, дроселі, з'єднувальні проводи з великими струмами, роз'єми, гребінки, гучномовці, кабельні лінії.

3.3 Інформативні (небезпечні) сигнали можуть виникати на елементах технічних засобів, чутливих до впливу:

- електричного поля (неекрановані проводи та елементи технічних засобів);
- магнітного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле);
- акустичного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле).

За наявності в технічних засобах елементів, здатних перетворювати ці поля в електричні сигнали, можливий витік інформації незахищеними колами

абонентських ліній зв'язку, електроживлення, заземлення, керування, сигналізації.

3.4 Паразитна високочастотна генерація (ПВЧГ) у ТЗПІ та ДТЗС виникає внаслідок самозбудження підсилювальних пристроїв (активна ПВЧГ) або внаслідок відбиття сигналів від кінців ліній зв'язку між підсилювачами під час перехідних процесів (пасивна ПВЧГ).

Високочастотні паразитні коливання, промодульовані інформативним (небезпечним) сигналом за амплітудою, частотою і фазою (активна ПВЧГ) або за амплітудою і частотою (пасивна ПВЧГ), створюють канал витоку інформації.

ПВЧГ утворюється в елементах апаратури, які охоплені негативним зворотним зв'язком і не мають достатнього запасу стійкості, у кінцях ліній зв'язку між підсилювальними пристроями в моменти перемикачів через виникнення перехідних процесів.

3.5 У процесі роботи ТЗПІ та ДТЗС можливий витік інформації через джерела електроживлення:

- у результаті проходження інформативного (небезпечного) сигналу через технічні засоби на входному опорі його джерела живлення може виникнути напруга, що несе сигнал, який містить інформативну складову. Через випрямний пристрій та силовий трансформатор цей сигнал поширюється мережевими лініями за межі контрольованої території;

- під час проходження мовного сигналу через кінцевий підсилювальний пристрій може мати місце нерівномірне споживання струму від джерела живлення. Струм, що споживається підсилювачем від мережі живлення, може бути промодульований інформативним (небезпечним) сигналом, який проходить через підсилювач.

3.6 Траси кабельних кіл, що несуть ІзОД, можуть прокладатися в одній кабельній каналізації з незахищеними каналами ТЗПІ та ДТЗС і проходити через спільні протяжні коробки і шафи.

Під час пересилання інформативного (небезпечного) сигналу одним колом у сусідніх колах - за їх паралельного пробігу - з'являються струми, наведені внаслідок електромагнітного впливу. Перехід електромагнітної енергії з одного кола в інше є можливим каналом витоку інформації.

Джерелами утворення інформативних (небезпечних) сигналів є ділянки, охоплені випадковими ємкісними і магнітними зв'язками. Такими ділянками можуть бути відрізки паралельного пробігу ліній, що несуть ІзОД, з незахищеними лініями, які уходять за межі контрольованої території, плінти кабельні, що служать для комутації вихідних ліній у кросах, монтажні колодки, роз'єми блоків, контакти перемикачів та реле, використовувані для комутації вихідних ліній, блоки, що зазнають впливу електромагнітного поля.

3.7 Витік інформації колом заземлення може статися з таких причин:

- за наявності контурів у системі заземлення, коли існують дві чи більше точки сполучення кіл, що несуть ІзОД, із заземлювачем;

- внаслідок недосконалості екранів і виникнення паразитних зв'язків. Витік може поширюватися як симетричними, так і несиметричними шляхами.

Джерелом утворення інформативних (небезпечних) сигналів є елементи кіл і схем, якщо ці елементи знаходяться під потенціалом таких сигналів і виходять з екранів.

3.8 Під час надходження високочастотних сигналів у нелінійні (або параметричні) кола, що несуть ІзОД, відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних (небезпечних) сигналів і створюють канал витоку інформації.

Лініями, на які подається або з яких знімається високочастотний сигнал, можуть бути незахищені лінії зв'язку, кола електроживлення, заземлення, керування і сигналізації, кола, утворені паразитними зв'язками, конструктивними елементами будинків, споруд, обладнання тощо. Джерелами інформативних (небезпечних) сигналів є нелінійні радіоелементи, на яких відбувається модуляція таких сигналів.

3.9 Під час виникнення несправностей в апаратурі або несанкціонованих діях обслуговуючого персоналу у схемах керування може виникнути небажана комутація інформативного (небезпечного) сигналу, яка призводить до виходу ІзОД у незахищений канал зв'язку.

Джерелами інформативного (небезпечного) сигналу цього каналу є пульти керування, щити розподілу та комутації, блоки контролю, реле, трансформатори, роз'єми, перемикачі або запам'ятовувальні пристрої, в яких може виникнути хибна комутація в результаті несправностей або несанкціонованих дій.

3.10 Основними параметрами можливого витоку інформації каналами ПЕМВН є:

- напруженість електричного поля інформативного (небезпечного) сигналу;
- напруженість магнітного поля інформативного (небезпечного) сигналу;
- величина звукового тиску;
- величина напруги інформативного (небезпечного) сигналу;
- величина напруги наведеного інформативного (небезпечного) сигналу;
- величина напруги шумів (завад);
- величина струму інформативного (небезпечного) сигналу;
- величина чутливості до впливу магнітних полів для точкового джерела;
- величина чутливості апаратури до впливу електричних полів (власна ємність апаратури);
- величина чутливості до впливу акустичних полів;
- відношення "інформативний сигнал/шум";
- відношення напруги небезпечного сигналу до напруги шумів (завад) у діапазоні частот інформативного сигналу.

Зазначені параметри визначаються і розраховуються за результатами вимірювань у заданих точках.

Гранично допустимі значення основних параметрів є нормованими величинами і визначаються за відповідними методиками.

3.11 Відношення розрахункових (вимірних) значень основних параметрів до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

## **4 Загальні рекомендації з технічного захисту інформації з обмеженим доступом від витоку каналами ПЕМВН**

### **4.1 Організаційні заходи**

4.1.1 На етапі проведення організаційних заходів потрібно:

- визначити перелік відомостей з обмеженим доступом, що підлягають технічному захисту (визначає власник інформації згідно з чинним законодавством України);

- обґрунтувати необхідність розроблення і реалізації захисних заходів з урахуванням матеріальної або іншої шкоди, яка може бути завдана внаслідок можливого порушення цілісності ІзОД чи її витоку технічними каналами;

- установити перелік виділених приміщень, в яких не допускається реалізація загроз та витік інформації з обмеженим доступом;

- визначити перелік технічних засобів, що повинні використовуватися як ОТЗ;

- визначити технічні засоби, застосування яких не обґрунтовано службовою та виробничою необхідністю та які підлягають демонтажу;

- визначити наявність задіяних і незадіяних повітряних, наземних, настінних та закладених у приховану каналізацію кабелів, кіл і проводів, що уходять за межі виділених приміщень;

- визначити системи, що підлягають демонтажу, потребують переобладнання кабельних мереж, кіл живлення, заземлення або установаження в них захисних пристроїв.

4.1.2 За результатами обстеження складається акт довільної форми з переліком виконаних заходів і прикладанням (за необхідністю):

- переліку ОТЗ, розміщених у виділених приміщеннях;

- плану виділених приміщень із зазначенням місць установаження ОТЗ, а також схем прокладання кабелів, проводів, кіл;

- переліку технічних засобів, кабелів, кіл, проводів, що підлягають демонтажу.

Акт підписується виконавцем робіт і затверджується керівником організації (підприємства).

### **4.2 Підготовчі технічні заходи**

4.2.1 Підготовчі технічні заходи включають у себе первинні заходи блокування електроакустичних перетворювачів і ліній зв'язку, які виходять за межі виділених приміщень.

4.2.2 Блокування ліній зв'язку може виконуватися такими способами:

- відключенням ліній зв'язку ТЗПІ та ДТЗС або встановленням найпростіших схем захисту;

- демонтажем технічних засобів, кабелів, кіл, проводів, що уходять за межі виділених приміщень;

- видаленням за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

4.2.3 Блокування каналів можливого витоку ІзОД у системах міського та відомчого телефонного зв'язку може здійснюватися:

- відключенням дзвінкових (викличних) ліній телефонного апарата;
- установленням у колі телефонного апарата безрозривної розетки для тимчасового відключення;
- установленням найпростіших пристроїв захисту.

4.2.4 Запобігання витоку ІзОД через діючі системи гучномовного диспетчерського та директорського зв'язку здійснюється застосуванням таких захисних заходів:

- установленням у викличних колах вимикачів для розриву кіл;
- установленням на вході гучномовців вимикачів (реле), які дають можливість розривати кола по двох проводах;
- забезпеченням можливості відключення живлення мікрофонних підсилювачів;
- установленням найпростіших пристроїв захисту.

4.2.5 Захист ІзОД від витоку через радіотрансляційну мережу, що виходить за межі виділеного приміщення, може бути забезпечений:

- відключенням гучномовців по двох проводах;
- вмиканням найпростіших пристроїв захисту.

Для служби оповіщення слід виділити чергові абонентські пристрої поза виділеними приміщеннями; кола до цих пристроїв повинні бути прокладені окремим кабелем.

4.2.6 Блокування каналів витоку ІзОД через кола вторинних електроапаратів системи електроапаратизації здійснюється відключенням їх на період проведення закритих заходів.

4.2.7 Запобігання витоку ІзОД через системи пожежної та охоронної сигналізації здійснюється відключенням датчиків пожежної та охоронної сигналізації на період проведення важливих заходів, що містять ІзОД, або застосуванням датчиків, які не потребують спеціальних заходів захисту.

4.2.8 З метою виключення можливості витоку ІзОД під час роботи незахищених технічними засобами телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури необхідно на період проведення важливих заходів зазначені пристрої відключати від мережі електроживлення по двох проводах.

4.2.9 Блокування витоку ІзОД через системи електронної оргтехніки та кондиціонування може бути забезпечене такими заходами:

- розташуванням зазначених систем усередині контрольованої території без винесення окремих компонентів за її межі;
- електроживленням систем від трансформаторної підстанції, що знаходиться всередині контрольованої території.

При невиконанні зазначених вище умов системи повинні відключатися від мережі електроживлення по двох проводах.

4.2.10 Захист ІзОД від витоку через кола електроосвітлення та електроживлення побутової техніки повинен здійснюватися підключенням зазначених кіл до окремого фідера трансформаторної підстанції, до якого не допускається підключення сторонніх користувачів.

У випадку невиконання зазначеної вимоги електрообутові прилади на період проведення закритих заходів повинні відключатися від кіл електроживлення.

### **4.3 Технічні заходи**

4.3.1 Технічні заходи є основним етапом робіт з технічного захисту ІзОД і полягають у встановленні ОТЗ, забезпеченні ТЗПІ та ДТЗС пристроями ТЗІ.

4.3.2 Під час вибору, встановлення, заміни технічних засобів слід керуватися паспортами, технічними описами, інструкціями з експлуатації, рекомендаціями з установа, монтажу та експлуатації, що додаються до цих засобів.

4.3.3 ОТЗ повинні розміщуватися, по можливості, ближче до центру будинку або в бік найбільшої частини контрольованої території. Складові елементи ОТЗ повинні розміщуватися в одному приміщенні або в суміжних.

Якщо зазначені вимоги невиконувати, слід вжити додаткових заходів захисту:

- встановити високочастотні ОТЗ в екрановане приміщення (камеру);
- встановити в незахищені канали зв'язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.
- прокласти проводи і кабелі в екранувальних конструкціях;
- зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;
- виконати технічні заходи щодо захисту ІзОД від витоків колами заземлення та електроживлення.

4.3.4 До засобів технічного захисту відносяться:

- фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоків мовної ІзОД через двопровідні лінії телефонного зв'язку, системи директорського та диспетчерського зв'язку;
- пристрої захисту абонентських однопрограмних гучномовців для блокування витоків мовної ІзОД через радіотрансляційні лінії;
- фільтри мережеві для блокування витоків мовної ІзОД колами електроживлення змінного (постійного) струму;
- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв'язку;
- генератори лінійного зашумлення;
- генератори просторового зашумлення;
- екрановані камери спеціальної розробки.

4.3.5 Для телефонного зв'язку, не призначеного для пересилання ІзОД, рекомендується застосовувати апарати вітчизняного виробництва, сумісні з пристроями захисту. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку компетентних організацій системи ТЗІ про їх сумісність з пристроями захисту.

4.3.6 Вибір методів і способів захисту елементів ТЗПІ та ДТЗС, що мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1 кГц.

Елементи з вхідним опором менше 600 Ом (головки гучномовців, електродвигуни вентиляторів, трансформатори тощо) рекомендується відключати

по двох проводах або встановлювати у розрив кіл пристрої захисту з високим вихідним опором для зниження до мінімальної величини інформативної складової струму.

Елементи з високим вхідним опором (електричні дзвінки, телефонні капсулі, електромагнітні реле) рекомендується не тільки відключати від кіл, а й замикати на низький опір або закорочувати, щоб зменшити електричне поле від цих елементів, зумовлене напругою, наведеною під час впливу акустичного поля. При цьому слід враховувати, що обраний спосіб захисту не повинен порушувати працездатність технічного засобу і погіршувати його технічні параметри.

4.3.7 Високочастотні автогенератори, підсилювачі (мікрофонні, приймання, пересилання, гучномовного зв'язку) та інші пристрої, що містять активні елементи, рекомендується відключати від ліній електроживлення у "черговому режимі" або "режимі чекання виклику".

4.3.8 Підключення пристроїв захисту слід проводити без порушення або зміни електричної схеми і ТЗП, і ДТЗС.

4.3.9 Захист ІЗОД від витоку кабелями та проводами рекомендується здійснювати шляхом:

- застосування екранувальних конструкцій;
- роздільного прокладання кабелів ОТЗ, ТЗП та ДТЗС.

4.3.10 При неможливості виконання вимог щодо рознесення кабелів електроживлення ОТЗ, ТЗП та ДТЗС електроживлення останніх слід здійснювати або екранованими кабелями, або від розділових систем, або через мережеві фільтри.

4.3.11 Не допускається утворення петель та контурів кабельними лініями. Перехрещення кабельних трас різного призначення рекомендується здійснювати під прямим кутом одна до одної.

4.3.12 Електроживлення ОТЗ повинно бути стабілізованим за напругою та струмом для нормальних умов функціонування ОТЗ і забезпечення норм захищеності.

У колах випрямного пристрою джерела живлення необхідно встановлювати фільтри нижніх частот. Фільтри повинні мати фільтрацію по симетричних і несиметричних шляхах поширення.

Необхідно передбачити відключення електромережі від джерела живлення ОТЗ під час зникнення напруги в мережі, під час відхилення параметрів електроживлення від норм, заданих в ТУ, та під час появи несправностей у колах електроживлення.

4.3.13 Усі металеві конструкції ОТЗ (шафи, пульти, корпуси розподільних пристроїв та металеві оболонки кабелів) повинні бути заземлені.

Заземлення ОТЗ слід здійснювати від загального контуру заземлення, розміщеного в межах контрольованої території, з опором заземлення за постійним струмом відповідно до вимог стандартів.

Система заземлення повинна бути єдиною для всіх елементів ОТЗ і будуватися за радіальною схемою.

Утворення петель і контурів у системі заземлення не допускається.

4.3.14 Екрани кабельних ліній ТЗП, що виходять за межі контрольованої території, повинні заземлятися в кросах від загального контуру

заземлення в одній точці для виключення можливості утворення петель по екрану та корпусах.

У кожному пристрої повинна виконуватися умова безперервності екрана від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватися як другий провід сигнального кола або кола живлення.

Екрани кабелів не повинні мати електричного контакту з металоконструкціями. Для монтажу слід застосовувати екрановані кабелі з ізоляцією або одягати на екрани ізоляційну трубку.

У довгих екранованих лініях (мікрофонних, лінійних, звукопідсилювальних) рекомендується ділити екран на ділянки для одержання малих опорів для високочастотних струмів і кожен ділянку заземляти тільки з одного боку.

4.3.15 Вихідні дані для здійснення ТЗІ наведені у додатку 1.

4.3.16 Результати виконання технічних заходів оформляються актом приймання робіт, складеним у довільній формі, підписуються виконавцем робіт і затверджуються керівником організації (підприємства).

## **5 Порядок контролю за станом технічного захисту інформації**

5.1 Метою контролю є виявлення можливих технічних каналів витоку інформативного (небезпечного) сигналу (проведення спецдосліджень), вироблення заходів, що забезпечують його приховування, оцінка достатності й ефективності вжитих заходів захисту, оперативний контроль за станом технічного захисту каналів витоку інформативного сигналу.

5.2 Технічний канал витоку вважається захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення "інформативний сигнал/шум".

Пристрої захисту і захищені технічні засоби вважаються справними, якщо їх параметри відповідають вимогам експлуатаційних документів.

5.3 Контроль за виконанням організаційних та підготовчих технічних заходів щодо захисту інформації здійснюється візуальним оглядом прокладки проводів і кабелів, що виходять за межі об'єкта захисту, а також технічних засобів захисту та захищеної техніки. Контроль слід проводити з урахуванням рекомендацій, наведених у додатку 2.

5.4 У ході перевірки визначаються:

- наявність електромагнітного зв'язку між лініями ОТЗ, ТЗПІ та ДТЗС (проходження в одному кабелі чи жгуті), між різними видами ТЗПІ та ДТЗС (спільний пробіг проводів систем пожежно-охоронної сигналізації, годинофікації, радіотрансляції);

- наявність виходів ліній зв'язку, сигналізації, годинофікації, радіотрансляції за межі виділених приміщень;

- наявність незадіяних ТЗПІ, ДТЗС, проводів, кабелів;

- можливість відключення ТЗПІ на період проведення конфіденційних переговорів або важливих нарад;
- рознесення джерел електромагнітних та акустичних полів на максимально можливу відстань у межах виділених приміщень;
- виконання заземлення апаратури, яке виключає можливість утворення петель з проводів та екранів;
- рознесення кабелів електроживлення ОТЗ, ТЗПІ та ДТЗС з метою виключення наводок небезпечних сигналів;
- виконання розведення кіл електроживлення екранованим або крученим кабелем;
- наявність можливості відключення електроживлення ОТЗ під час обезструмлення мережі; відхилення параметрів електроживлення від норм, заданих в ТУ, під час появи несправностей у колах живлення.

5.5 У процесі проведення спецдосліджень, перевірки ефективності технічних заходів захисту підлягають інструментальному контролю ОТЗ і лінії зв'язку.

У ході контролю перевіряються електромагнітні поля інформативних (небезпечних) сигналів у широкому діапазоні частот навколо апаратури та кабельних з'єднань ОТЗ, наявність інформативних (небезпечних) сигналів у колах, проводах електроживлення та заземленні ТЗПІ та ДТЗС.

Під час спецдосліджень визначається радіус, за межами якого відношення "інформативний сигнал/шум" менше гранично допустимої величини. Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витoku каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витoku, проводиться порівняння фактичних параметрів з нормованими.

У випадку перевищення допустимих значень розробляються захисні заходи, використовуються засоби захисту (екранування джерел випромінювання, встановлення фільтрів, стабілізаторів, засобів активного захисту).

5.6 Після проведення спецдосліджень, вироблення та впровадження засобів захисту проводиться контроль за ефективністю застосованих технічних засобів захисту.

5.7 У процесі роботи технічних засобів і захищеної техніки, у міру необхідності, проводиться оперативний контроль за ефективністю захисту каналів витoku інформативного (небезпечного) сигналу.

5.8 Результати контролю (спецдосліджень) оформляються актом, складеним у довільній формі, підписуються перевіряючим та затверджуються керівником організації (підприємства).

## Додаток 1 Таблиця вихідних даних для здійснення ТЗІ

Середовище поширення	Можливий канал витоку інформації	Умови експлуатації, за яких найбільш імовірний витік інформації	Контрольований параметр	Рекомендації із захисту ІзОД
Навколишній простір	1. Побічні електромагнітні випромінювання у мовному діапазоні	Під час експлуатації обладнання ТЗП (системи звукопідсилення, гучномовного зв'язку, магнітофони, мережі внутрішнього телефонного зв'язку тощо)	Напруженість електричного і магнітного полів	Забезпечити зменшення електромагнітних полів раціональним розміщенням і монтажем апаратури Здійснити екранування випромінювачів магнітних полів, а також джерел електричних полів (проводів, блоків) Застосовувати пристрої активного захисту для створення магнітних та електричних полів завад зі спектром, подібним до спектра інформативного сигналу Виконати заземлення екранів, проводів і приладів для зниження потенціалу інформативного сигналу
	2. Побічні електромагнітні випромінювання під час самозбудження підсилювальних каскадів	Під час експлуатації обладнання ТЗП, до складу яких входять підсилювачі (системи звукопідсилення, гучномовного зв'язку, магнітофони, мережі внутрішнього телефонного зв'язку тощо)	Відсутність самозбудження	Забезпечити штатний режим роботи апаратури При виявленні паразитної високочастотної модуляції за допомогою КВА відключити апаратуру від джерела живлення
	3. Побічні електромагнітні випромінювання високочастотних сигналів, що несуть інформативний (небезпечний) сигнал за рахунок паразитної модуляції: а) на нелінійних елементах	Під час експлуатації ТЗП, до складу яких входять високочастотні генератори (магнітофони, диктофони тощо)	Коефіцієнт модуляції	Контролювати за допомогою КВА проходження інформативних сигналів в абонентських лініях, колах електроживлення, заземлення, керування, сигналізації тощо При виявленні інформативного сигналу відключити апаратуру від мережі живлення Застосувати активні засоби захисту від проникнення ВЧ сигналу в апаратуру за рахунок модуляції шумовою завадою
	б) під час акустичного впливу інформативних сигналів	Під час експлуатації ТЗП та ДТЗС, до складу яких входять високочастотні генератори		Заземлити екрани приладів, кабелі та проводи, якими можуть наводитися потенціали інформативних сигналів під час впливу електричних полів
	в) під час впливу	Під час експлуатації ТЗП та ДТЗС, до		Зменшити величину напруги наведеного інформативного сигналу штучним розриванням

<b>Середовище поширення</b>	<b>Можливий канал витоку інформації</b>	<b>Умови експлуатації, за яких найбільш імовірний витік інформації</b>	<b>Контрольований параметр</b>	<b>Рекомендації із захисту ІзОД</b>
Проводи і кола ДТЗС	<p>електричних і магнітних полів інформативних (небезпечних) сигналів</p> <p>1. Електроакустичні перетворення в елементах обладнання ДТЗС, ОТЗ</p> <p>2. Наводки інформативних (небезпечних) сигналів на обладнання і кола ДТЗС, ОТЗ у мовному та височастотному діапазонах</p>	<p>складу яких входять височастотні генератори, під час їх спільного використання з ОТЗ</p> <p>Під час установавання обладнання ТЗП та ДТЗС</p> <p>1. Під час включення в обладнання ОТЗ ліній ТЗП та ДТЗС</p> <p>2. Під час спільного встановлення обладнання ОТЗ, ТЗП та ДТЗС</p> <p>3. Під час спільного прокладання ліній ОТЗ та ДТЗС</p>	<p>Напруга перетвореного інформативного (небезпечного) сигналу</p> <p>Напруга наведеного інформативного сигналу</p> <p>Коефіцієнт модуляції наведеного ВЧ сигналу</p> <p>Напруга інформативного (небезпечного) сигналу</p> <p>Напруга інформативного (небезпечного) сигналу</p>	<p>ліній, невикористовуваних для пересилання ІзОД, за допомогою тумблерів, реле, перемикачів тощо</p> <p>Застосувати спеціальні фільтри захисту з метою подавлення інформативних сигналів</p> <p>У лініях керування, сигналізації, контролю, що несуть мовну інформацію з обмеженим доступом, рекомендується ставити фільтри, які вирізають мовний діапазон частот</p> <p>Створити за допомогою активних засобів захисту шумові завади зі спектром, подібним до спектра інформативного сигналу</p> <p>Рознести вхідні та вихідні лінії, зменшити їх паралельний пробіг</p> <p>Раціонально розмістити елементи апаратури для зменшення створюваних ними магнітних полів</p> <p>Застосувати активні засоби захисту для створення шумової завади зі спектром, аналогічним спектру наведеного сигналу</p>
Кола електроживлення	<p>Наводки інформативних (небезпечних) сигналів, електроакустичні перетворення, нерівномірне споживання струму</p>	<p>1. Під час експлуатації обладнання ОТЗ</p> <p>2. Під час установавання ОТЗ, ТЗП та ДТЗС</p>	<p>Напруга інформативного (небезпечного) сигналу</p>	<p>Застосувати стабілізоване джерело живлення апаратури паралельного типу з мінімально можливим внутрішнім опором</p> <p>Застосувати активні засоби захисту з метою створення в колах електроживлення шумової завади зі спектром, подібним до спектра мовного сигналу або обгинаючої мовного сигналу</p>
Кола заземлення	Те ж	Під час експлуатації обладнання ОТЗ, ТЗП та ДТЗС	Струм інформативного (небезпечного) сигналу	<p>Виконати заземлення апаратури, виключивши утворення петель і контурів із заземлювальних проводів та екранів</p> <p>Максимально зменшити опір контуру заземлення</p>

## Додаток 2 Методи і зміст контролю за підготовчими технічними заходами

Захисний захід	Метод контролю	Зміст контролю
Відключення дзвінків телефонних апаратів, не призначених для пересилання ІзОД, за допомогою тумблерів	Візуальний	а) Установлюється наявність тумблера і відповідність його вмикання схемі б) Перевіряється працездатність тумблера шляхом посилення виклику з іншого телефонного апарата в) Установлюється наявність безрозривної розетки
Установлення у дзвінкове коло телефонних апаратів, не призначених для пересилання ІзОД, елементів діодного захисту	Апаратурний	Під час відключення апарата приладом типу Ц-4313 на шкалі x10 зчитується величина опору паралельно ввімкнутих діодів, яка повинна знаходитися в інтервалі 50 - 170 Ом
Відключення гучномовця на період проведення конфіденційних переговорів лініями ОТЗ, під час проведення нарад	Візуальний	Перевіряється можливість відключення гучномовця від мережі
Виключення можливості витоку інформативного (небезпечного) сигналу під час роботи переговорних, звукопідсилювальних, звукозаписувальних та звуковідтворювальних пристроїв	Візуальний	Перевіряється можливість відключення зазначених технічних засобів від кіл живлення
Виключення можливості витоку інформативного (небезпечного) сигналу через електронні годинники	Візуальний	Відстань від меж приміщення - не менше 2 м
Виключення можливості витоку інформативного (небезпечного) сигналу через систему пожежно-охоронної сигналізації	Візуальний	Перевіряється відсутність електромагнітного зв'язку з іншими лініями, що виходять з приміщення Перевіряється можливість відключення ліній зв'язку
Виключення можливості витоку інформативного (небезпечного) сигналу через засоби оргтехніки	Візуальний	Перевіряється можливість відключення від кіл живлення